Amazon Relational Database Service

Guide de l'utilisateur

Copyright © 2020 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

Qu'est-ce que Amazon RDS ? 1
- Présentation 1
- Instances DB 2
- Régions et zones de disponibilité AWS 3
- Sécurité 3
- Surveillance d'une instance de base de données Amazon RDS 3
- Comment utiliser Amazon RDS 3
  - AWS Management Console 3
  - interface de ligne de commande 4
  - Programmation avec Amazon RDS 4
- Comment fonctionne la facturation pour Amazon RDS 4
- Quelle est la prochaine étape ? 4
  - Mise en route 4
  - Rubriques spécifiques au moteur de base de données 4
- Instances DB 5
- Classes d'instances de base de données 6
  - Types de classes d'instance de base de données 6
  - Moteurs de base de données pris en charge 7
  - Modification d'une classe d'instance de base de données 13
  - Configuration du processeur 13
  - Spécifications matérielles 25
- Stockage d'instance de base de données 30
  - Types de stockage 30
  - Stockage SSD à usage général 31
  - Stockage sur volumes IOPS provisionnés 33
  - Stockage magnétique 35
  - Surveillance des performances de stockage 35
  - Autres facteurs ayant un impact sur les performances de stockage 36
- Régions, zones de disponibilité et zones locales 39
  - Régions AWS 40
  - Zones de disponibilité 40
  - Zones locales 41
  - Disponibilité dans les régions 41
- Haute disponibilité (Multi-AZ) 43
  - Modification d'une instance de base de données pour qu'elle devienne un déploiement Multi-AZ 44
  - Processus de basculement pour Amazon RDS 45
- Facturation des instances de base de données pour Amazon RDS 47
  - Instances de base de données à la demande 48
  - Instances DB réservées 48

Configuration de 62
- Inscrivez-vous à AWS 62
- Création d'un utilisateur IAM 62
- Déterminer les exigences 64
- Créer un groupe de sécurité qui autorise l'accès à votre instance de base de données dans votre VPC 66

Mise en route 69
- Création d'une instance de base de données MariaDB et connexion à une base de données 69
  - Création d'une instance de base de données MariaDB 70
  - Connexion à une base de données sur une instance de base de données exécutant MariaDB 74
  - Suppression d'une instance DB 76
- Création d'une instance de base de données Microsoft SQL Server et connexion à une instance de base de données 76
  - Création d'un exemple d'instance de base de données SQL Server 77
  - Connexion à votre exemple d'instance de base de données 81
  - Exploration de votre exemple d'instance de base de données 82

Suppression de votre exemple d'instance de base de données 84
Création d'une instance de base de données MySQL et connexion à une base de données 85
Création d'une instance de base de données MySQL 86
Connexion à une base de données sur une instance de base de données exécutant MySQL 90
Suppression d'une instance DB 92
Création d'une instance de base de données Oracle et connexion à une base de données 93
Création d'un exemple d'instance de base de données Oracle 93
Connexion à votre exemple d'instance de base de données 97
Suppression de votre exemple d'instance de base de données 99
Création d'une instance de base de données PostgreSQL et connexion à une base de données 99
Création d'une instance de base de données PostgreSQL 100
Connexion à une instance de base de données PostgreSQL 104
Suppression d'une instance DB 108
Didacticiel : Créer un serveur web et une instance de base de données Amazon RDS 109
Créez une instance de base de données. 110
Créer un serveur web 121
Didacticiels 134
Bonnes pratiques relatives à Amazon RDS. 135
Directives opérationnelles de base Amazon RDS 135
Recommandations RAM d'une instance de base de données 136
Utilisation de la surveillance améliorée pour identifier les problèmes de système d'exploitation 136
Utilisation des métriques pour identifier les problèmes de performances 137
Consultation des métriques de performances 137
Évaluation des métriques de performances 138
Réglage des requêtes 140
Bonnes pratiques pour utiliser les moteurs de stockage MySQL 141
Bonnes pratiques pour utiliser les moteurs de stockage MariaDB 142
Bonnes pratiques d'utilisation d'Oracle 142
Bonnes pratiques pour utiliser les moteurs de stockage PostgreSQL 142
Chargement des données dans une instance de base de données PostgreSQL 142
Utilisation de la fonction autovacuum de PostgreSQL 143
Bonnes pratiques pour l'utilisation de SQL Server 144
Vidéo sur les bonnes pratiques SQL Server Amazon RDS 145
Utilisation des groupes de paramètres DB 145
Vidéo de présentation des nouvelles fonctionnalités et des bonnes pratiques pour Amazon RDS 145
Configuration d'une instance de base de données 146
Création d'une instance de base de données 146
Paramètres disponibles 151
Exemple de console d'origine 165
Connexion à une instance de base de données 169
Gestion des connexions avec RDS Proxy 169
Utilisation de groupes d'options 209
Présentation des groupes d'options 210
Création d'un groupe d'options 212
Copie d'un groupe d'options 213
Ajout d'une option à un groupe d'options 214
Liste des options et des paramètres d'options pour un groupe d'options 219
Modification d'un paramètre d'option 219
Suppression d'une option d'un groupe d'options 222
Suppression d'un groupe d'options 224
Utilisation des groupes de paramètres 225
Création d'un groupe de paramètres de bases de données 227
Modification de paramètres dans un groupe de paramètres de bases de données 229
Copie d'un groupe de paramètres de bases de données 231
Liste des groupes de paramètres de bases de données 233
Affichage des valeurs de paramètres pour un groupe de paramètres de bases de données 234
Comparaison des groupes de paramètres de bases de données 235

Valeurs de paramètres de bases de données 235
Gestion d'une instance de base de données 239
Arrêt d'une instance de base de données 239
Avantages 240
Limites 240
Considérations relatives au groupe d'options et de paramètres 241
Considérations VPC 241
Arrêt d'une instance de base de données 241
Démarrage d'une instance de base de données 242
Modification d'une instance de base de données 243
Paramètre Appliquer immédiatement 244
Paramètres disponibles 245
Entretien d'une instance de base de données 260
Application des mises à jour 262
Maintenance pour les déploiements multi-AZ 264
Le créneau de maintenance 264
Ajustement du créneau de maintenance pour une instance de bases de données 266
Mise à niveau de la version du moteur 267
Mise à niveau manuelle de la version du moteur 268
Mise à niveau automatique de la version mineure du moteur 269
Affectation d'un nouveau nom à une instance DB 270
Renommer pour remplacer une instance de base de données existante 271
Redémarrage d'une instance DB 272
Utilisation des réplicas en lecture 275
Présentation 276
Création d'un réplica en lecture 280
Promotion d'un réplica en lecture 282
Création d'un réplica en lecture dans une autre région AWS 284
Supervision de la réplication en lecture 291
Balisage des ressources RDS 293
Présentation 294
Utilisation des ARN 298
Construction d'un ARN 298
Obtention d'un ARN existant 302
Utilisation du stockage 304
Augmentation de la capacité de stockage d'une instance de base de données 304
Gestion automatique de la capacité avec le dimensionnement automatique du stockage 306
Modification des IOPS provisionnées 311
Suppression d'une instance de base de données 313
Protection contre la suppression 313
Instantanés finaux et sauvegardes conservées 313
Suppression d'une instance DB 314
Sauvegarde et restauration d'une instance de base de données 317
Utilisation des sauvegardes 317
Stockage de sauvegarde 318
Fenêtre de sauvegarde 318
Période de rétention des sauvegardes 319
Désactivation des sauvegardes automatiques 320
Activation des sauvegardes automatiques 321
Conservation des sauvegardes automatiques 323
Sauvegardes automatiques avec moteurs de stockage MySQL non pris en charge 326
Sauvegardes automatiques avec moteurs de stockage MariaDB non pris en charge 327
..... 327
Création d'un instantané de base de données 327
Restauration à partir d'un instantané de base de données 329
Groupes de paramètres 330
Groupes de sécurité 330

Groupes d'options ... 330
Microsoft SQL Server ... 331
Oracle ... 331
Restaurer à partir d'un instantané ... 331
Copie d'un instantané ... 332
Limites ... 332
Conservation des instantanés ... 333
Instantanés partagés ... 333
Chiffrement ... 333
Copie d'instantané incrémentielle ... 334
Copie d'instantanés dans des régions AWS ... 334
Groupes d'options ... 335
Groupes de paramètres ... 335
Copie d'un instantané de base de données ... 335
Partage d'un instantané ... 342
Partage d'un instantané chiffré ... 343
Partage d'un instantané ... 346
Exportation de données d'instantanés vers Amazon S3 ... 349
Présentation de l'exportation des données d'instantané ... 350
Configuration de l'accès à un compartiment S3 ... 351
Exportation d'un instantané vers un compartiment S3 ... 353
Surveillance des exportations d'instantanés ... 355
Annulation d'une exportation d'instantané ... 357
Dépannage des erreurs d'autorisations PostgreSQL ... 358
Conversion des données ... 358
Restauration à un instant dans le passé ... 365
Suppression d'un instantané ... 367
Suppression d'un instantané de base de données ... 367
Didacticiel : restaurer une instance de base de données à partir d'un instantané de base de données ... 368
Conditions requises pour la restauration d'une instance de base de données à partir d'un instantané de base de données ... 369
Restauration d'une instance de base de données à partir d'un instantané de base de données ... 370
Modification d'une instance de base de données restaurée ... 371
Surveillance d'une instance de base de données ... 373
Présentation de la surveillance ... 373
Plan de surveillance ... 373
Référence des performances ... 373
Instructions sur les performances ... 374
Outils de surveillance ... 374
Surveillance avec CloudWatch ... 376
Publication dans CloudWatch Logs. ... 383
Statut d'instance de bases de données ... 386
Utilisation des recommandations Amazon RDS ... 389
Réponse aux recommandations ... 391
Surveillance améliorée ... 394
Disponibilité de la surveillance améliorée ... 394
Différences entre les métriques CloudWatch et de surveillance améliorée ... 395
Configuration et activation de la surveillance améliorée ... 395
Affichage de la surveillance améliorée ... 398
Affichage de la surveillance améliorée à l'aide de CloudWatch Logs ... 401
Performance Insights ... 410
Présentation ... 411
Activation et désactivation de Performance Insights ... 413
Accès à Performance Insights ... 418
Surveillance avec le tableau de bord de Performance Insights ... 419
Personnalisation du tableau de bord de Performance Insights ... 440
Récupération de données avec l'API Performance Insights ... 451

Métriques publiées dans CloudWatch 464
Journalisation des appels d'Analyse des performances à l'aide d'AWS CloudTrail 465
Utilisation de la notification d'événement Amazon RDS 467
Catégories d'événements et messages d'événements Amazon RDS 469
Abonnement à la notification d'événement Amazon RDS 478
Liste des abonnements aux notifications d'événements Amazon RDS 480
Modification d'un abonnement aux notifications d'événements Amazon RDS 481
Ajout d'un identifiant source à un abonnement aux notifications d'événements Amazon RDS 482
Suppression d'un identifiant source d'un abonnement aux notifications d'événements Amazon RDS 483
Affichage des catégories aux notifications d'événements Amazon RDS 484
Suppression d'un abonnement aux notifications d'événements Amazon RDS 485
Affichage d'événements Amazon RDS 486
Console 486
AWS CLI 487
API 487
..... 487
Événements CloudWatch Events et EventBridge pour Amazon RDS 487
Envoi d'événements Amazon RDS à CloudWatch Events 488
Événements d'instance de base de données 488
Événements de groupe de paramètres de base de données 489
Événements de groupe de sécurité de base de données 489
Événements d'instantané de bases de données 490
Fichiers journaux de base de données 490
Liste et affichage des fichiers journaux de base de données 491
Téléchargement d'un fichier journal de base de données 491
Consultation d'un fichier journal de base de données 493
Publication dans CloudWatch Logs. 493
Lecture du contenu des fichiers journaux avec REST 493
Fichiers journaux de base de données MariaDB 494
Fichiers journaux de base de données Microsoft SQL Server 503
Fichiers journaux de base de données MySQL 506
Fichiers journaux de base de données Oracle 515
Fichiers journaux de base de données PostgreSQL 521
Utilisation de AWS CloudTrail et Amazon RDS 526
Intégration de CloudTrail à Amazon RDS 526
Entrées de fichier journal Amazon RDS 527
Utilisation de RDS sur AWS Outposts 530
Prérequis 530
Prise en charge pour les fonctions Amazon RDS 531
Classes d'instances de bases de données prises en charge 534
Création d'instances de bases de données 535
MariaDB sur Amazon RDS 542
Tâches courantes de gestion 542
Versions de MariaDB 544
Prise en charge des fonctions MariaDB 546
Prise en charge de MariaDB 10.4 546
Prise en charge de MariaDB 10.3 546
Prise en charge de MariaDB 10.2 547
Prise en charge de MariaDB 10.1 547
Prise en charge de MariaDB 10.0 547
Fonctions non prises en charge 548
Moteurs de stockage pris en charge 548
Limites de taille des fichiers 549
Sécurité MariaDB 550
SSL Support 551
Préparation du cache 553

Vidage et chargement du pool de tampons à la demande 554
Paramètres de la base de données. 554
Tâches d'administrateur de base de données courantes 554
Fuseau horaire local 554
Connexion à une instance de base de données exécutant MariaDB 556
Connexion depuis l'utilitaire mysql 558
Connexion à SSL 558
Dépannage 559
Mise à jour des applications pour les nouveaux certificats SSL/TLS 560
Contrôle de la nécessité d'une vérification du certificat du client pour qu'il puisse se connecter 561
Mise à jour du magasin d'approbations de votre application 562
Exemple de code Java pour l'établissement de connexions SSL 563
Mise à niveau du moteur de base de données MariaDB 564
Présentation 564
Mises à niveau de version majeure. 566
Mise à niveau d'une instance de base de données MariaDB 566
Mises à niveau automatiques des versions mineures 566
Migration des données à partir d'un instantané de base de données MySQL vers une instance de base de données MariaDB 568
Incompatibilités entre MariaDB et MySQL 569
Exécution de la migration 569
Utilisation de la réplication MariaDB 573
Utilisation de réplicas en lecture MariaDB 574
Configuration de la réplication GTID 577
Importation de données dans une instance de base de données MariaDB 580
Options pour MariaDB 581
Prise en charge du plug-in d'audit MariaDB 581
Paramètres pour MariaDB 584
Référence MariaDB sur SQL Amazon RDS 589
mysql.rds_set_external_master_gtid 589
mysql.rds_kill_query_id 591
Microsoft SQL Server sur Amazon RDS 592
Tâches courantes de gestion 593
Restrictions 594
Assistance pour les classes d'instance de base de données 597
Sécurité 598
Programmes de conformité 599
HIPAA 599
Prise en charge SSL 600
Prise en charge des versions 600
Gestion des versions 602
Correctifs et versions de moteur de base de données 602
Calendrier d'obsolescence 602
Prise en charge des fonctionnalités 602
Fonctionnalités de SQL Server 2019 603
Fonctionnalités de SQL Server 2017 603
Fonctionnalités de SQL Server 2016 604
Fonctionnalités de SQL Server 2014 604
Fonctionnalités de SQL Server 2012 604
SQL Server 2008 R2 obsolète sur Amazon RDS 605
Prise en charge des CDC 605
Fonctions non prises en charge et fonctions avec prise en charge limitée 606
Déploiements multi-AZ 606
Utilisation de TDE 607
Fonctions et procédures stockées 607
Fuseau horaire local 609
Fuseaux horaires pris en charge 610

Gestion des licences SQL Server sur Amazon RDS 617
Restauration des instances de bases de données résiliées faute de licence 618
SQL Server Developer Edition 618
Connexion à une instance de base de données exécutant SQL Server 618
Connexion à votre instance de base de données avec SSMS 619
Connexion à votre instance de base de données avec SQL Workbench/J 622
Considérations relatives aux groupes de sécurité 624
Dépannage 624
Mise à jour des applications pour les nouveaux certificats SSL/TLS 625
Contrôle de la connexion des applications aux instances de bases de données Microsoft SQL Server avec un protocole SSL 626
Contrôle de la nécessité d'une vérification du certificat du client pour qu'il puisse se connecter 626
Mise à jour du magasin d'approbations de votre application 628
Mise à niveau du moteur de base de données SQL Server 629
Présentation 630
Mises à niveau de version majeure. 631
Considérations relatives à l'environnement Multi-AZ et à l'optimisation en mémoire 632
Considérations relatives au groupe d'options et de paramètres 632
Test d'une mise à niveau 633
Mise à niveau d'une instance de base de données SQL Server 634
Mise à niveau des instances de base de données obsolètes avant la fin de la prise en charge 634
Importation et exportation de bases de données SQL Server 634
Limitations et recommandations 635
Configuration de 637
Utilisation des sauvegarde et restauration natives 639
Compression des fichiers de sauvegarde 650
Dépannage 651
..... 652
Importation et exportation de données SQL Server à l'aide d'autres méthodes 652
Utilisation des réplicas en lecture SQL Server 662
Configuration des réplicas en lecture pour SQL Server 662
Limites des réplicas en lecture avec SQL Server 663
Résolution d'un problème de réplica en lecture SQL Server 663
Multi-AZ pour SQL Server 664
Ajout de Multi-AZ à une instance de base de données SQL Server 665
Notes et recommandations 665
Détermination de l'emplacement du réplica secondaire 667
Migration vers les groupes de disponibilité Always On 668
Fonctionnalités supplémentaires pour SQL Server 668
Utilisation de SSL avec une instance DB SQL Server 669
Configuration des protocoles de sécurité et des chiffrements 672
Utilisation de l'authentification Windows avec une instance de base de données d'instance de base de données 676
Intégration Amazon S3 686
Options pour SQL Server 699
Sauvegarde et restauration natives 701
Transparent Data Encryption 704
SQL Server Audit 707
SQL Server Analysis Services 713
SQL Server Integration Services 724
SQL Server Reporting Services 738
Microsoft Distributed Transaction Coordinator 748
Tâches d'administrateur de base de données courantes pour SQL Server 759
Accès à la base de données tempdb 760
Analyse de la charge de travail de votre base de données avec l'Assistant de réglage SQL Server 762
Collectes et jeux de caractères 766
Détermination d'un modèle de récupération 768

Détermination de l'heure du dernier basculement 769
Désactivation des insertions rapides 770
Suppression d'une base de données SQL Server 770
Modification du nom d'une base de données Multi-AZ 771
Réinitialisation du mot de passe du rôle `db_owner` 771
Restauration des instances de bases de données résiliées faute de licence 771
Passage d'une base de données de l'état OFFLINE à l'état ONLINE 772
Utilisation de CDC 772
Utilisation de SQL Server Agent 775
Utilisation des journaux SQL Server 776
Utilisation des fichiers de trace et de vidage 777
MySQL sur Amazon RDS 779
Tâches courantes de gestion 779
Versions MySQL 782
Fonctions MySQL non prises en charge par Amazon RDS 785
Moteurs de stockage pris en charge 785
Sécurité MySQL 786
Plug-in de validation de mot de passe 787
SSL Support 788
Utilisation de memcached et d'autres options avec MySQL 790
Préparation du cache InnoDB 790
Vidage et chargement du pool de tampons à la demande 791
Fuseau horaire local 791
Limites et problèmes connus 793
Connexion à une instance de base de données exécutant MySQL 793
Connexion depuis le client MySQL 795
Connexion à SSL 795
Connexion depuis MySQL Workbench 796
Dépannage 798
Mise à jour des applications pour les nouveaux certificats SSL/TLS 799
Contrôle de la connexion des applications aux instances de bases de données MySQL avec le protocole SSL 800
Contrôle de la nécessité d'une vérification du certificat du client pour qu'il puisse se connecter 801
Mise à jour du magasin d'approbations de votre application 802
Exemple de code Java pour l'établissement de connexions SSL 803
Mise à niveau du moteur de base de données MySQL 804
Présentation 805
Mises à niveau de version majeure. 806
Test d'une mise à niveau 809
Mise à niveau d'une instance de base de données MySQL 810
Mises à niveau automatiques des versions mineures 810
Mise à niveau d'une base de données MySQL avec des temps d'arrêt réduits 812
Mise à niveau d'un instantané de base de données MySQL 813
Importation de données dans une instance de base de données MySQL 815
Présentation 815
Considérations sur l'importation de données 817
Restauration d'une sauvegarde dans une instance de base de données MySQL Amazon RDS 821
Importation de données à partir d'une base de données MySQL ou MariaDB vers une instance de base de données MySQL ou MariaDB Amazon RDS 830
Importation de données vers une instance de base de données MySQL ou MariaDB Amazon RDS avec un temps réduit 832
Importation de données à partir d'une source vers une instance de base de données MySQL ou MariaDB 846
Utilisation de la réplication MySQL 850
Utilisation de réplicas en lecture MySQL 851
Utilisation de la réplication basée sur des identifiants de transaction globaux (GTID) 857
Réplication avec une instance MySQL ou MariaDB s'exécutant à l'extérieur d'Amazon RDS 863

Exportation de données à partir d'une instance de base de données MySQL 869
Préparer une base de données MySQL externe 870
Préparer l'instance de base de données MySQL source 870
Copier la base de données 871
Terminer l'exportation 873
Options pour MySQL 873
Plug-in d'audit MariaDB 874
memcached 877
Tâches d'administrateur de base de données courantes pour MySQL 881
Mettre fin à une session ou à une requête 881
Ignorer une erreur de réplication 881
Utilisation des tablespaces InnoDB pour améliorer les temps de récupération sur incident 882
Gestion de l'historique global des statuts 884
Utilisation de l'authentification Kerberos pour MySQL 885
Configuration de l'authentification Kerberos pour les instances de base de données MySQL 887
Gestion d'une instance de base de données dans un domaine 894
Connexion à MySQL avec l'authentification Kerberos 895
Restauration d'une instance de base de données MySQL et ajout de cette instance à un domaine 895
Limitations MySQL de l'authentification Kerberos 895
Limites et problèmes connus 896
Taille de pool de mémoires tampons InnoDB incohérente 896
L'optimisation de la fusion d'index retourne des résultats erronés 896
Taille des fichiers journaux 897
Exceptions des paramètres MySQL pour les instances de base de données Amazon RDS 897
Limites de taille des fichiers MySQL dans Amazon RDS 898
Plug-in MySQL Keyring non pris en charge 899
Référence SQL de MySQL sur Amazon RDS 899
Présentation 899
Conventions du guide de référence SQL 900
mysql.rds_set_master_auto_position 901
mysql.rds_set_external_master 901
mysql.rds_set_external_master_with_delay 904
mysql.rds_set_external_master_with_auto_position 907
mysql.rds_reset_external_master 909
mysql.rds_import_binlog_ssl_material 910
mysql.rds_remove_binlog_ssl_material 912
mysql.rds_set_source_delay 912
mysql.rds_start_replication 913
mysql.rds_start_replication_until 914
mysql.rds_start_replication_until_gtid 915
mysql.rds_stop_replication 916
mysql.rds_skip_transaction_with_gtid 916
mysql.rds_skip_repl_error 917
mysql.rds_next_master_log 918
mysql.rds_innodb_buffer_pool_dump_now 920
mysql.rds_innodb_buffer_pool_load_now 920
mysql.rds_innodb_buffer_pool_load_abort 920
mysql.rds_set_configuration 921
mysql.rds_show_configuration 922
mysql.rds_kill 923
mysql.rds_kill_query 924
mysql.rds_rotate_general_log 924
mysql.rds_rotate_slow_log 924
mysql.rds_enable_gsh_collector 925
mysql.rds_set_gsh_collector 925
mysql.rds_disable_gsh_collector 925
mysql.rds_collect_global_status_history 926

mysql.rds_enable_gsh_rotation 926
mysql.rds_set_gsh_rotation 926
mysql.rds_disable_gsh_rotation 926
mysql.rds_rotate_global_status_history 926
Oracle sur Amazon RDS 928
Tâches courantes de gestion 928
Licences 930
Licence incluse 930
Bring Your Own License (Licence à fournir) 931
Licences des déploiements multi-AZ Oracle 933
Migration d'une édition Oracle à une autre 933
Assistance pour les classes d'instance de base de données 933
Classes d'instance de base de données db.t2 obsolètes 935
Classes d'instance de base de données db.m3 et db.r3 obsolètes 936
Classes d'instance de base de données db.m1 et db.m2 obsolètes 936
Limites de taille des fichiers 937
Sécurité 937
SSL Support 937
Oracle 19c 938
Modifications des paramètres Amazon RDS pour Oracle 19c version 19.0.0.0 938
Oracle 18c 939
Évolution des paramètres Amazon RDS pour Oracle 18c version 18.0.0.0 939
Oracle 12c 940
Oracle 12c, version 12.2.0.1 940
Oracle 12c, version 12.1.0.2 943
Prise en charge des fonctions Oracle Database 950
Prise en charge des paramètres Oracle Database 952
Gestion de la version du moteur 953
Obsolescence d'Oracle 11.2.0.4 953
Utilisation de HugePages 954
Utilisation de utl_http, utl_tcp et utl_smtp 957
Utilisation d'OEM, d'APEX, de TDE et d'autres options 959
Utilisation des types de données étendus 959
Activation des types de données étendus pour une nouvelle instance de base de données 960
Activation des types de données étendus pour une instance de base de données existante 960
Synonymes publics 961
Connexion à une instance Oracle 961
Recherche du point de terminaison 961
SQL Developer 963
SQL*Plus 966
Considérations relatives aux groupes de sécurité 967
Processus serveur dédiés et partagés 967
Dépannage 968
Mise à jour des applications pour les nouveaux certificats SSL/TLS 969
Déterminer si les applications utilisent SSL pour votre instance de base de données 970
Mise à jour du magasin d'approbations de votre application 970
Exemple de code Java pour l'établissement de connexions SSL 972
Modification des paramètres Oracle sqlnet.ora 972
Définition des paramètres sqlnet.ora 973
Paramètres sqlnet.ora pris en charge 973
Affichage des paramètres sqlnet.ora 974
Mise à niveau du moteur de base de données Oracle 975
Présentation des mises à niveau Oracle 976
Mises à niveau de version majeure. 977
Mises à niveau de version mineure. 979
Chemins de mise à niveau SE2 979
Considérations relatives aux mises à niveau 980

Test d'une mise à niveau 981
Mise à niveau automatique de 11g SE1 982
Mise à niveau d'une instance de base de données Oracle 987
Mise à niveau d'un instantané de base de données Oracle 988
Console 988
AWS CLI 989
API RDS 989
Importation de données dans Oracle 990
Importation à l'aide d'Oracle SQL Developer 991
Importation à l'aide d'Oracle Data Pump 991
Utilitaires Oracle Export/Import 1000
Oracle SQL*Loader 1001
Vues matérialisées Oracle 1002
Utilisation des réplicas Oracle 1003
Présentation des réplicas Oracle 1003
Exigences de réplica pour Oracle 1004
Préparation de la création d'un réplica pour Oracle 1005
Création d'un réplica Oracle en mode monté 1007
Modification du mode réplica Oracle 1008
Dépannage des réplicas Oracle 1009
Jeux de caractères Oracle 1010
Jeu de caractères de base de données 1010
Jeu de caractères national 1012
Options pour Oracle 1013
Intégration Amazon S3 1014
Application Express (APEX) 1026
Enterprise Manager 1037
Java Virtual Machine (JVM) 1052
Label Security 1054
Locator 1057
Multimédia 1060
Chiffrement de réseau natif (Native Network Encryption, NNE) 1062
OLAP 1066
Secure Sockets Layer (SSL) 1068
Spatial 1077
SQLT 1080
Statspack 1085
Fuseau horaire 1088
Transparent Data Encryption (TDE) (Chiffrement transparent des données) 1091
UTL_MAIL 1093
XML DB 1096
Tâches courantes d'administrateur de base de données pour Oracle 1097
Tâches système 1103
Tâches de base de données 1115
Tâches de journal 1129
Tâches RMAN 1136
Tâches Oracle Scheduler 1153
Tâches de diagnostic 1158
Autres tâches 1164
Utilisation de l'authentification Kerberos 1168
Configuration de 1170
Gestion d'une instance de base de données 1179
Connexion avec l'authentification Kerberos 1181
Outils et des logiciels tiers pour Oracle 1182
Configuration de 1182
Utilisation d'Oracle GoldenGate 1188
Utilisation de l'utilitaire Oracle Repository Creation Utility 1200

Installation d'une base de données Siebel sur Oracle sur Amazon RDS 1205
Notes de mise à jour pour le moteur de base de données Oracle 1208
Oracle versions 19.0.0, 18.0.0 et 12.2.0.1 1208
Oracle 12.1.0.2 et 11.2.0.4 1209
Moteur de base de données : 19.0.0.0 1210
Moteur de base de données : 18.0.0.0 1231
Moteur de base de données : 12.2.0.1 1248
Moteur de base de données : 12.1.0.2 1277
Moteur de base de données : 11.2.0.4 1321
PostgreSQL sur Amazon RDS 1361
Tâches courantes de gestion pour PostgreSQL sur Amazon RDS 1362
Connexion à une instance de base de données exécutant le moteur de base de données PostgreSQL . 1364
Utilisation de pgAdmin pour se connecter à une instance de base de données PostgreSQL 1365
Utilisation de psql pour se connecter à une instance de base de données PostgreSQL 1368
Résolution des problèmes de connexion à votre instance PostgreSQL 1368
Mise à jour des applications pour les nouveaux certificats SSL/TLS 1369
Contrôle de la connexion des applications aux instances de bases de données PostgreSQL avec le protocole SSL 1370
Contrôle de la nécessité d'une vérification du certificat du client pour qu'il puisse se connecter 1371
Mise à jour du magasin d'approbations de votre application 1371
Utilisation des connexions SSL/TLS pour différents types d'application 1372
Mise à niveau du moteur de base de données PostgreSQL 1373
Présentation de la mise à niveau 1374
Numéros de version PostgreSQL 1375
Choix d'une mise à niveau de version majeure 1375
Comment effectuer une mise à niveau de version majeure 1377
Mises à niveau automatiques des versions mineures 1381
Mise à niveau des extensions PostgreSQL 1382
Mise à niveau d'un instantané de base de données PostgreSQL 1382
Utilisation de réplicas en lecture PostgreSQL 1384
Configuration de réplicas en lecture avec PostgreSQL 1385
Surveillance des réplicas en lecture PostgreSQL 1386
Limites des réplicas en lecture avec PostgreSQL 1386
Interruption de réplication avec les réplicas en lecture PostgreSQL 1386
Dépannage d'un problème de réplica en lecture PostgreSQL 1387
Importation de données dans PostgreSQL sur Amazon RDS 1388
Importation d'une base de données PostgreSQL à partir d'une instance Amazon EC2 1390
Utilisation de la commande \copy pour importer des données dans une table sur une instance de base de données PostgreSQL 1392
Importation de données S3 dans RDS for PostgreSQL 1393
Transport de bases de données PostgreSQL entre des instances de base de données 1405
Exportation de données PostgreSQL vers des fichiers Amazon S3 1409
Présentation de l'exportation vers S3 1410
Spécification du chemin d'accès au fichier Amazon S3 vers lequel effectuer l'exportation 1411
Configuration de l'accès à un compartiment Amazon S3 1411
Exportation de données de requête à l'aide de la fonction aws_s3.query_export_to_s3 1414
Guide de référence des fonctions 1416
Tâches DBA courantes pour PostgreSQL 1419
Création de rôles 1420
Gestion d'un accès à la base de données PostgreSQL 1420
Utilisation des paramètres PostgreSQL 1421
Utilisation de la fonction autovacuum de PostgreSQL 1431
Journalisation d'audit pour une instance de base de données PostgreSQL 1440
Utilisation de l'extension pgaudit 1440
Utilisation de l'extension pg_repack 1442
Utilisation de PostGIS 1443
Utilisation de pgBadger pour l'analyse de journal serveur avec PostgreSQL 1445

Affichage du contenu de pg_config 1445
Utilisation de l'extension orafce 1446
Accès aux données externes à l'aide de l'extension postgres_fdw 1447
Utilisation d'un serveur DNS personnalisé pour l'accès réseau sortant. 1448
Restriction de la gestion des mots de passe 1449
Utilisation de l'authentification Kerberos 1450
Présentation de l'authentification Kerberos 1451
Configuration de 1452
Gestion d'une instance de base de données dans un domaine 1462
Connexion avec l'authentification Kerberos 1463
Utilisation de l'environnement en préversion de base de données 1465
Fonctions non prises en charge dans l'environnement en préversion 1465
Extensions PostgreSQL prises en charge dans l'environnement en préversion 1466
Création d'une nouvelle instance de base de données dans l'environnement en préversion 1467
Versions et extensions PostgreSQL 1468
Versions de base de données PostgreSQL prises en charge 1468
Fonctions et extensions prises en charge 1488
Sécurité 1518
Authentification de base de données 1519
Authentification par mot de passe 1519
Authentification de base de données IAM 1520
Authentification Kerberos 1520
Protection des données 1521
Chiffrement des données 1521
Confidentialité du trafic inter-réseaux 1535
Identity and Access Management 1536
Public ciblé 1536
Authentification avec des identités 1537
Gestion de l'accès à l'aide de stratégies 1539
Fonctionnement d'Amazon RDS avec IAM 1540
Exemples de stratégies basées sur l'identité 1544
Authentification de base de données IAM pour MySQL et PostgreSQL 1554
Dépannage 1581
Journalisation et surveillance 1583
Validation de la conformité 1584
Résilience 1585
Sauvegarde et restauration 1585
Réplication 1586
Basculement 1586
Sécurité de l'infrastructure 1586
Groupes de sécurité 1586
Accessibilité publique 1587
Points de terminaison d'un VPC AWS PrivateLink 1587
Considérations 1587
Disponibilité 1588
Création d'un point de terminaison d'un VPC d'interface 1588
Création d’une stratégie de point de terminaison de VPC 1589
Bonnes pratiques de sécurité 1590
Contrôle d'accès par groupe de sécurité 1590
Groupes de sécurité VPC 1591
Groupes de sécurité DB 1591
Groupes de sécurité de base de données vs. Groupes de sécurité VPC 1592
Scénario de groupes de sécurité 1592
Création d'un groupe de sécurité VPC 1593
Association à une instance de bases de données 1593
Suppression de Security Group DB VPC 1593
Groupes de sécurité de base de données sur EC2-Classic 1596

Privilèges du compte utilisateur principal 1605
Rôles liés à un service 1606
Autorisations des rôles liés à un service pour Amazon RDS 1607
Création d'un rôle lié à un service pour Amazon RDS 1608
Modification d'un rôle lié à un service pour Amazon RDS 1609
Suppression d'un rôle lié à un service pour Amazon RDS 1609
Utilisation de Amazon RDS avec Amazon VPC 1610
Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic 1611
Scénarios d'accès à une instance de base de données d'un VPC 1613
Utilisation d'une instance de base de données dans un VPC 1620
Mise à jour du VPC pour une instance de base de données 1627
Didacticiel : créer un Amazon VPC à utiliser avec une instance de base de données 1629
Quotas et contraintes 1635
Quotas dans Amazon RDS 1635
Contraintes d'affectation de noms dans Amazon RDS 1636
Nombre maximal de connexions à une base de données 1637
Limites de taille des fichiers dans Amazon RDS 1638
Dépannage 1639
Impossible de se connecter à l'instance de base de données 1639
Test de connexion d'une instance de base de données 1641
Dépannage des problèmes d'authentification de connexion 1641
Problèmes de sécurité 1641
Message d'erreur « Échec de l'extraction des attributs du compte. Certaines fonctions de la console sont peut être dégradées. » 1642
Réinitialisation du mot de passe du propriétaire de l'instance de base de données 1642
Panne ou redémarrage d'une instance de base de données 1642
Modifications de paramètre n'entrant pas en vigueur 1643
Instance de base de données à court de stockage 1643
Capacité d'instance de base de données insuffisante 1645
Problèmes MySQL et MariaDB 1645
Maximum de connexions MySQL et MariaDB 1646
Diagnostic et résolution du retard entre réplicas en lecture 1646
Diagnostic et résolution d'une défaillance de la réplication en lecture MySQL ou MariaDB 1648
La création de déclencheurs avec la journalisation binaire activée requiert le privilège SUPER 1649
Diagnostic et résolution des défaillances de restauration à un point donné dans le passé 1650
Erreur d'arrêt de réplication 1651
La création de réplica en lecture échoue ou la réplication s'arrête avec l'erreur irrécupérable 1236 1651
Impossible de définir la période de rétention des sauvegardes sur 0 1652
Référence d'API Amazon RDS 1653
Utilisation de l'API Query 1653
Paramètres Query (Requête) 1653
Authentification de demande Query 1654
Applications de dépannage 1654
Récupération d'erreurs 1654
Conseils pour le dépannage 1654
Historique du document 1656
Mises à jour antérieures 1696
Glossaire AWS 1721

Qu'est-ce que Amazon Relational Database Service (Amazon RDS) ?

Amazon Relational Database Service (Amazon RDS) est un service web qui facilite la configuration, l'exploitation et la mise à l'échelle d'une base de données relationnelle dans le Cloud AWS. Il fournit des capacités redimensionnables, à faible coût, pour les bases de données relationnelles classiques, et gère les tâches courantes d'administration de base de données.

> Note
>
> Ce guide traite des moteurs de base de données Amazon RDS autres que Amazon Aurora. Pour plus d'informations sur l'utilisation d'Amazon Aurora, consultez le Guide de l'utilisateur Amazon Aurora.
> Ce guide concerne l'utilisation de Amazon RDS dans le cloud AWS. Pour de plus amples informations sur l'utilisation de Amazon RDS dans des environnements VMware sur site, veuillez consulter le Guide de l'utilisateur Amazon RDS on VMware.

Présentation d'Amazon RDS

Pourquoi vouloir un service géré de base de données relationnelle ? Parce qu'Amazon RDS prend le contrôle de la plupart des tâches de gestion difficiles ou fastidieuses d'une base de données relationnelle:

- Quand vous achetez un serveur, l'UC, la mémoire, le stockage et les IOPS sont tous regroupés ensemble. Avec Amazon RDS, ceux-ci sont séparés les uns des autres, de telle sorte que vous pouvez les faire évoluer indépendamment. Si vous avez besoin de plus d'UC, de moins d'IOPS ou de plus de stockage, vous pouvez les allouer facilement.
- Amazon RDS gère les sauvegardes, les correctifs logiciels, la détection automatique des pannes et la récupération.
- Pour offrir une expérience de service géré, Amazon RDS ne fournit pas l'accès shell aux instances de base de données. Il restreint également l'accès à certaines procédures système et tables qui requièrent des privilèges avancés.
- Vous pouvez avoir des sauvegardes automatiques lorsque vous en avez besoin, ou créer manuellement votre propre instantané de sauvegarde. Vous pouvez utiliser ces sauvegardes pour restaurer une base de données. Le processus de restauration Amazon RDS est fiable et efficace.
- Vous pouvez utiliser les produits de base de données familiers avec : MySQL, MariaDB, PostgreSQL, Oracle ou Microsoft SQL Server.
- Vous pouvez obtenir une haute disponibilité avec une instance principale et une instance secondaire synchrone vers laquelle vous pouvez effectuer le basculement quand le problème se produit. Vous pouvez également utiliser les réplicas en lecture MariaDB, Microsoft SQL Server, MySQL, Oracle et PostgreSQL pour augmenter le dimensionnement en lecture.
- En plus de la sécurité de votre package de base de données, vous pouvez définir les personnes qui ont accès à vos bases de données RDS à l'aide d'AWS Identity and Access Management (IAM) pour définir les utilisateurs et les autorisations. Vous pouvez aussi aider à protéger vos bases de données en les plaçant dans un Virtual Private Cloud.

Si vous n'êtes pas encore familiarisé avec les produits et services AWS, commencez par prendre connaissance des ressources suivantes :

- Pour une présentation de tous les produits AWS, veuillez consulter Qu'est-ce que le cloud computing ?
- Amazon Web Services fournit un certain nombre de services de base de données. Pour obtenir des conseils sur le service le mieux adapté à votre environnement, veuillez consulter Exécution de bases de données sur AWS.

Instances DB

La fondation de base d'Amazon RDS est l'instance de base de données. Une instance de base de données est un environnement de base de données isolé dans le Cloud AWS. Votre instance de base de données peut comporter plusieurs bases de données créées par l'utilisateur. Vous pouvez accéder à votre instance de base de données en utilisant les mêmes outils et applications que ceux utilisés avec une instance de base de données autonome. Vous pouvez créer et modifier une instance de base de données en utilisant l'AWS Command Line Interface, l'API Amazon RDS ou la AWS Management Console.

Chaque instance de base de données exécute un moteur de base de données. Amazon RDS prend actuellement en charge les moteurs de base de données MySQL, MariaDB, PostgreSQL, Oracle et Microsoft SQL Server. Chaque moteur DB a ses propres fonctions prises en charge et chaque version d'un moteur DB peut inclure plusieurs fonctions. En outre, chaque moteur DB possède un ensemble de paramètres au sein d'un groupe de paramètres DB qui contrôle le comportement des bases de données qu'il gère.

Les capacités de calcul et de mémoire d'une instance de base de données sont déterminées par sa classe d'instance de base de données. Vous pouvez sélectionner l'instance de base de données qui correspond le mieux à vos besoins. Si vos besoins évoluent au fil du temps, vous pouvez modifier les instances de base de données. Pour plus d'informations, consultez Classes d'instances de base de données (p. 6).

> Note
>
> Pour les informations de tarification des classes d'instance de base de données, consultez la section Tarification de la page produit Amazon RDS.

Le stockage d'instance de base de données se présente sous trois types : magnétique, à usage général (SSD) et IOPS provisionnées (PIOPS). Ces options se différencient par leurs performances et leurs tarifs, ce qui vous permet d'adapter vos performances de stockage et vos coûts en fonction des besoins de votre base de données. Chaque instance de base de données dispose d'exigences de stockage minimal et maximal en fonction du type de stockage et du moteur de base de données qu'elle prend en charge. Il est important de disposer d'un stockage suffisant pour que vos bases de données puissent devenir plus importantes. De plus, grâce à un stockage suffisant, les fonctionnalités du moteur de base de données ont de l'espace pour écrire des contenus ou des entrées de journal. Pour plus d'informations, consultez Stockage d'instance de base de données Amazon RDS (p. 30).

Vous pouvez exécuter une instance de base de données sur un Virtual Private Cloud (VPC) à l'aide du service Amazon Virtual Private Cloud (Amazon VPC). Lorsque vous utilisez un VPC, vous disposez d'un contrôle total sur l'environnement de réseau virtuel. Vous pouvez choisir votre propre plage d'adresses IP, créer des sous-réseaux et configurer le routage et les listes de contrôle d'accès. Les fonctionnalités de base de Amazon RDS sont les mêmes, qu'il s'exécute dans un VPC ou pas ; Amazon RDS gère les sauvegardes, les correctifs logiciels, la détection automatique de pannes et la récupération. Il n'y a pas de frais supplémentaires pour exécuter votre instance de base de données dans un VPC. Pour de plus amples informations sur l'utilisation de Amazon VPC avec RDS, veuillez consulter VPC Amazon Virtual Private Cloud et Amazon RDS (p. 1610).

Amazon RDS utilise le protocole NTP (Network Time Protocol) pour synchroniser le temps sur les instances de base de données.

Régions et zones de disponibilité AWS

Les ressources du cloud computing Amazon sont hébergées dans des installations de centres de données hautement disponible de différentes régions du monde (par exemple, Amérique du Nord, Europe et Asie). Chaque emplacement de centre de données est appelé région AWS.

Chaque région AWS contient plusieurs emplacements distincts appelés Zones de disponibilité ou AZ. Chaque zone de disponibilité est conçue pour être isolée des défaillances dans d'autres zones de disponibilité. Chacune est conçue pour fournir une connectivité réseau économique à faible latence à d'autres zones de disponibilité de la même région AWS. En lançant des instances dans des zones de disponibilité distinctes, vous pouvez protéger vos applications de la défaillance d'un seul emplacement. Pour plus d'informations, consultez Régions, zones de disponibilité et zones locales (p. 39).

Vous pouvez exécuter votre instance de base de données dans plusieurs zones de disponibilité, option appelée déploiement Multi-AZ. Lorsque vous choisissez cette option, Amazon effectue automatiquement la mise en service et la maintenance d'une instance de base de données de secours secondaire dans une autre zone de disponibilité. Votre instance de base de données principale est répliquée de manière synchrone entre les zones de disponibilité (AZ) dans l'instance secondaire. Cette approche permet de fournir la redondance des données et le support de basculement, élimine les figements d'E/S et minimise les pics de latence pendant les sauvegardes du système. Pour plus d'informations, consultez Haute disponibilité (multi-AZ) pour Amazon RDS (p. 43).

Sécurité

Un groupe de sécurité contrôle l'accès à une instance de base de données. Il y parvient en autorisant l'accès aux plages d'adresses IP ou aux instances Amazon EC2 que vous spécifiez.

Pour plus d'informations sur les groupes de sécurité, consultez Sécurité dans Amazon RDS (p. 1518).

Surveillance d'une instance de base de données Amazon RDS

Il existe plusieurs façons dont vous pouvez suivre les performances et l'état d'une instance de base de données. Vous pouvez utiliser le service Amazon CloudWatch pour surveiller les performances et l'intégrité d'une instance de base de données. Les graphiques de performances CloudWatch sont affichés dans la console Amazon RDS. Vous pouvez également vous abonner aux événements Amazon RDS pour être averti de toute modification d'une instance de base de données, d'un instantané de base de données, d'un groupe de paramètres de base de données ou d'un groupe de sécurité de base de données. Pour de plus amples informations, veuillez consulter Surveillance d'une instance de base de données Amazon RDS (p. 373).

Comment utiliser Amazon RDS

Il existe plusieurs manières d'interagir avec Amazon RDS.

AWS Management Console

AWS Management Console est une interface utilisateur web simple. Vous pouvez gérer vos instances de bases de données à partir de la console sans programmation requise. Pour accéder à la console Amazon RDS, connectez-vous à AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds.

interface de ligne de commande

Vous pouvez utiliser l'AWS Command Line Interface (AWS CLI) pour accéder à l'API Amazon RDS de manière interactive. Pour installer l'AWS CLI, consultez Installation de l'interface de ligne de commande AWS. Pour commencer à utiliser l'AWS CLI pour RDS, consultez la Référence de l'AWS Command Line Interface pour Amazon RDS.

Programmation avec Amazon RDS

Si vous êtes un développeur, vous pouvez accéder à Amazon RDS par programmation. Pour plus d'informations, consultez Référence d'Interface de programmation d'application (API) Amazon RDS (p. 1653).

Pour le développement d'applications, nous vous recommandons d'utiliser l'un des kits SDK AWS. Les kits SDK AWS gèrent les détails de bas niveau, tels que l'authentification, la logique de nouvelle tentative et le traitement des erreurs, pour vous permettre de vous concentrer sur la logique de l'application. Les kits SDK AWS sont disponibles dans une grande variété de langues. Pour de plus amples informations, veuillez consulter Outils pour Amazon Web Services.

AWS fournit également des bibliothèques, des exemples de code, des didacticiels et d'autres ressources pour vous aider à faire vos premiers pas. Pour de plus amples informations, veuillez consulter Exemples de codes et bibliothèques.

Comment fonctionne la facturation pour Amazon RDS

Lorsque vous utilisez Amazon RDS, vous pouvez choisir d'utiliser des instances de base de données à la demande ou réservées. Pour plus d'informations, consultez Facturation d'une instance de base de données pour Amazon RDS (p. 47).

Pour plus d'informations sur la tarification de Amazon RDS, consultez la page produit de Amazon RDS.

Quelle est la prochaine étape ?

La section précédente vous a présenté les composants de base de l'infrastructure que propose RDS. Qu'allez-vous faire ensuite ?

Mise en route

Créez une instance de base de données à l'aide des instructions dans Mise en route avec Amazon RDS (p. 69).

Rubriques spécifiques au moteur de base de données

Vous pourrez vérifier les informations spécifiques à un moteur DB particulier dans les sections suivantes :

- MariaDB sur Amazon RDS (p. 542)
- Microsoft SQL Server sur Amazon RDS (p. 592)
- MySQL sur Amazon RDS (p. 779)
- Oracle sur Amazon RDS (p. 928)
- PostgreSQL sur Amazon RDS (p. 1361)

Instances de base de données Amazon RDS

Une instance de bases de données est un environnement de base de données isolé s'exécutant dans le cloud. Elle constitue la composante de base d'Amazon RDS. Une instance de base de données peut comporter plusieurs bases de données créées par l'utilisateur et est accessible avec les mêmes applications et outils clients que ceux que vous utiliseriez pour accéder à une instance de base de données autonome. Les instances de bases de données sont simples à créer et à modifier avec les outils de ligne de commande Amazon AWS, les opérations d'API Amazon RDS ou l'AWS Management Console.

> **Note**
>
> Amazon RDS prend en charge l'accès aux bases de données à l'aide de toute application client SQL standard. Amazon RDS ne permet pas d'accès direct à l'hôte.

Vous pouvez avoir jusqu'à 40 instances de base de données Amazon RDS, avec les limitations suivantes :

- 10 instances de chaque édition SQL Server (Enterprise, Standard, Web et Express) sous le modèle « license-included (licence incluse) »
- 10 instances pour Oracle sous le modèle « license-included (licence incluse) »
- 40 instances pour MySQL, MariaDB ou PostgreSQL
- 40 instances pour Oracle sous le modèle « Réutilisez vos licences »

> **Note**
>
> Si votre application nécessite plusieurs instances de bases de données, vous pouvez demander des instances de bases de données supplémentaires à l'aide de ce formulaire.

Chaque instance de base de données possède un identifiant d'instance de base de données. Ce nom fourni par le client identifie de façon unique l'instance de base de données lors de l'interaction avec les API Amazon RDS et les commandes de l'AWS CLI. L'identifiant d'instance de base de données doit être unique pour ce client dans une région AWS.

Il est utilisé comme partie intégrante du nom d'hôte DNS alloué à votre instance par RDS. Par exemple, si vous spécifiez `db1` comme identifiant d'instance de base de données, RDS attribue automatiquement un point de terminaison DNS pour votre instance, tel que `db1.123456789012.us-east-1.rds.amazonaws.com`, où `123456789012` représente l'identifiant fixe d'une région spécifique pour votre compte.

Chaque instance de base de données prend en charge un moteur de base de données. Amazon RDS prend actuellement en charge les moteurs de base de données MySQL, MariaDB, PostgreSQL, Oracle, Microsoft SQL Server et les moteurs de base de données Amazon Aurora.

Lorsque vous créez une instance de base de données, certains moteurs de base de données nécessitent qu'un nom de base de données soit spécifié. Une instance de base de données peut héberger plusieurs bases de données ou une seule base de données Oracle avec plusieurs schémas. La valeur du nom de base de données dépend du moteur de base de données :

- Pour les moteurs de base de données MySQL et MariaDB, le nom de base de données est le nom d'une base de données hébergée dans votre instance de base de données. Les bases de données hébergées par la même instance de base de données doivent avoir un nom unique au sein de cette instance.
- Pour le moteur de base de données Oracle, le nom de base de données est utilisé pour définir la valeur d'ORACLE_SID, qui doit être fournie lors de la connexion à l'instance Oracle RDS.
- Pour le moteur de base de données Microsoft SQL Server, le nom de base de données n'est pas un paramètre pris en charge.
- Pour le moteur de base de données PostgreSQL, le nom de base de données est le nom d'une base de données hébergée dans votre instance de base de données. Un nom de base de données n'est pas

obligatoire lors de la création d'une instance de base de données. Les bases de données hébergées par la même instance de base de données doivent avoir un nom unique au sein de cette instance.

Amazon RDS crée un compte utilisateur principal pour votre instance de base de données comme partie intégrante du processus de création. Cet utilisateur principal dispose des autorisations pour créer des bases de données et exécuter des opérations de création, suppression, sélection, mise à jour et insertion sur les tables créées par l'utilisateur principal. Vous devez définir le mot de passe de l'utilisateur principal quand vous créez une instance de base de données, mais vous pouvez le modifier à tout moment à l'aide des outils de ligne de commande Amazon AWS, des opérations d'API Amazon RDS ou de l'AWS Management Console. Vous pouvez aussi modifier le mot de passe de l'utilisateur principal et gérer les utilisateurs à l'aide des commandes SQL standard.

> Note
>
> Ce guide traite des moteurs de base de données Amazon RDS non-Aurora. Pour plus d'informations sur l'utilisation d'Amazon Aurora, consultez le Guide de l'utilisateur Amazon Aurora.

Classes d'instances de base de données

La classe d'instance de base de données détermine la capacité de calcul et de mémoire d'une instance de base de données Amazon RDS. La classe d'instance de bases de données dont vous avez besoin varie selon vos exigences en mémoire et en puissance de traitement.

Pour de plus amples informations sur la tarification des classes d'instance, veuillez consulter Tarification Amazon RDS.

Rubriques

- Types de classes d'instance de base de données (p. 6)
- Moteurs de base de données pris en charge pour les classes d'instance de base de données (p. 7)
- Modification d'une classe d'instance de base de données (p. 13)
- Configuration du processeur pour une classe d'instance de base de données (p. 13)
- Spécifications matérielles pour les classes d'instance de base de données (p. 25)

Types de classes d'instance de base de données

Amazon RDS prend en charge trois types de classes d'instances : standard, mémoire optimisée et à capacité extensible. Pour de plus amples informations sur les types d'instances Amazon EC2, veuillez consulter Type d'instance dans la documentation Amazon EC2.

Les classes d'instance de bases de données standard disponibles sont :

- db.m6g – Classes d'instance générale de nouvelle génération optimisées par les processeurs AWS Graviton2. Celles-ci fournissent des capacités de calcul, de mémoire et de réseau équilibrées pour une large gamme de charges de travail à usage général.
- db.m5 – Classes d'instances à usage général de dernière génération qui fournissent un équilibre entre ressources de calcul, de mémoire et de réseau et qui constituent le choix idéal pour de nombreuses applications. Les classes d'instances db.m5 offrent une plus grande capacité de calcul que les précédentes classes d'instance db.m4. Elles sont alimentées par le système AWS Nitro, qui allie un matériel dédié et un hyperviseur léger.
- db.m4 – Classes d'instances à usage général de génération actuelle qui offrent une plus grande capacité de calcul que les précédentes classes d'instance db.m3.
- db.m4 – Classes d'instances à usage général de génération précédente qui offrent une plus grande capacité de calcul que les précédentes classes d'instance db.m1.

- db.m1 – Classes d'instances à usage général de génération précédente.

Les classes d'instance de bases de données à mémoire optimisée disponibles sont :

- db.z1d – Classes d'instances de dernière génération optimisées pour les applications à usage intensif de la mémoire. Elles offrent une forte capacité de calcul et une forte empreinte mémoire. Les instances z1d haute fréquence présentent une fréquence de tous les cœurs maintenue à 4,0 GHz au maximum.
- db.x1e – Classes d'instances de dernière génération optimisées pour les applications exigeantes en mémoire. Elles offrent l'un des prix les moins élevés par gibioctet (GiO) de RAM parmi les classes d'instances de bases de données et jusqu'à 3 904 Gio de mémoire d'instance basée sur DRAM. Les classes d'instances db.x1e sont disponibles uniquement dans les régions suivantes : USA Est (Virginie du Nord), USA Ouest (Oregon), Europe (Irlande), Asie-Pacifique (Tokyo) et Asie-Pacifique (Sydney).
- db.x1 – Classes d'instances de la génération actuelle optimisées pour les applications exigeantes en mémoire. Elles offrent l'un des prix les moins élevés par Gio de RAM parmi les classes d'instances de bases de données et jusqu'à 1 952 Gio de mémoire d'instance basée sur DRAM.
- db.r6g – Classes d'instance de nouvelle génération optimisées par les processeurs AWS Graviton2. Elles sont idéales pour exécuter des charges de travail exigeantes en mémoire dans des bases de données open source telles que MySQL et PostgreSQL.
- db.r5 – Classes d'instances de dernière génération optimisées pour les applications à usage intensif de la mémoire. Elles offrent une amélioration de la mise en réseau et des performances Amazon Elastic Block Store (Amazon EBS). Elles sont alimentées par le système AWS Nitro, qui allie un matériel dédié et un hyperviseur léger.
- db.r4 – Classes d'instances de la génération actuelle optimisées pour les applications exigeantes en mémoire. Elles offrent une amélioration de la mise en réseau et des performances Amazon EBS.
- db.r3 – Classes d'instances de génération précédente qui fournissent une optimisation de la mémoire. Les classes d'instance db.r3 ne sont pas disponibles dans la région Europe (Paris) et la région Amérique du Sud (São Paulo).
- db.m2 – Classes d'instances à mémoire optimisée de la génération précédente.

Les classes d'instance de bases de données à capacité extensible disponibles sont :

- db.t3 – Classes d'instances de dernière génération qui fournissent un niveau de performance de base, avec la possibilité de transmission étendue jusqu'à une utilisation intégrale de l'UC. Ces classes d'instances offrent une plus grande capacité de calcul que les précédentes classes d'instance db.t2. Elles sont alimentées par le système AWS Nitro, qui allie un matériel dédié et un hyperviseur léger.
- db.t2 – Classes d'instances de la génération actuelle qui fournissent un niveau de performance de base, avec la possibilité de transmission étendue jusqu'à une utilisation intégrale de l'UC.

> **Note**
>
> Les classes d'instance de base de données qui utilisent le système AWS Nitro (db.m5, db.r5, db.t3) ont une limite de charge de travail combinée de lecture et d'écriture.

Pour de plus amples informations sur les spécifications matérielles de classe d'instance de base de données, veuillez consulter Spécifications matérielles pour les classes d'instance de base de données (p. 25).

Moteurs de base de données pris en charge pour les classes d'instance de base de données

Vous trouverez ci-après des considérations relatives au moteur de base de données pour les classes d'instances de base de données :

MariaDB

Les classes d'instance Graviton2 db.m6g et db.r6g sont prises en charge pour MariaDB versions 10.4.13 et ultérieures.

Microsoft SQL Server

La prise en charge des classes d'instance varie selon la version et l'édition de SQL Server. Pour une prise en charge des classes d'instances par version et édition, consultez Prise en charge de la classe d'instance de base de données pour Microsoft SQL Server (p. 597).

MySQL

Les classes d'instance en version préliminaire Graviton2 db.m6g et db.r6g sont prises en charge pour Amazon RDS MySQL versions 8.0.17 et ultérieures.

Oracle

La prise en charge des classes d'instance varie selon la version et l'édition d'Oracle. Pour une prise en charge des classes d'instances par version et édition, consultez Prise en charge des classes d'instance de base de données pour Oracle (p. 933).

PostgreSQL

Les classes d'instance Graviton2 db.m6g et db.r6g sont prises en charge pour Amazon RDS PostgreSQL versions 12.3 et ultérieures.

Le tableau suivant vous présente des détails sur les classes d'instances de base de données Amazon RDS prises en charge pour chaque moteur de base de données Amazon RDS.

Classe d'instance	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.m6g – Classes d'instance standard de nouvelle génération					
db.m6g.16xlarge	MariaDB versions 10.4.13 et ultérieures	Non	MySQL versions 8.0.17 et ultérieures	Non	PostgreSQL versions 12.3 et ultérieures
db.m6g.12xlarge	MariaDB versions 10.4.13 et ultérieures	Non	MySQL versions 8.0.17 et ultérieures	Non	PostgreSQL versions 12.3 et ultérieures
db.m6g.8xlarge	MariaDB versions 10.4.13 et ultérieures	Non	MySQL versions 8.0.17 et ultérieures	Non	PostgreSQL versions 12.3 et ultérieures
db.m6g.4xlarge	MariaDB versions 10.4.13 et ultérieures	Non	MySQL versions 8.0.17 et ultérieures	Non	PostgreSQL versions 12.3 et ultérieures
db.m6g.2xlarge	MariaDB versions 10.4.13 et ultérieures	Non	MySQL versions 8.0.17 et ultérieures	Non	PostgreSQL versions 12.3 et ultérieures
db.m6g.xlarge	MariaDB versions 10.4.13 et ultérieures	Non	MySQL versions 8.0.17 et ultérieures	Non	PostgreSQL versions 12.3 et ultérieures
db.m6g.large	MariaDB versions 10.4.13 et ultérieures	Non	MySQL versions 8.0.17 et ultérieures	Non	PostgreSQL versions 12.3 et ultérieures

Classe d'instance	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.m5 – Classes d'instance standard de dernière génération					
db.m5.24xlarge	Oui	Oui	Oui	Oui	Oui
db.m5.16xlarge	Oui	Oui	Oui	Oui	PostgreSQL 11.6 et versions suivantes, 10.11 et versions suivantes, 9.6.16 et versions suivantes, 9.5.20 et versions suivantes
db.m5.12xlarge	Oui	Oui	Oui	Oui	Oui
db.m5.8xlarge	Oui	Oui	Oui	Oui	PostgreSQL 11.6 et versions suivantes, 10.11 et versions suivantes, 9.6.16 et versions suivantes, 9.5.20 et versions suivantes
db.m5.4xlarge	Oui	Oui	Oui	Oui	Oui
db.m5.2xlarge	Oui	Oui	Oui	Oui	Oui
db.m5.xlarge	Oui	Oui	Oui	Oui	Oui
db.m5.large	Oui	Oui	Oui	Oui	Oui
db.m4 – Classes d'instance standard de génération actuelle					
db.m4.16xlarge	Oui	Oui	MySQL 8.0, 5.7, 5.6	Oui	Oui
db.m4.10xlarge	Oui	Oui	Oui	Oui	Oui
db.m4.4xlarge	Oui	Oui	Oui	Oui	Oui
db.m4.2xlarge	Oui	Oui	Oui	Oui	Oui
db.m4.xlarge	Oui	Oui	Oui	Oui	Oui
db.m4.large	Oui	Oui	Oui	Oui	Oui

Classe d'instance	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.m3 – Classes d'instance standard de génération précédente					
db.m3.2xlarge	Non	Oui	Oui	Obsolète	Oui
db.m3.xlarge	Non	Oui	Oui	Obsolète	Oui
db.m3.large	Non	Oui	Oui	Obsolète	Oui
db.m3.medium	Non	Oui	Oui	Obsolète	Oui
db.m1 – Classes d'instance standard de génération précédente					
db.m1.xlarge	Non	Oui	Obsolète	Obsolète	Obsolète
db.m1.large	Non	Oui	Obsolète	Obsolète	Obsolète
db.m1.medium	Non	Oui	Obsolète	Obsolète	Obsolète
db.m1.small	Non	Oui	Obsolète	Obsolète	Obsolète
db.z1d – Classes d'instance à mémoire optimisée de dernière génération					
db.z1d.12xlarge	Non	Oui	Non	Oui	Non
db.z1d.6xlarge	Non	Oui	Non	Oui	Non
db.z1d.3xlarge	Non	Oui	Non	Oui	Non
db.z1d.2xlarge	Non	Oui	Non	Oui	Non
db.z1d.xlarge	Non	Oui	Non	Oui	Non
db.z1d.large	Non	Oui	Non	Oui	Non
db.x1e – Classes d'instance à mémoire optimisée de dernière génération					
db.x1e.32xlarge	Non	Oui	Non	Oui	Non
db.x1e.16xlarge	Non	Oui	Non	Oui	Non
db.x1e.8xlarge	Non	Oui	Non	Oui	Non
db.x1e.4xlarge	Non	Oui	Non	Oui	Non
db.x1e.2xlarge	Non	Oui	Non	Oui	Non
db.x1e.xlarge	Non	Oui	Non	Oui	Non
db.x1 – Classes d'instance à mémoire optimisée de génération actuelle					
db.x1.32xlarge	Non	Oui	Non	Oui	Non
db.x1.16xlarge	Non	Oui	Non	Oui	Non
db.r6g – Classes d'instance à mémoire optimisée de dernière génération					
db.r6g.16xlarge	MariaDB versions 10.4.13 et ultérieures	Non	MySQL versions 8.0.17 et ultérieures	Non	PostgreSQL versions 12.3 et ultérieures

Classe d'instance	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r6g.12xlarge	MariaDB versions 10.4.13 et ultérieures	Non	MySQL versions 8.0.17 et ultérieures	Non	PostgreSQL versions 12.3 et ultérieures
db.r6g.4xlarge	MariaDB versions 10.4.13 et ultérieures	Non	MySQL versions 8.0.17 et ultérieures	Non	PostgreSQL versions 12.3 et ultérieures
db.r6g.2xlarge	MariaDB versions 10.4.13 et ultérieures	Non	MySQL versions 8.0.17 et ultérieures	Non	PostgreSQL versions 12.3 et ultérieures
db.r6g.xlarge	MariaDB versions 10.4.13 et ultérieures	Non	MySQL versions 8.0.17 et ultérieures	Non	PostgreSQL versions 12.3 et ultérieures
db.r6g.large	MariaDB versions 10.4.13 et ultérieures	Non	MySQL versions 8.0.17 et ultérieures	Non	PostgreSQL versions 12.3 et ultérieures
db.r5 – Classes d'instance à mémoire optimisée de dernière génération					
db.r5.24xlarge	Oui	Oui	Oui	Oui	Oui
db.r5.16xlarge	Oui	Oui	Oui	Oui	PostgreSQL 11.6 et versions suivantes, 10.11 et versions suivantes, 9.6.16 et versions suivantes, 9.5.20 et versions suivantes
db.r5.12xlarge	Oui	Oui	Oui	Oui	Oui
db.r5.8xlarge	Oui	Oui	Oui	Oui	PostgreSQL 11.6 et versions suivantes, 10.11 et versions suivantes, 9.6.16 et versions suivantes, 9.5.20 et versions suivantes
db.r5.4xlarge	Oui	Oui	Oui	Oui	Oui

Classe d'instance	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r5.2xlarge	Oui	Oui	Oui	Oui	Oui
db.r5.xlarge	Oui	Oui	Oui	Oui	Oui
db.r5.large	Oui	Oui	Oui	Oui	Oui
db.r4 – Classes d'instance à mémoire optimisée de génération actuelle					
db.r4.16xlarge	Oui	Oui	MySQL 8.0, 5.7, 5.6	Oui	Oui
db.r4.8xlarge	Oui	Oui	MySQL 8.0, 5.7, 5.6	Oui	Oui
db.r4.4xlarge	Oui	Oui	MySQL 8.0, 5.7, 5.6	Oui	Oui
db.r4.2xlarge	Oui	Oui	MySQL 8.0, 5.7, 5.6	Oui	Oui
db.r4.xlarge	Oui	Oui	MySQL 8.0, 5.7, 5.6	Oui	Oui
db.r4.large	Oui	Oui	MySQL 8.0, 5.7, 5.6	Oui	Oui
db.r3 – Classes d'instance à mémoire optimisée de génération précédente					
db.r3.8xlarge	Oui	Oui	Oui	Obsolète	Oui
db.r3.4xlarge	Oui	Oui	Oui	Obsolète	Oui
db.r3.2xlarge	Oui	Oui	Oui	Obsolète	Oui
db.r3.xlarge	Oui	Oui	Oui	Obsolète	Oui
db.r3.large	Oui	Oui	Oui	Obsolète	Oui
db.m2 – Classes d'instance à mémoire optimisée de génération précédente					
db.m2.4xlarge	Non	Oui	Obsolète	Obsolète	Obsolète
db.m2.2xlarge	Non	Oui	Obsolète	Obsolète	Obsolète
db.m2.xlarge	Non	Oui	Obsolète	Obsolète	Obsolète
db.t3 – Classes d'instance à capacité extensible de génération actuelle					
db.t3.2xlarge	Oui	Oui	Oui	Oui	Oui
db.t3.xlarge	Oui	Oui	Oui	Oui	Oui
db.t3.large	Oui	Oui	Oui	Oui	Oui
db.t3.medium	Oui	Oui	Oui	Oui	Oui
db.t3.small	Oui	Oui	Oui	Oui	Oui
db.t3.micro	Oui	Non	Oui	Oui	Oui

Classe d'instance	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.t2 – Classes d'instance à capacité extensible de génération actuelle					
db.t2.2xlarge	Oui	Non	MySQL 8.0, 5.7, 5.6	Obsolète	PostgreSQL 9.6, 9.5
db.t2.xlarge	Oui	Non	MySQL 8.0, 5.7, 5.6	Obsolète	PostgreSQL 9.6, 9.5
db.t2.large	Oui	Oui	Oui	Obsolète	Oui
db.t2.medium	Oui	Oui	Oui	Obsolète	Oui
db.t2.small	Oui	Oui	Oui	Obsolète	Oui
db.t2.micro	Oui	Oui	Oui	Obsolète	Oui

Modification d'une classe d'instance de base de données

Vous pouvez modifier la capacité de calcul et de mémoire d'une instance de base de données en modifiant sa classe d'instance de base de données. Pour modifier une classe d'instance de base de données, modifiez l'instance de base de données en suivant les instructions fournies dans Modification d'une instance de base de données Amazon RDS (p. 243).

Certaines classes d'instances nécessitent que l'instance de base de données soit dans un VPC. Si votre instance de base de données actuelle n'est pas dans un VPC et que vous souhaitez utiliser une classe d'instance nécessitant un VPC, vous devez d'abord placer votre instance de base de données dans un VPC. Pour plus d'informations, consultez Déplacement vers un VPC d'une instance de base de données n'appartenant pas à un VPC (p. 1627).

Configuration du processeur pour une classe d'instance de base de données

Les classes d'instances de base de données Amazon RDS prennent en charge la technologie hyper-threading d'Intel, qui permet l'exécution simultanée de plusieurs threads sur un seul cœur d'UC Intel Xeon. Chaque thread est représenté comme UC virtuelle (vCPU) sur l'instance de base de données. Par défaut, une instance de base de données possède un certain nombre de cœurs d'UC, qui varie en fonction du type d'instance de base de données. Par exemple, un type d'instance de base de données db.m4.xlarge a deux cœurs d'UC et deux threads par cœur par défaut (quatre vCPU au total).

> Note
>
> Chaque vCPU est un hyperthread d'un cœur d'UC Intel Xeon.

Rubriques

- Présentation de la configuration du processeur (p. 14)
- Cœurs d'UC et threads par cœur d'UC par classe d'instance de base de données (p. 14)
- Définition des cœurs d'UC et des threads par cœur d'UC pour une classe d'instance de base de données (p. 17)

Présentation de la configuration du processeur

Dans la plupart des cas, vous pouvez trouver une classe d'instance de base de données qui possède une combinaison de mémoire et d'un certain nombre de vCPU pour convenir à vos charges de travail. Cependant, vous pouvez également spécifier les fonctionnalités de processeur afin d'optimiser votre instance de base de données pour des besoins métier ou des charges de travail spécifiques :

- Nombre de cœurs d'UC – Vous pouvez personnaliser le nombre de cœurs d'UC pour l'instance de base de données. Vous pourriez agir ainsi pour optimiser potentiellement les coûts de licence de vos logiciels avec une instance de base de données ayant une quantité suffisante de RAM pour les charges de travail exigeantes en mémoire, mais moins de cœurs d'UC.
- Threads par cœur – Vous pouvez désactiver la technologie hyper-threading d'Intel en spécifiant une seul thread par cœur d'UC. Vous pourriez agir ainsi pour certaines charges de travail, telles que les charges de travail de calcul haute performance (HPC).

Vous pouvez contrôler le nombre de cœurs d'UC et de threads pour chaque cœur séparément. Vous pouvez définir l'un ou les deux dans une demande. Une fois qu'un paramètre est associé à une instance de base de données, il persiste jusqu'à ce que vous le changiez.

Les paramètres du processeur pour une instance de base de données sont associés aux instantanés de l'instance de base de données. Lorsqu'un instantané est restauré, son instance de base de données restaurée utilise les paramètres des fonctionnalités du processeur qui ont servi lors de la prise de l'instantané.

Si vous modifiez la classe d'une instance de base de données avec des paramètres de processeur autres que ceux définis par défaut, spécifiez les paramètres de processeur par défaut ou spécifiez explicitement les paramètres de processeur par défaut lors de la modification de l'instance de base de données. Cela vous permet d'avoir connaissance des coûts de licence tiers susceptibles d'être encourus lorsque vous modifiez l'instance de base de données.

Il n'y a pas de frais supplémentaires ou réduits pour la spécification des fonctionnalités du processeur sur une instance de base de données Amazon RDS. Le même montant vous est facturé pour les instances de base de données qui sont lancées avec les configurations de l'UC par défaut.

Cœurs d'UC et threads par cœur d'UC par classe d'instance de base de données

Le tableau suivant présente les classes d'instances de base de données qui prennent en charge la définition d'un certain nombre de cœurs d'UC et de threads d'UC par cœur. Il contient également la valeur par défaut et les valeurs valides pour le nombre de cœurs d'UC et de threads d'UC par cœur pour chaque classe d'instance de base de données.

Classe d'instance de base de données	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Nombre valide de cœurs d'UC	Nombre valide de threads par cœur
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

Classe d'instance de base de données	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Nombre valide de cœurs d'UC	Nombre valide de threads par cœur
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, 20, 22, 24, 26, 28, 30, 32	1, 2
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.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.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.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.r5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Classe d'instance de base de données	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Nombre valide de cœurs d'UC	Nombre valide de threads par cœur
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.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.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.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

Classe d'instance de base de données	vCPU par défaut	Cœurs d'UC par défaut	Threads par défaut par cœur	Nombre valide de cœurs d'UC	Nombre valide de threads par cœur
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

Actuellement, vous pouvez configurer le nombre de cœurs de processeur et de threads par cœur uniquement lorsque les conditions suivantes sont remplies :

- Vous configurez une instance de base de données Oracle. Pour obtenir des informations sur les classes d'instances de base de données prises en charge par les différentes éditions d'Oracle Database, veuillez consulter Prise en charge des classes d'instance de base de données pour Oracle (p. 933)
- Votre instance utilise l'option de licence Apportez votre propre licence (BYOL). Pour plus d'informations sur les options de licence Oracle, consultez Options de licence Oracle (p. 930).

> **Note**
>
> Vous pouvez utiliser AWS CloudTrail pour surveiller et contrôler les modifications apportées à la configuration du processus des instances de base de données Amazon RDS for Oracle. Pour plus d'informations sur l'utilisation de CloudTrail, consultez Utilisation de AWS CloudTrail et Amazon RDS (p. 526).

Définition des cœurs d'UC et des threads par cœur d'UC pour une classe d'instance de base de données

Vous pouvez configurer le nombre de cœurs de l'UC et de threads par cœur pour la classe de l'instance de base de données lorsque vous exécutez les opérations suivantes :

- Création d'une instance de base de données Amazon RDS (p. 146)
- Modification d'une instance de base de données Amazon RDS (p. 243)
- Restauration à partir d'un instantané de base de données (p. 329)

- Restauration d'une instance de base de données à une date spécifiée (p. 365)

> **Note**
>
> Lorsque vous modifiez une instance de base de données pour configurer le nombre de cœurs de l'UC ou de threads par cœur, il se produit une courte interruption de l'instance de base de données.

Vous pouvez définir les cœurs de l'UC et les threads par cœur d'UC pour une classe d'instance de base de données à l'aide de la AWS Management Console, de l'AWS CLI ou de l'API RDS.

Console

Lorsque vous créez, modifiez ou restaurez une instance de base de données, vous définissez la classe d'instance de base de données dans l'AWS Management Console. La section Spécifications de l'instance comporte les options du processeur. L'image suivante montre les options relatives aux fonctionnalités du processeur.

Définissez les options suivantes sur les valeurs appropriées pour votre classe d'instance de base de données sous Fonctions du processeur :

- Nombre de cœurs – Définissez le nombre de cœurs d'UC à l'aide de cette option. La valeur doit être égale ou inférieure au nombre maximum de cœurs d'UC pour la classe d'instance de base de données.
- Threads par cœur – Spécifiez 2 pour activer plusieurs threads par cœur ou spécifiez 1 pour désactiver plusieurs threads par cœur.

Lorsque vous modifiez ou restaurez une instance de base de données, vous pouvez également définir les cœurs d'UC et les threads par cœur d'UC sur les valeurs par défaut pour la classe d'instance.

Lorsque vous affichez les détails d'une instance de base de données dans la console, vous pouvez afficher les informations de processeur pour sa classe d'instance de base de données dans l'onglet Configuration. L'image suivante montre une classe d'instance de base de données avec un cœur d'UC et plusieurs threads par cœur activés.

En ce qui concerne les instances de base de données Oracle, les informations du processeur apparaissent uniquement pour les instances de base de données Réutilisez vos licences (BYOL).

AWS CLI

Vous pouvez définir les fonctions de processeur pour une instance de base de données lorsque vous exécutez l'une des commandes d'AWS CLI suivantes :

- create-db-instance
- modify-db-instance
- restore-db-instance-from-db-snapshot
- restore-db-instance-from-s3
- restore-db-instance-to-point-in-time

Pour configurer le processeur d'une classe d'instance de base de données pour une instance de base de données en utilisant l'AWS CLI, incluez l'option `--processor-features` dans la commande. Spécifiez

le nombre de cœurs d'UC avec le nom de fonction `coreCount`, et spécifiez si plusieurs threads par cœur sont activés avec le nom de fonction `threadsPerCore`.

L'option a la syntaxe suivante.

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

Vous trouverez ci-après des exemples de configuration du processeur :

Exemples

- Définition du nombre de cœurs d'UC pour une instance de base de données (p. 21)
- Définition du nombre de cœurs d'UC et désactivation de plusieurs threads pour une instance de base de données (p. 21)
- Affichage des valeurs de processeur valides pour une classe d'instance de base de données (p. 22)
- Réinitialiser les paramètres de processeur par défaut pour une instance de base de données (p. 23)
- Rétablissement du nombre de cœurs d'UC par défaut pour une instance de base de données (p. 23)
- Rétablissement du nombre de threads par cœur par défaut pour une instance de base de données (p. 24)

Définition du nombre de cœurs d'UC pour une instance de base de données

Example

L'exemple suivant modifie `mydbinstance` en définissant le nombre de cœurs d'UC sur 4. Les modifications sont appliquées immédiatement en utilisant `--apply-immediately`. Si vous souhaitez appliquer les modifications pendant la fenêtre de maintenance planifiée, omettez l'option `--apply-immediately`.

Pour Linux, macOS ou Unix :

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

Pour Windows :

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

Définition du nombre de cœurs d'UC et désactivation de plusieurs threads pour une instance de base de données

Example

L'exemple suivant modifie `mydbinstance` en définissant le nombre de cœurs d'UC sur `4` et en désactivant plusieurs threads par cœur. Les modifications sont appliquées immédiatement en utilisant `--apply-immediately`. Si vous souhaitez appliquer les modifications pendant la fenêtre de maintenance planifiée, omettez l'option `--apply-immediately`.

Pour Linux, macOS ou Unix :

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

```
    --apply-immediately
```

Pour Windows :

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

Affichage des valeurs de processeur valides pour une classe d'instance de base de données

Example

Vous pouvez afficher les valeurs de processeur valides pour une classe d'instance de base de données spécifique en exécutant la commande describe-orderable-db-instance-options et en spécifiant la classe d'instance pour l'option `--db-instance-class`. Par exemple, la sortie de la commande suivante montre les options de processeur pour la classe d'instance db.r3.large.

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

Voici un exemple de sortie pour la commande au format JSON.

```
    {
                "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
    }
```

De plus, vous pouvez exécuter les commandes suivantes pour les informations de processeur de la classe d'instance de base de données :

- describe-db-instances – Affiche les informations de processeur pour l'instance de base de données spécifiée.
- describe-db-snapshots – Affiche les informations de processeur pour l'instantané de base de données spécifié.
- describe-valid-db-instance-modifications – Affiche les modifications valides du processeur pour l'instance de base de données spécifiée.

Dans la sortie des commandes précédentes, les fonctions du processeur n'ont pas la valeur null seulement si les conditions suivantes sont remplies :

- Vous utilisez une instance de base de données Oracle.
- Votre instance de base de données Oracle prend en charge des valeurs de processeur changeantes.
- Les paramètres actuels de cœurs de processeur et de threads sont définis sur des valeurs personnalisées.

Si les conditions précédentes ne sont pas remplies, vous pouvez obtenir le type d'instance en utilisant describe-db-instances. Vous pouvez obtenir les informations de processeur pour ce type d'instance en exécutant l'opération EC2 describe-instance-types.

Réinitialiser les paramètres de processeur par défaut pour une instance de base de données

Example

L'exemple suivant modifie `mydbinstance` en rétablissant les valeurs de processeur par défaut pour la classe d'instance de base de données. Les modifications sont appliquées immédiatement en utilisant `--apply-immediately`. Si vous souhaitez appliquer les modifications pendant la fenêtre de maintenance planifiée, omettez l'option `--apply-immediately`.

Pour Linux, macOS ou Unix :

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

Pour Windows :

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

Rétablissement du nombre de cœurs d'UC par défaut pour une instance de base de données

Example

L'exemple suivant modifie `mydbinstance` en rétablissant le nombre de cœurs d'UC par défaut pour la classe d'instance de base de données. Le paramètre des threads par cœur n'est pas modifié. Les modifications sont appliquées immédiatement en utilisant `--apply-immediately`. Si vous souhaitez appliquer les modifications pendant la fenêtre de maintenance planifiée, omettez l'option `--apply-immediately`.

Pour Linux, macOS ou Unix :

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

Pour Windows :

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

Rétablissement du nombre de threads par cœur par défaut pour une instance de base de données

Example

L'exemple suivant modifie `mydbinstance` en rétablissant le nombre de threads par cœur par défaut pour la classe d'instance de base de données. Le nombre de cœurs d'UC n'est pas modifié. Les modifications sont appliquées immédiatement en utilisant `--apply-immediately`. Si vous souhaitez appliquer les modifications pendant la fenêtre de maintenance planifiée, omettez l'option `--apply-immediately`.

Pour Linux, macOS ou Unix :

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

Pour Windows :

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

API RDS

Vous pouvez définir les fonctions de processeur pour une instance de base de données lorsque vous appelez l'une des opérations d'API Amazon RDS suivantes :

- CreateDBInstance
- ModifyDBInstance
- RestoreDBInstanceFromDBSnapshot
- RestoreDBInstanceFromS3
- RestoreDBInstanceToPointInTime

Pour configurer les fonctions de processeur d'une classe d'instance de base de données pour une instance de base de données en utilisant l'API Amazon RDS, incluez le paramètre `ProcessFeatures` dans l'appel.

Le paramètre a la syntaxe suivante.

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

Spécifiez le nombre de cœurs d'UC avec le nom de fonction `coreCount`, et spécifiez si plusieurs threads par cœur sont activés avec le nom de fonction `threadsPerCore`.

Vous pouvez afficher les valeurs de processeur valides pour une classe d'instance de base de données spécifique en exécutant l'opération DescribeOrderableDBInstanceOptions et en spécifiant la classe

d'instance pour le paramètre `DBInstanceClass`. Vous pouvez également utiliser les opérations suivantes :

- DescribeDBInstances – Affiche les informations de processeur pour l'instance de base de données spécifiée.
- DescribeDBSnapshots – Affiche les informations de processeur pour l'instantané de base de données spécifié.
- DescribeValidDBInstanceModifications – Affiche les modifications valides du processeur pour l'instance de base de données spécifiée.

Dans la sortie des opérations précédentes, les fonctions du processeur n'ont pas la valeur null seulement si les conditions suivantes sont remplies :

- Vous utilisez une instance de base de données Oracle.
- Votre instance de base de données Oracle prend en charge des valeurs de processeur changeantes.
- Les paramètres actuels de cœurs de processeur et de threads sont définis sur des valeurs personnalisées.

Si les conditions précédentes ne sont pas remplies, vous pouvez obtenir le type d'instance en utilisant DescribeDBInstances. Vous pouvez obtenir les informations de processeur pour ce type d'instance en exécutant l'opération EC2 DescribeInstanceTypes.

Spécifications matérielles pour les classes d'instance de base de données

La terminologie suivante est utilisée pour décrire les spécifications matérielles des classes d'instances de base de données :

vCPU

Nombre d'unités de traitement central (CPU) virtuelles. Un processeur virtuel est une unité de capacité que vous pouvez utiliser pour comparer les classes d'instances de base de données. Au lieu d'acheter ou de louer un processeur particulier pour l'utiliser pendant plusieurs mois ou plusieurs années, vous louez la capacité à l'heure. Notre but est de fournir une quantité constante et spécifique de capacité CPU, dans les limites du matériel sous-jacent.

ECU

Mesure relative de la puissance de traitement des nombres entiers d'une instance Amazon EC2. Pour aider les développeurs à comparer les capacités d'UC entre les différentes classes d'instance, nous avons défini une unité de calcul Amazon EC2. La quantité de CPU allouée à une instance particulière est exprimée par ces unités de calcul EC2. Une unité de calcul EC2 fournit actuellement une capacité d'UC équivalente à un processeur 2007 Opteron ou 2007 Xeon 1,0 – 1,2 GHz.

Mémoire (Gio)

Mémoire RAM, en gibioctets (Gio), allouée à l'instance de base de données. Il existe souvent un ratio cohérent entre la mémoire et le processeur virtuel. Citons, par exemple, la classe d'instance db.r4, qui a un ration mémoire/processeur virtuel similaire à celui de la classe db.r5. Toutefois, dans la plupart des cas d'utilisation, la classe d'instance db.r5 fournit de meilleures performances, plus cohérentes, que la classe d'instance db.r4.

VPC uniquement

La classe d'instance est prise en charge uniquement pour les instances de base de données se trouvant dans un VPC sur le service Amazon VPC. Dans certains cas, vous pouvez souhaiter utiliser une classe d'instance nécessitant un VPC alors que votre instance de base de données actuelle ne se

trouve pas dans un VPC. Dans ces cas, commencez par déplacer votre instance de base de données dans un VPC. Pour plus d'informations, consultez Déplacement vers un VPC d'une instance de base de données n'appartenant pas à un VPC (p. 1627).

Optimisé pour EBS

Une instance de base de données a recours à une pile de configuration optimisée et fournit une capacité supplémentaire dédiée pour les E/S. Cette optimisation offre les meilleures performances en réduisant les conflits entre les I/O et le trafic restant de votre instance. Pour de plus amples informations sur les types d'instances optimisés pour Amazon EBS, veuillez consulter Instances optimisées Amazon EBS– dans le Amazon EC2 Guide de l'utilisateur pour les instances Linux.

Taille max. Largeur de bande (Mbit/s)

Bande passante maximale en mégabits par seconde. Divisez cette valeur par 8 pour calculer le débit attendu en mégaoctets par seconde.

Important

Les volumes à usage général SSD (gp2) pour les instances de base de données Amazon RDS possèdent une limite de débit de 250 Mio/s dans la plupart des cas. Toutefois, cette limite peut varier en fonction de la taille du volume. Pour de plus amples informations, veuillez consulter Types de volumes Amazon EBS dans le Amazon EC2 Guide de l'utilisateur pour les instances Linux. Pour plus d'informations sur l'estimation de la bande passante pour le stockage gp2, consultez Stockage SSD à usage général (p. 31).

Performances réseau

Vitesse du réseau par rapport à d'autres classes d'instance de base de données.

Le tableau suivant vous présente des détails sur les classes d'instances de base de données Amazon RDS .

Pour de plus amples informations sur le moteur de base de données Amazon RDS pris en charge pour chaque classe de base de données, veuillez consulter Moteurs de base de données pris en charge pour les classes d'instance de base de données (p. 7).

Classe d'instance	vCPU	ECU	Mémoire (Gio)	VPC uniquemer	Optimisé EBS	Bande passante max (Mo/s)**	Performances réseau
db.m6g – Classes d'instance standard de nouvelle génération							
db.m6g.16xlarge	64	–	256	Oui	Oui	19 000	25 Gb/s
db.m6g.12xlarge	48	–	192	Oui	Oui	13 500	20 Gb/s
db.m6g.8xlarge	32	–	128	Oui	Oui	9 500	12 Gb/s
db.m6g.4xlarge	16	–	64	Oui	Oui	6 800	Jusqu'à 10 Gbit/s
db.m6g.2xlarge*	8	–	32	Oui	Oui	Jusqu'à 4 750	Jusqu'à 10 Gbit/s
db.m6g.xlarge*	4	–	16	Oui	Oui	Jusqu'à 4 750	Jusqu'à 10 Gbit/s
db.m6g.large*	2	–	8	Oui	Oui	Jusqu'à 4 750	Jusqu'à 10 Gbit/s
db.m5 – Classes d'instance standard de dernière génération							

Classe d'instance	vCPU	ECU	Mémoire (Gio)	VPC uniquemer	Optimisé EBS	Bande passante max (Mo/s)**	Performances réseau
db.m5.24xlarge	96	345	384	Oui	Oui	19 000	25 Gb/s
db.m5.16xlarge	64	262	256	Oui	Oui	13 600	20 Gb/s
db.m5.12xlarge	48	173	192	Oui	Oui	9 500	10 Gb/s
db.m5.8xlarge	32	131	128	Oui	Oui	6 800	10 Gb/s
db.m5.4xlarge	16	61	64	Oui	Oui	4 750	Jusqu'à 10 Gbit/s
db.m5.2xlarge*	8	31	32	Oui	Oui	Jusqu'à 4 750	Jusqu'à 10 Gbit/s
db.m5.xlarge*	4	15	16	Oui	Oui	Jusqu'à 4 750	Jusqu'à 10 Gbit/s
db.m5.large*	2	10	8	Oui	Oui	Jusqu'à 4 750	Jusqu'à 10 Gbit/s
db.m4 – Classes d'instance standard de génération actuelle							
db.m4.16xlarge	64	188	256	Oui	Oui	10 000	25 Gb/s
db.m4.10xlarge	40	124,5	160	Oui	Oui	4 000	10 Gb/s
db.m4.4xlarge	16	53,5	64	Oui	Oui	2 000	Élevée
db.m4.2xlarge	8	25,5	32	Oui	Oui	1 000	Élevée
db.m4.xlarge	4	13	16	Oui	Oui	750	Élevée
db.m4.large	2	6,5	8	Oui	Oui	450	Modérée
db.m3 – Classes d'instance standard de génération précédente							
db.m3.2xlarge	8	26	30	Non	Oui	1 000	Élevée
db.m3.xlarge	4	13	15	Non	Oui	500	Élevée
db.m3.large	2	6,5	7,5	Non	Non	—	Modérées
db.m3.medium	1	3	3,75	Non	Non	—	Modérée
db.m1 – Classes d'instance standard de génération précédente							
db.m1.xlarge	4	4	15	Non	Oui	450	Élevée
db.m1.large	2	2	7,5	Non	Oui	450	Modérée
db.m1.medium	1	1	3,75	Non	Non	—	Modérée
db.m1.small	1	1	1,7	Non	Non	—	Très faible
db.z1d – Classes d'instance à mémoire optimisée de dernière génération							
db.z1d.12xlarge	48	271	384	Oui	Oui	14 000	25 Gbit/s
db.z1d.6xlarge	24	134	192	Oui	Oui	7 000	10 Gbit/s

Classe d'instance	vCPU	ECU	Mémoire (Gio)	VPC uniquemer	Optimisé EBS	Bande passante max (Mo/s)**	Performances réseau
db.z1d.3xlarge	12	75	96	Oui	Oui	3 500	Jusqu'à 10 Gbit/s
db.z1d.2xlarge	8	53	64	Oui	Oui	2 333	Jusqu'à 10 Gbit/s
db.z1d.xlarge*	4	28	32	Oui	Oui	Jusqu'à 2 333	Jusqu'à 10 Gbit/s
db.z1d.large*	2	15	16	Oui	Oui	Jusqu'à 2 333	Jusqu'à 10 Gbit/s
db.x1e – Classes d'instance à mémoire optimisée de dernière génération							
db.x1e.32xlarge	128	340	3 904	Oui	Oui	14 000	25 Gbit/s
db.x1e.16xlarge	64	179	1 952	Oui	Oui	7 000	10 Gbit/s
db.x1e.8xlarge	32	91	976	Oui	Oui	3 500	Jusqu'à 10 Gbit/s
db.x1e.4xlarge	16	47	488	Oui	Oui	1 750	Jusqu'à 10 Gbit/s
db.x1e.2xlarge	8	23	244	Oui	Oui	1 000	Jusqu'à 10 Gbit/s
db.x1e.xlarge	4	12	122	Oui	Oui	500	Jusqu'à 10 Gbit/s
db.x1 – Classes d'instance à mémoire optimisée de génération actuelle							
db.x1.32xlarge	128	349	1 952	Oui	Oui	14 000	25 Gbit/s
db.x1.16xlarge	64	174,5	976	Oui	Oui	7 000	10 Gbit/s
db.r6g – Classes d'instance à mémoire optimisée de dernière génération							
db.r6g.16xlarge	64	–	512	Oui	Oui	19 000	25 Gb/s
db.r6g.12xlarge	48	–	384	Oui	Oui	13 500	20 Gb/s
db.r6g.4xlarge	16	–	128	Oui	Oui	4 750	Jusqu'à 10 Gbit/s
db.r6g.2xlarge*	8	–	64	Oui	Oui	Jusqu'à 4 750	Jusqu'à 10 Gbit/s
db.r6g.xlarge*	4	–	32	Oui	Oui	Jusqu'à 4 750	Jusqu'à 10 Gbit/s
db.r6g.large*	2	–	16	Oui	Oui	Jusqu'à 4 750	Jusqu'à 10 Gbit/s
db.r5 – Classes d'instance à mémoire optimisée de dernière génération							
db.r5.24xlarge	96	347	768	Oui	Oui	19 000	25 Gb/s

Classe d'instance	vCPU	ECU	Mémoire (Gio)	VPC uniquemer	Optimisé EBS	Bande passante max (Mo/s)**	Performances réseau
db.r5.16xlarge	64	264	512	Oui	Oui	13 600	20 Gb/s
db.r5.12xlarge	48	173	384	Oui	Oui	9 500	10 Gb/s
db.r5.8xlarge	32	132	256	Oui	Oui	6 800	10 Gb/s
db.r5.4xlarge	16	71	128	Oui	Oui	4 750	Jusqu'à 10 Gbit/s
db.r5.2xlarge*	8	38	64	Oui	Oui	Jusqu'à 4 750	Jusqu'à 10 Gbit/s
db.r5.xlarge*	4	19	32	Oui	Oui	Jusqu'à 4 750	Jusqu'à 10 Gbit/s
db.r5.large*	2	10	16	Oui	Oui	Jusqu'à 4 750	Jusqu'à 10 Gbit/s
db.r4 – Classes d'instance à mémoire optimisée de génération actuelle							
db.r4.16xlarge	64	195	488	Oui	Oui	14 000	25 Gbit/s
db.r4.8xlarge	32	99	244	Oui	Oui	7 000	10 Gbit/s
db.r4.4xlarge	16	53	122	Oui	Oui	3 500	Jusqu'à 10 Gbit/s
db.r4.2xlarge	8	27	61	Oui	Oui	1 700	Jusqu'à 10 Gbit/s
db.r4.xlarge	4	13,5	30,5	Oui	Oui	850	Jusqu'à 10 Gbit/s
db.r4.large	2	7	15,25	Oui	Oui	425	Jusqu'à 10 Gbit/s
db.r3 – Classes d'instance à mémoire optimisée de génération précédente							
db.r3.8xlarge	32	104	244	Non	Non	—	10 Gbit/s
db.r3.4xlarge	16	52	122	Non	Oui	2 000	Élevée
db.r3.2xlarge	8	26	61	Non	Oui	1 000	Élevée
db.r3.xlarge	4	13	30,5	Non	Oui	500	Modérée
db.r3.large	2	6,5	15,25	Non	Non	—	Modérée
db.m2 – Classes d'instance à mémoire optimisée de génération précédente							
db.m2.4xlarge	8	26	68,4	Non	Oui	1 000	Élevée
db.m2.2xlarge	4	13	34,2	Non	Oui	500	Modérée
db.m2.xlarge	2	6,5	17,1	Non	Non	—	Modérée
db.t3 – Classes d'instance à capacité extensible de génération actuelle							

Classe d'instance	vCPU	ECU	Mémoire (Gio)	VPC uniquemer	Optimisé EBS	Bande passante max (Mo/s)**	Performances réseau
db.t3.2xlarge*	8	Variable	32	Oui	Oui	Jusqu'à 2 048	Jusqu'à 5 Gbit/s
db.t3.xlarge*	4	Variable	16	Oui	Oui	Jusqu'à 2 048	Jusqu'à 5 Gbit/s
db.t3.large*	2	Variable	8	Oui	Oui	Jusqu'à 2 048	Jusqu'à 5 Gbit/s
db.t3.medium*	2	Variable	4	Oui	Oui	Jusqu'à 1 536	Jusqu'à 5 Gbit/s
db.t3.small*	2	Variable	2	Oui	Oui	Jusqu'à 1 536	Jusqu'à 5 Gbit/s
db.t3.micro*	2	Variable	1	Oui	Oui	Jusqu'à 1 536	Jusqu'à 5 Gbit/s
db.t2 – Classes d'instance à capacité extensible de génération actuelle							
db.t2.2xlarge	8	Variable	32	Oui	Non	—	Modérée
db.t2.xlarge	4	Variable	16	Oui	Non	—	Modérée
db.t2.large	2	Variable	8	Oui	Non	—	Modérée
db.t2.medium	2	Variable	4	Oui	Non	—	Modérée
db.t2.small	1	Variable	2	Oui	Non	—	Faible
db.t2.micro	1	Variable	1	Oui	Non	—	Faible

* Ces classes d'instance de base de données peuvent prendre en charge des performances maximales pendant 30 minutes au moins une fois toutes les 24 heures. Pour en savoir plus sur les performances de base de ces types d'instance, consultez Instances optimisées pour Amazon EBS dans le Amazon EC2 Guide de l'utilisateur pour les instances Linux.

Stockage d'instance de base de données Amazon RDS

Les instances de base de données pour Amazon RDS pour MySQL, MariaDB, PostgreSQL, Oracle et Microsoft SQL Server utilisent les volumes Amazon Elastic Block Store (Amazon EBS) pour le stockage des bases de données et des journaux. En fonction du volume de stockage demandé, Amazon RDS ajuste automatiquement sur plusieurs volumes Amazon EBS pour améliorer la performance

Types de stockage Amazon RDS

Amazon RDS propose trois types de stockage : le stockage SSD à usage général (également connu sous le nom de gp2), le stockage d'E/S par seconde provisionnées (également connu sous le nom d'io1) et le stockage magnétique (également connu sous le nom de standard). Ils se distinguent par leurs caractéristiques de performance et leur tarif, ce qui signifie que vous avez la possibilité d'adapter vos

performances de stockage et vos coûts à vos besoins en matière de charge de travail de base de données. Vous pouvez créer des instances de base de données RDS MySQL, MariaDB, Oracle et PostgreSQL dont la capacité de stockage atteint 64 tébioctets (TiO). Vous pouvez créer des instances de base de données SQL Server RDS avec jusqu'à 16 Tio de stockage. Pour ce volume de stockage, utilisez les types de stockage SSD d'I/O par seconde provisionnées et à usage général.

La liste suivante décrit rapidement les trois types de stockage :

- SSD à usage général : les volumes SSD à usage général offrent un stockage économique, idéal pour un large éventail de charges de travail. Ces volumes fournissent des latences inférieures à 10 millisecondes, avec la capacité d'émettre en rafale jusqu'à 3 000 E/S par seconde pendant de longues périodes de temps. Les performances de base de ces volumes sont déterminées par leur taille.

  Pour plus d'informations sur le stockage SSD à usage général, y compris les plages de tailles de stockage, consultez Stockage SSD à usage général (p. 31).
- IOPS provisionnés – Le stockage d'IOPS provisionnés est conçu pour satisfaire les besoins des charges de travail gourmandes en I/O, notamment les charges de travail de base de données qui requièrent une faible latence des I/O et un débit d'I/O homogène.

  Pour plus d'informations sur le stockage IOPS provisionnées, y compris les plages de tailles de stockage, consultez Stockage SSD d'I/O par seconde provisionnées (p. 33).
- Magnétique – Amazon RDS prend également en charge le stockage magnétique pour assurer la rétrocompatibilité. Nous vous recommandons d'utiliser le stockage SSD à usage général ou d'I/O par seconde provisionnées pour tout nouveau besoin de stockage. La capacité maximale de stockage autorisée pour les instances de bases de données sur le stockage magnétique est inférieure à celle des autres types de stockage. Pour plus d'informations, consultez Stockage magnétique (p. 35).

Plusieurs facteurs peuvent affecter les performances des volumes Amazon EBS, tels que la configuration d'instance, les caractéristiques d'I/O et la demande en matière de charge de travail. Pour de plus amples informations sur la façon d'exploiter au mieux vos volumes IOPS provisionnés, veuillez consulter Performances des volumes Amazon EBS.

Stockage SSD à usage général

Le stockage SSD à usage général offre un stockage économique qui est approprié pour la plupart des charges de travail de bases de données. Les plages de tailles de stockage pour les instances de bases de données à usage général SSD sont les suivantes :

- Instances de base de données MariaDB, MySQL, Oracle et PostgreSQL : entre 20 Gio et 64 Tio
- Éditions SQL Server Enterprise, Standard, Web et Express : 20 Gio–16 Tio

Les performances d'I/O de base pour le stockage SSD à usage général sont de 3 IOPS pour chaque Gio, avec un minimum de 100 IOPS. Cette relation signifie que des volumes plus importants obtiennent de meilleures performances. Par exemple, les performances de base pour un volume de 100 Gio sont de 300 I/O par seconde. Les performances de base pour un volume de 1 Tio sont de 3 000 E/S par seconde. Les performances de base pour un volume de 5,34 Tio sont de 16 000 E/S par seconde.

Les volumes inférieurs à 1 Tio peuvent également atteindre 3 000 E/S par seconde pendant des périodes de temps étendues . Le mode rafale n'est pas pertinent pour les volumes supérieurs à 1 Tio. Le solde de crédit des E/S de l'instance détermine les performances de la rafale. Pour plus d'informations sur les crédits d'I/O d'instance, consultez Crédits E/S et performances en rafale (p. 32).

De nombreuses charges de travail n'épuisent jamais le solde de la rafale, c'est pourquoi le stockage SSD à usage général est une solution idéale pour la plupart d'entre elles. Toutefois, certaines charges de travail peuvent épuiser le solde de crédit d'I/O de rafale de 3 000 I/O par seconde. En conséquence, prévoyez votre capacité de stockage de sorte qu'elle corresponde aux besoins de vos charges de travail.

Crédits E/S et performances en rafale

Les performances du stockage SSD à usage général sont régies par la taille du volume, qui dicte le niveau de performance de base du volume, ainsi que la vitesse à laquelle il accumule des crédits d'I/O. Les volumes les plus gros ont un niveau de performance de base plus élevé et accumulent des crédits I/O plus vite. Les crédits I/O représentent la bande passante disponible que votre stockage SSD à usage général peut utiliser pour émettre en rafale de grandes quantités d'I/O lorsqu'il est nécessaire de dépasser le niveau de performance de base. Plus votre stockage dispose de crédits pour les I/O, plus il peut émettre en rafale au-delà de son niveau de performances de base, et plus il est performant quand votre charge de travail en a besoin.

Lors de l'utilisation du stockage SSD à usage général, votre instance de base de données reçoit un solde de crédit d'I/O de 5,4 millions. Ce solde de crédit initial est suffisant pour soutenir les performances en rafale de 3 000 I/O par seconde pour 30 minutes. Ce solde est conçu de façon à fournir un cycle de démarrage initial rapide pour les volumes de démarrage, ainsi qu'une bonne expérience d'action d'amorçage (bootstrap) pour les autres applications. Les volumes gagnent des crédits d'I/O, au rythme de performances de base de 3 I/O par seconde pour chaque Gio de taille du volume. Par exemple, un volume SSD de 100 Gio a une performance de base de 300 I/O par seconde.

Lorsque votre stockage a besoin d'un niveau de performances d'I/O plus élevé que le niveau de base, il utilise les crédits d'I/O du solde de crédits pour émettre en rafale, jusqu'au niveau de performances requis. Ce type de rafale peut atteindre un maximum de 3 000 I/O par seconde. Les stockages supérieurs à 1 000 Gio ont une performance de base égale ou supérieure à la performance rafale maximum. Lorsque votre stockage utilise moins de crédits I/O qu'il n'en gagne en une seconde, les crédits I/O inutilisés sont ajoutés au solde de crédits I/O. Le solde de crédits d'I/O maximum pour une instance de base de données utilisant un stockage SSD à usage général est égal au solde de crédits d'I/O initial (5,4 millions de crédits I/O).

Supposons que votre stockage utilise tout son solde de crédit d'I/O. Ses performances maximales ne dépasseront pas le niveau de base jusqu'à ce que la demande en I/O passe en-dessous du niveau de base et que les crédits non utilisés soient ajoutés au solde de crédits d'I/O. (Le niveau de performance de base est le rythme auquel votre stockage gagne des crédits I/O.) Plus le stockage est important, plus la performance de base est grande et plus la vitesse à laquelle le volume réapprovisionne son solde de crédits I/O est grande.

> **Note**
>
> Les conversions entre le stockage magnétique et le stockage SSD à usage général sont susceptibles d'épuiser votre solde de crédit d'I/O, et d'entraîner ainsi des temps de conversion plus longs. Pour plus d'informations sur le dimensionnement du stockage, consultez Utilisation du stockage pour les instances de base de données Amazon RDS (p. 304).

Le tableau suivant répertorie plusieurs tailles de stockage. Pour chaque taille de stockage, il répertorie les performances de base associées du stockage, qui correspondent également au rythme auquel celui-ci accumule des crédits I/O. Ce tableau répertorie également la durée d'émission en rafales au débit maximum de 3 000 IOPS, en commençant avec un solde de crédits I/O plein. En outre, le tableau répertorie la durée en secondes nécessaire au stockage pour remplir un solde de crédits E/S vide.

> **Note**
>
> La figure E/S par seconde atteint sa valeur maximale à la taille de stockage de 5 334 Gio.

Taille de stockage (Gio)	Performances de base (IOPS)	Durée maximum de performances en rafale à 3 000 IOPS (en secondes)	Secondes nécessaires pour remplir un solde de crédits I/O vide
1	100	1,862	54 000

Taille de stockage (Gio)	Performances de base (IOPS)	Durée maximum de performances en rafale à 3 000 IOPS (en secondes)	Secondes nécessaires pour remplir un solde de crédits I/O vide
100	300	2 000	18 000
250	750	2 400	7 200
500	1 500	3 600	3 600
750	2 250	7 200	2 400
1 000	3 000	Infini	S/O
5 334	16 000	S/O	S/O

La durée des performances en rafale de votre stockage dépend de sa taille, des IOPS en rafale nécessaires et du solde de crédits I/O au début de la rafale. Cette relation est représentée dans l'équation suivante.

```
                              (Credit balance)
Burst duration =  ------------------------------------
                  (Burst IOPS) - 3*(Storage size in GiB)
```

Vous constaterez peut-être que la performance de votre stockage est fréquemment limitée au niveau de base en raison d'un solde de crédits d'I/O nul. Le cas échéant, envisagez d'allouer davantage de stockage SSD à usage général avec un niveau de performance de base plus élevé. Vous pouvez également passer à un stockage des IOPS provisionnées pour les charges de travail nécessitant des performances IOPS soutenues.

Pour les charges de travail dont les exigences en termes d'I/O sont stables, mettre en service un stockage SSD à usage général inférieur à 100 Gio peut entraîner des latences plus importantes si vous épuisez votre solde de crédits d'I/O.

> **Note**
>
> En général, la plupart des charges de travail ne dépassent jamais le solde de crédits I/O.

Pour obtenir une description plus complète de l'impact des performances de base et du solde de crédits d'E/S sur les performances, veuillez consulter Comprendre les performances de rafale et de base avec Amazon RDS et GP2.

Stockage SSD d'I/O par seconde provisionnées

Pour une application de production nécessitant des performances d'I/O rapides et cohérentes, nous recommandons d'utiliser le stockage des IOPS provisionnés. Le stockage des I/O par seconde provisionnées est un type de stockage qui offre des performances de débit prévisibles et une faible latence homogène. Le stockage IOPS provisionnées est optimisé pour les charges de travail de traitement transactionnel en ligne (OLTP) ayant des exigences de performances régulières. Les I/O par seconde provisionnées aident à ajuster ces charges de travail.

> **Note**
>
> La charge de travail de votre base de données ne sera peut-être pas capable d'atteindre 100% des E/S par seconde que vous avez provisionnées. Pour plus d'informations, consultez Autres facteurs ayant un impact sur les performances de stockage (p. 36).

Lorsque vous créez une instance de bases de données, vous spécifiez le taux d'IOPS et la taille du volume. Le rapport entre les IOPS et le stockage alloué (en Gio) doit être d'au moins 0,5. Amazon RDS fournit ce taux d'IOPS pour l'instance de base de données jusqu'à ce que vous le modifiez.

Le tableau suivant contient la plage des I/O par seconde provisionnées et la plage de la taille de stockage pour chaque moteur de base de données.

Moteur de base de données	Plage des IOPS provisionnées	Plage de stockage
MariaDB	1 000–80 000 E/S par seconde	100 Gio–64 Tio
SQL Server Enterprise, Standard et Web Editions	1 000–64 000 IOPS*	20 Gio–16 Tio
SQL Server Express Edition	1 000–64 000 IOPS*	100 Gio–16 Tio
MySQL	1 000–80 000 E/S par seconde	100 Gio–64 Tio
Oracle	1 000–80 000 E/S par seconde	100 Gio–64 Tio
PostgreSQL	1 000–80 000 E/S par seconde	100 Gio–64 Tio

* Le nombre maximal de 64 000 IOPS est garanti uniquement sur les instances basées sur Nitro qui résident sur les types d'instances m5, r5 et z1d. Les autres familles d'instances garantissent des performances jusqu'à 32 000 IOPS. Pour de plus amples informations sur les performances d'IOPS des instances de base de données, veuillez consulter Instances optimisées pour Amazon EBS.

Combinaison du stockage des IOPS provisionnés aux déploiements multi-AZ ou aux réplicas en lecture

Pour les cas d'utilisation de traitement de transaction en ligne (OLTP) de production, nous vous recommandons d'utiliser des déploiements multi-AZ, pour profiter d'une meilleure tolérance aux pannes et d'un meilleur stockage des I/O par seconde provisionnées, et ainsi bénéficier de performances rapides et prévisibles.

Vous pouvez également utiliser le stockage SSD des IOPS provisionnés avec les réplicas en lecture pour MySQL, MariaDB ou PostgreSQL. Le type de stockage pour un réplica en lecture est indépendant de celui de l'instance de base de données principale. Par exemple, vous pouvez utiliser le stockage SSD à usage général pour les réplicas en lecture avec une instance de base de données principale qui utilise le stockage SSD d'IOPS provisionnés afin de réduire les coûts. Dans ce cas toutefois, les performances de vos réplicas en lecture peuvent différer de celles d'une configuration où l'instance de base de données principale et les réplicas en lecture utilisent tous deux le stockage SSD d'IOPS provisionnés.

Coûts du stockage IOPS provisionnées

Avec le stockage d'I/O par seconde provisionnées, vous devez payer pour les ressources provisionnées, que vous les utilisiez ou non au cours d'un mois donné.

Pour de plus amples informations sur la tarification, veuillez consulter Tarification Amazon RDS.

Obtention des meilleures performances du stockage SSD des IOPS provisionnés Amazon RDS

Si votre charge de travail est limitée en I/O, l'utilisation du stockage SSD d'I/O provisionnées peut augmenter le nombre de demandes d'I/O pouvant être traitées simultanément par le système. L'augmentation de la simultanéité permet de réduire la latence, étant donné que les demandes I/O passent moins de temps en file d'attente. La réduction de la latence permet des validations de base de données plus rapides, ce qui améliore le temps de réponse et augmente le débit de la base de données.

Le stockage SSD d'I/O par seconde provisionnées permet de réserver la capacité d'I/O en spécifiant les I/O par seconde. Toutefois, comme avec tout autre attribut de capacité système, le débit maximal sous charge sera limité par la ressource qui sera utilisée en premier. Cette ressource peut être la bande passante réseau, l'UC, la mémoire ou les ressources internes de la base de données.

Stockage magnétique

Amazon RDS prend également en charge le stockage magnétique, pour assurer la compatibilité descendante. Nous vous recommandons d'utiliser le stockage SSD à usage général ou à I/O par seconde provisionnées pour tout nouveau besoin de stockage. Voici quelques limitations pour le stockage magnétique :

- Ne vous permet pas de dimensionner le stockage lors de l'utilisation d'un moteur de base de données SQL Server.
- Ne prend pas en charge le dimensionnement automatique du stockage.
- Ne prend pas en charge les volumes élastiques.
- Limité à une taille maximum de 3 Tio.
- Limité à un maximum de 1 000 I/O par seconde.

Surveillance des performances de stockage

Amazon RDS propose différentes métriques pour déterminer les performances de votre instance de bases de données. Vous pouvez consulter les métriques sur la page de résumé de votre instance sur l'Amazon RDS Management Console. Vous pouvez également utiliser Amazon CloudWatch pour contrôler ces métriques. Pour plus d'informations, consultez Affichage des métriques d'instances de base de données (p. 384). La surveillance améliorée offre des métriques d'I/O plus détaillées. Pour plus d'informations, consultez Surveillance améliorée (p. 394).

Les métriques suivantes sont utiles pour surveiller le stockage de votre instance de base de données :

- IOPS – Nombre d'opérations d'I/O terminées par seconde. Cette métrique est considérée comme l'IOPS moyen pour un intervalle donné. Amazon RDS signale séparément l'IOPS de lecture et d'écriture à des intervalles d'1 minute. L'IOPS total est la somme des IOPS de lecture et d'écriture. Les valeurs habituelles pour les IOPS vont de zéro à des dizaines de milliers par seconde.
- Latence – Temps écoulé entre l'envoi d'une requête d'I/O et sa fin. Cette métrique est considérée comme la latence moyenne pour un intervalle donné. Amazon RDS signale séparément la latence de lecture et d'écriture à des intervalles d'1 minute, en unités de secondes. Les valeurs habituelles pour la latence sont de l'ordre des millisecondes (ms). Par exemple, Amazon RDS indique 2 ms sous la forme de 0,002 seconds.
- Débit – Nombre d'octets transférés chaque seconde depuis et vers le disque. Cette métrique est considérée comme le débit moyen pour un intervalle donné. Amazon RDS signale séparément le débit de lecture et d'écriture à des intervalles d'1 minute, en unités de mégaoctets par seconde (Mo/s). Les valeurs habituelles pour le débit vont de zéro à la taille maximale de la bande passante du canal d'E/S.

- Longueur de la file d'attente – Nombre de demandes d'I/O dans la file d'attente en attente de traitement. Ces demandes d'I/O ont été envoyées par l'application, mais n'ont pas été envoyées à l'appareil, car ce dernier est occupé à traiter d'autres demandes d'I/O. Le temps passé dans une file d'attente est un élément de la latence et du temps de service (non disponible en tant que métrique). Cette métrique est considérée comme la longueur de file d'attente moyenne pour un intervalle donné. Amazon RDS signale séparément la longueur de file d'attente à des intervalles d'1 minute. Les valeurs habituelles pour la longueur de file d'attente vont de zéro à plusieurs centaines.

Les valeurs d'I/O par seconde mesurées sont indépendantes de la taille de l'opération d'I/O individuelle. Cela signifie que lorsque vous mesurez les performances d'I/O, vous devez observer le débit de l'instance et pas simplement le nombre d'opérations d'I/O.

Autres facteurs ayant un impact sur les performances de stockage

Les activités du système et la charge de travail de la base de données peuvent affecter les performances de stockage.

Activités du système

Les activités suivantes liées au système utilisent de la capacité d'I/O et peuvent réduire les performances de l'instance de bases de données lorsqu'elles s'exécutent :

- Création de veille dans plusieurs zones de disponibilité
- Création d'un réplica en lecture
- Modification des types de stockage

Charge de travail d'une base de données

Dans certains cas, la conception de votre base de données ou application entraîne des problèmes de simultanéité, des verrouillages ou d'autres formes de conflit de base de données. Vous pouvez alors rencontrer des difficultés pour utiliser toute la bande passante provisionnée directement. De plus, vous pouvez rencontrer les situations suivantes liées aux charges de travail :

- La limite de débit du type d'instance sous-jacent a été atteinte.
- La longueur de la file d'attente est constamment inférieure à 4 car votre application n'a pas suffisamment d'opérations d'I/O.
- Vous rencontrez un conflit de requête dans la base de données même si une partie de la capacité d'I/O n'est pas utilisée.

Si aucune ressource du système n'a atteint la limite et qu'aucune n'en est proche, et que l'ajout de threads n'augmente pas la vitesse de transaction de la base de données, le conflit est probablement dû au goulot d'étranglement. Les formes les plus courantes sont les conflits des verrous de ligne et des verrous des pages d'index, mais il existe bien d'autres possibilités. Si vous vous trouvez dans cette situation, consultez une personne spécialisée dans le réglage des performances des bases de données.

Classe d'instance de base de données

Afin d'optimiser les performances de votre instance de base de données Amazon RDS, choisissez un type d'instance de la génération actuelle avec suffisamment de bande passante pour prendre en charge votre type de stockage. Par exemple, vous pouvez choisir des instances optimisées EBS et des instances avec une connectivité réseau de 10 gigabits.

Pour obtenir la liste complète des types d'instance Amazon EC2 qui prennent en charge l'optimisation EBS, consultez Types d'instance qui prennent en charge l'optimisation EBS.

Pour obtenir des performances optimales, nous vous encourageons à utiliser la dernière génération d'instances. Les instances de base de données de la génération précédente ont une limite de stockage d'instance plus faible. Le tableau suivant montre le stockage maximum que chaque classe d'instance de base de données peut atteindre pour chaque moteur de base de données. Toutes les valeurs sont exprimées en tebioctets (Tio).

Classe d'instance	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.m5 – Classes d'instances standard de dernière génération					
db.m5.24xlarge	64	16	64	64	64
db.m5.16xlarge	64	16	64	64	64
db.m5.12xlarge	64	16	64	64	64
db.m5.8xlarge	64	16	64	64	64
db.m5.4xlarge	64	16	64	64	64
db.m5.2xlarge	64	16	64	64	64
db.m5.xlarge	64	16	64	64	64
db.m5.large	64	16	64	64	64
db.m4 – Classes d'instances standard de génération actuelle					
db.m4.16xlarge	64	16	64	64	64
db.m4.10xlarge	64	16	64	64	64
db.m4.4xlarge	64	16	64	64	64
db.m4.2xlarge	64	16	64	64	64
db.m4.xlarge	64	16	64	64	64
db.m4.large	64	16	64	64	64
db.m3 – Classes d'instances standard de la génération précédente					
db.m3.2xlarge	6	16	6	6	6
db.m3.xlarge	6	16	6	6	6
db.m3.large	6	16	6	6	6
db.m3.medium	32	16	32	32	32
db.r5 – Classes d'instances à mémoire optimisée de dernière génération					
db.r5.24xlarge	64	16	64	64	64
db.r5.16xlarge	64	16	64	64	64
db.r5.12xlarge	64	16	64	64	64
db.r5.8xlarge	64	16	64	64	64

Classe d'instance	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r5.4xlarge	64	16	64	64	64
db.r5.2xlarge	64	16	64	64	64
db.r5.xlarge	64	16	64	64	64
db.r5.large	64	16	64	64	64
db.r4 – Classes d'instances à mémoire optimisée de génération actuelle					
db.r4.16xlarge	64	16	64	64	64
db.r4.8xlarge	64	16	64	64	64
db.r4.4xlarge	64	16	64	64	64
db.r4.2xlarge	64	16	64	64	64
db.r4.xlarge	64	16	64	64	64
db.r4.large	64	16	64	64	64
db.r3 – Classes d'instances à mémoire optimisée de génération précédente					
db.r3.8xlarge	64	16	64	64	64
db.r3.4xlarge	64	16	64	64	64
db.r3.2xlarge	64	16	64	64	64
db.r3.xlarge	64	16	64	64	64
db.r3.large	64	16	64	64	64
db.t3 – Classes d'instances à capacité extensible de génération actuelle					
db.t3.2xlarge	16	16	16	64	64
db.t3.xlarge	16	16	16	64	64
db.t3.large	16	16	16	64	64
db.t3.medium	16	16	16	32	32
db.t3.small	16	16	16	32	16
db.t3.micro	16	16	16	32	16
db.t2 – Classes d'instances à capacité extensible de génération actuelle					
db.t2.2xlarge	64	16	64	64	64
db.t2.xlarge	64	16	64	64	64
db.t2.large	64	16	64	64	64
db.t2.medium	32	16	32	32	32
db.t2.small	16	16	16	16	16

Classe d'instance	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.t2.micro	16	16	16	16	16
db.x1e – Classes d'instances à mémoire optimisée de dernière génération					
db.x1e.32xlarge		16		64	
db.x1e.16xlarge		16		64	
db.x1e.8xlarge		16		64	
db.x1e.4xlarge		16		64	
db.x1e.2xlarge		16		64	
db.x1e.xlarge		16		64	
db.x1 – Classes d'instances à mémoire optimisée de génération actuelle					
db.x1.32xlarge		16		64	
db.x1.16xlarge		16		64	

Pour Oracle, l'augmentation jusqu'à 80 000 E/S par seconde est uniquement prise en charge sur les classes d'instances suivantes :

- db.m5.24xlarge
- db.r5.24xlarge
- db.x1.32xlarge
- db.x1e.32xlarge

Pour de plus amples informations sur les classes d'instances prises en charge, veuillez consulter Instances de bases de données de la génération précédente.

Régions, zones de disponibilité et zones locales

Les ressources de cloud computing Amazon sont hébergées dans plusieurs emplacements à travers le monde. Ces emplacements sont composés de régions AWS, de zones de disponibilité et de zones locales. Chaque Région AWS est une zone géographique séparée. Chaque région AWS se compose de plusieurs emplacements isolés appelés zones de disponibilité.

> Note
>
> Pour de plus amples informations sur la recherche des zones de disponibilité d'une région AWS, veuillez consulter Description de vos régions, zones de disponibilité et zones locales dans la documentation Amazon EC2.

En utilisant les zones locales, vous pouvez placer des ressources, telles que le calcul et le stockage, dans plusieurs emplacements plus proches de vos utilisateurs. Amazon RDS vous permet de placer des ressources, par exemple des instances de base de données, et des données dans plusieurs emplacements. Les ressources ne sont répliquées d'une région AWS à l'autre que si vous le faites spécifiquement.

Amazon gère des centres de données à la pointe de la technologie et hautement disponibles. Bien qu'elles soient rares, des pannes touchant la disponibilité des instances se trouvant au même emplacement peuvent se produire. Si vous hébergez toutes vos instances dans un seul emplacement touché par une panne de ce type, aucune de vos instances n'est disponible.

Il importe de se souvenir que chaque région AWS est totalement indépendante. Toute activité Amazon RDS que vous initiez (par exemple, la création d'instances de bases de données ou l'affichage des instances de bases de données disponibles) s'exécute uniquement dans votre région AWS actuelle par défaut. La région AWS par défaut peut être modifiée dans la console en définissant la variable d'environnement EC2_REGION ou peut être remplacée à l'aide du paramètre `--region` avec l'AWS Command Line Interface (AWS CLI). Pour de plus amples informations, veuillez consulter Configuration de l'AWS Command Line Interface, plus précisément les sections sur les variables d'environnement et les options de ligne de commande.

Amazon RDS prend en charge une région AWS particulière appelée AWS GovCloud (US-West), destinée à permettre aux clients et aux agences gouvernementales américains de déplacer des charges de travail plus sensibles vers le cloud en respectant leurs exigences de conformité et de réglementation spécifiques. AWS GovCloud (US-West) répond aux exigences spécifiques de conformité et de réglementation du gouvernement américain. Pour de plus amples informations sur AWS GovCloud (US-West), veuillez consulter Qu'est-ce qu'AWS GovCloud (US-West) ?

Pour créer ou utiliser une instance de base de données Amazon RDS dans une région AWS spécifique, utilisez le point de terminaison du service régional correspondant.

Régions AWS

Chaque région AWS est conçue pour être isolée des autres régions AWS. Cette conception permet d'atteindre la plus grande tolérance aux pannes possible et une stabilité optimale.

Lorsque vous consultez vos ressources, vous voyez uniquement celles liées à la région AWS que vous avez spécifiée. Cela est dû au fait que les régions AWS sont éloignées les unes des autres et que nous ne répliquons pas automatiquement les ressources entre les régions AWS.

Zones de disponibilité

Lorsque vous créez une instance de base de données, vous pouvez choisir une zone de disponibilité ou demander à AWS d'en choisir une pour vous. Une zone de disponibilité est représentée par un code de région AWS suivi d'un identifiant à lettre (par exemple, `us-east-1a`).

Dans certains cas, vous pouvez distribuer vos instances de base de données sur plusieurs zones de disponibilité dans un déploiement multi-AZ. Dans ces cas de figure, si une instance de base de données échoue, vous pouvez concevoir votre application de sorte qu'une instance de base de données dans une

autre zone de disponibilité puisse gérer les demandes. Pour plus d'informations sur les déploiements multi-AZ, consultez Haute disponibilité (multi-AZ) pour Amazon RDS (p. 43).

Zones locales

Une zone locale est une extension d'une région AWS qui est géographiquement proche de vos utilisateurs. Vous pouvez étendre n'importe quel VPC de la région AWS parente dans les zones locales en créant un sous-réseau et en l'attribuant à la zone locale AWS. Lorsque vous créez un sous-réseau dans une zone locale, votre VPC est étendu à cette zone locale. Le sous-réseau de la zone locale fonctionne de la même manière que les autres sous-réseaux de votre VPC.

Lorsque vous créez une instance de base de données, vous pouvez choisir un sous-réseau dans une zone locale. Les zones locales ont leurs propres connexions à Internet et prennent en charge AWS Direct Connect. Ainsi, les ressources créées dans une zone locale peuvent servir les utilisateurs locaux avec des communications à très faible latence. Pour de plus amples informations, veuillez consulter les zones locales AWS.

Une zone locale est représentée par un code de région AWS suivi d'un identifiant qui indique l'emplacement ; par exemple, `us-west-2-lax-1a`.

> **Note**
>
> Une zone locale ne peut pas être incluse dans un déploiement multi-AZ.

Pour utiliser une zone locale

1. Activez la zone locale dans la console Amazon EC2.

   Pour de plus amples informations, veuillez consulter Activation des zones locales dans le Amazon EC2 Guide de l'utilisateur pour les instances Linux.
2. Créez un sous-réseau dans la zone locale.

   Pour de plus amples informations, veuillez consulter Création d'un sous-réseau dans votre VPC dans le Amazon VPC Guide de l'utilisateur.
3. Créez un groupe de sous-réseaux de base de données dans la zone locale.

   Lorsque vous créez un groupe de sous-réseaux de base de données, choisissez le groupe de zone de disponibilité pour la zone locale.

   Pour plus d'informations, consultez Création d'une instance de base de données dans un VPC (p. 1624).
4. Créez une instance de base de données qui utilise le groupe de sous-réseaux de base de données dans la zone locale.

   Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).

> **Important**
>
> Actuellement, les zones locales ne sont disponibles que dans la région USA Ouest (Oregon). Dans cette région AWS, la zone locale AWS de Los Angeles est disponible.

Disponibilité dans les régions

Le tableau suivant indique les régions AWS dans lesquelles Amazon RDS est actuellement disponible et le point de terminaison pour chaque région.

Nom de la région	Région	Point de terminaison	Protocole	
USA Est (Ohio)	us-east-2	rds.us-east-2.amazonaws.com rds-fips.us-east-2.amazonaws.com	HTTPS HTTPS	
USA Est (Virginie du Nord)	us-east-1	rds.us-east-1.amazonaws.com rds-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
USA Ouest (Californie du Nord)	us-west-1	rds.us-west-1.amazonaws.com rds-fips.us-west-1.amazonaws.com	HTTPS HTTPS	
USA Ouest (Oregon)	us-west-2	rds.us-west-2.amazonaws.com rds-fips.us-west-2.amazonaws.com	HTTPS HTTPS	
Afrique (Le Cap)	af-south-1	rds.af-south-1.amazonaws.com	HTTPS	
Asie-Pacifique (Hong Kong)	ap-east-1	rds.ap-east-1.amazonaws.com	HTTPS	
Asie-Pacifique (Mumbai)	ap-south-1	rds.ap-south-1.amazonaws.com	HTTPS	
Asie-Pacifique (Osaka-Local)	ap-northeast-3	rds.ap-northeast-3.amazonaws.com	HTTPS	
Asie-Pacifique (Séoul)	ap-northeast-2	rds.ap-northeast-2.amazonaws.com	HTTPS	
Asie-Pacifique (Singapour)	ap-southeast-1	rds.ap-southeast-1.amazonaws.com	HTTPS	
Asie-Pacifique (Sydney)	ap-southeast-2	rds.ap-southeast-2.amazonaws.com	HTTPS	
Asie-Pacifique (Tokyo)	ap-northeast-1	rds.ap-northeast-1.amazonaws.com	HTTPS	
Canada (Centre)	ca-central-1	rds.ca-central-1.amazonaws.com rds-fips.ca-central-1.amazonaws.com	HTTPS HTTPS	
Chine (Pékin)	cn-north-1	rds.cn-north-1.amazonaws.com.cn	HTTPS	

Nom de la région	Région	Point de terminaison	Protocole	
Chine (Ningxia)	cn-northwest-1	rds.cn-northwest-1.amazonaws.com.cn	HTTPS	
Europe (Francfort)	eu-central-1	rds.eu-central-1.amazonaws.com	HTTPS	
Europe (Irlande)	eu-west-1	rds.eu-west-1.amazonaws.com	HTTPS	
Europe (Londres)	eu-west-2	rds.eu-west-2.amazonaws.com	HTTPS	
Europe (Milan)	eu-south-1	rds.eu-south-1.amazonaws.com	HTTPS	
Europe (Paris)	eu-west-3	rds.eu-west-3.amazonaws.com	HTTPS	
Europe (Stockholm)	eu-north-1	rds.eu-north-1.amazonaws.com	HTTPS	
Moyen-Orient (Bahreïn)	me-south-1	rds.me-south-1.amazonaws.com	HTTPS	
Amérique du Sud (São Paulo)	sa-east-1	rds.sa-east-1.amazonaws.com	HTTPS	
AWS GovCloud (USA Est)	us-gov-east-1	rds.us-gov-east-1.amazonaws.com rds.us-gov-east-1.amazonaws.com	HTTPS HTTPS	
AWS GovCloud (US)	us-gov-west-1	rds.us-gov-west-1.amazonaws.com rds.us-gov-west-1.amazonaws.com	HTTPS HTTPS	

Si vous ne spécifiez pas explicitement de point de terminaison, le point de terminaison USA Ouest (Oregon) est la valeur par défaut.

Lorsque vous utilisez une instance de base de données à l'aide de l'AWS CLI ou des opérations d'API, assurez-vous de spécifier son point de terminaison régional.

Haute disponibilité (multi-AZ) pour Amazon RDS

Amazon RDS fournit une haute disponibilité et une prise en charge du basculement pour les instances de base de données grâce aux déploiements Multi-AZ. Amazon RDS utilise plusieurs technologies distinctes pour fournir la prise en charge du basculement. Les déploiements multi-AZ pour les instances de base de données MariaDB, MySQL, Oracle et PostgreSQL utilisent la technologie de basculement d'Amazon. Les instances de base de données SQL Server utilisent la mise en miroir de bases de données SQL Server (DBM) ou les groupes de disponibilité AlwaysOn.

Dans un déploiement multi-AZ, Amazon RDS fournit et maintient automatiquement un réplica de secours synchrone dans une autre zone de disponibilité. L'instance de base de données principale est répliquée de manière synchrone sur les Zones de disponibilité vers un réplica d'attente afin de fournir une redondance de données, d'éliminer les gels E/S et de minimiser les pics de latence pendant les sauvegardes du système. L'exécution d'une instance de base de données avec une haute disponibilité peut améliorer la disponibilité lors de la maintenance planifiée du système et contribuer à protéger vos bases de données contre toute défaillance d'une instance de base de données ou perturbation d'une zone de disponibilité. Pour plus d'informations sur les zones de disponibilité, consultez Régions, zones de disponibilité et zones locales (p. 39).

> **Note**
>
> La fonction de haute disponibilité n'est pas une solution de mise à l'échelle pour les scénarios en lecture seule ; vous ne pouvez pas utiliser un réplica de secours pour traiter le trafic en lecture. Pour traiter le trafic en lecture seule, vous devez utiliser un réplica en lecture. Pour plus d'informations, consultez Utilisation des réplicas en lecture (p. 275).

A l'aide de la console RDS, vous pouvez créer un déploiement Multi-AZ en spécifiant simplement l'option Multi-AZ lors de la création d'une instance de base de données. Vous pouvez utiliser la console pour convertir les instances de base de données existantes en déploiements Multi-AZ en modifiant l'instance de base de données et en spécifiant l'option multi-AZ. Vous pouvez également spécifier un déploiement multi-AZ avec l'API Amazon RDS ou AWS CLI. Utilisez les commandes CLI create-db-instance ou modify-db-instance CLI ou les opérations API CreateDBInstance ou ModifyDBInstance.

La console RDS affiche la zone de disponibilité du réplica de secours (appelée zone de disponibilité secondaire). Vous pouvez également utiliser la commande CLI describe-db-instances ou l'opération API DescribeDBInstances pour rechercher la zone de disponibilité secondaire.

Les instances de base de données qui utilisent les déploiements Multi-AZ peuvent avoir une latence d'écriture et de validation accrue par rapport à un déploiement mono-AZ, en raison de la réplication de données synchrone qui se produit. La latence peut évoluer si votre déploiement bascule vers le réplica de secours, même si AWS est conçu avec une connectivité réseau à faible latence entre les zones de disponibilité. Pour les charges de travail de production, nous vous recommandons d'utiliser les IOPS provisionnés et les classes d'instance de bases de données optimisées pour les IOPS provisionnés afin d'obtenir des performances rapides et régulières. Pour de plus amples informations sur les classes d'instance de base de données, veuillez consulter Classes d'instances de base de données (p. 6).

Modification d'une instance de base de données pour qu'elle devienne un déploiement Multi-AZ

Si vous disposez d'une instance de base de données dans un déploiement mono-AZ et que vous transformez ce dernier en déploiement Multi-AZ (pour les moteurs autres que Amazon Aurora), Amazon RDS procède en plusieurs étapes. D'abord, Amazon RDS prend un instantané de l'instance de base de

données principale de votre déploiement, puis restaure l'instantané dans une autre zone de disponibilité. Amazon RDS configure ensuite la réplication synchrone entre votre instance de base de données principale et la nouvelle instance.

Pour plus d'informations sur la modification d'une instance de base de données , consultez Modification d'une instance de base de données Amazon RDS (p. 243).

> **Important**
>
> Cette action évite les interruptions lorsque vous passez de mono-AZ à Multi-AZ, mais elle peut avoir des conséquences sur les performances pendant et après la conversion en déploiement Multi-AZ. Cet impact peut être significatif pour les instances de base de données qui nécessitent beaucoup d'écriture.
> Pour activer le déploiement Multi-AZ pour une instance de base de données, RDS prend un instantané du volume EBS de l'instance de base de données principale et le restaure sur le réplica de secours nouvellement créé, puis synchronise les deux volumes. Les volumes créés à partir d'instantanés EBS existants se chargent lentement en arrière-plan. Cette fonctionnalité permet de restaurer rapidement de grands volumes à partir d'un instantané, mais la latence peut être accrue pendant et après la modification. Pour de plus amples informations, veuillez consulter Restauration d'un volume Amazon EBS à partir d'un instantané dans la documentation Amazon EC2.

Une fois la modification terminée, Amazon RDS déclenche un événement (RDS-EVENT-0025) qui indique que le processus est terminé. Vous pouvez surveiller les événement Amazon RDS. Pour plus d'informations sur les types d'événements d'instance, consultez Utilisation de la notification d'événement Amazon RDS (p. 467).

Processus de basculement pour Amazon RDS

En cas de panne prévue ou imprévue de votre instance de base de données, Amazon RDS bascule automatiquement sur un réplica de secours d'une autre zone de disponibilité si vous avez activé l'option Multi-AZ. Le temps nécessaire pour que le basculement se termine dépend de l'activité de la base de données et d'autres conditions au moment où l'instance de base de données principale est devenu indisponible. Les durées de basculement oscillent généralement entre 60 et 120 secondes. Cependant, les transactions importantes ou les processus de récupération longs peuvent augmenter le temps de basculement. Lorsque le basculement est terminé, un temps supplémentaire peut être nécessaire pour que la console RDS reflète la nouvelle zone de disponibilité.

> **Note**
>
> Vous pouvez forcer le basculement manuel lorsque vous redémarrez une instance de base de données. Pour de plus amples informations, veuillez consulter Redémarrage d'une instance de base de données (p. 272).

Étant donné qu'Amazon RDS gère automatiquement les basculements, vous pouvez reprendre les opérations de base de données aussi rapidement que possible sans intervention administrative. L'instance de base de données principale bascule automatiquement vers le réplica de secours si l'une des conditions suivantes se produit :

- Panne d'une zone de disponibilité
- Échec de l'instance de bases de données principale
- Modification du type de serveur de l'instance de bases de données
- Le système d'exploitation de l'instance de bases de données est en cours de correction logicielle
- Un basculement manuel de l'instance de base de données a été initié à l'aide de Reboot with failover (Redémarrer avec basculement)

Il existe plusieurs façons de déterminer si votre instance de base de données Multi-AZ a basculé :

- Les abonnements aux événements de base de données peuvent être définis pour vous avertir par e-mail ou par SMS qu'un basculement a été initié. Pour plus d'informations sur les événements, consultez Utilisation de la notification d'événement Amazon RDS (p. 467).
- Vous pouvez afficher les événements DB à l'aide de la console Amazon RDS ou d'opérations d'API.
- Vous pouvez afficher l'état actuel de votre déploiement Multi-AZ à l'aide de la console Amazon RDS et d'opérations d'API.

Pour plus d'informations sur la façon dont vous pouvez réagir aux basculements ou réduire le temps de récupération et sur les autres bonnes pratiques pour Amazon RDS, consultez Bonnes pratiques relatives à Amazon RDS. (p. 135).

Configuration de la durée de vie de la JVM pour les recherches de nom DNS

Le mécanisme de basculement modifie automatiquement l'enregistrement DNS de l'instance de base de données pour pointer vers l'instance de base de données en attente. Par conséquent, vous devez rétablir toutes les connexions existantes à votre instance de base de données. Dans un environnement de machine virtuelle Java, vous devrez peut-être reconfigurer les paramètres de votre machine virtuelle Java, en raison du fonctionnement du mécanisme de mise en cache Java du DNS.

La machine virtuelle Java met en cache les recherches de noms DNS. Lorsque la JVM convertit un nom d'hôte en adresse IP, elle met en cache l'adresse IP pendant une période spécifiée, appelée durée de vie (TTL).

Comme les ressources AWS utilisent des entrées de nom DNS qui changent parfois, nous vous recommandons de configurer votre JVM avec une valeur de durée de vie de 60 secondes. De cette manière, lorsque l'adresse IP d'une ressource change, votre application peut recevoir et utiliser la nouvelle adresse IP de la ressource en interrogeant le DNS.

Dans certaines configurations Java, la durée de vie par défaut de la JVM est définie de façon à ce que la JVM n'actualise jamais les entrées DNS tant qu'elle n'est pas redémarrée. Par conséquent, si l'adresse IP d'une ressource AWS change pendant que votre application est en cours d'exécution, elle ne peut pas utiliser cette ressource tant que vous n'aurez pas redémarré manuellement la JVM et que les informations IP mises en cache n'auront pas été actualisées. Dans ce cas, il est essentiel de définir la durée de vie de la JVM de façon à ce que ses informations IP mises en cache soient régulièrement actualisées.

> **Note**
>
> La durée de vie par défaut peut varier en fonction de la version de votre JVM et selon qu'un gestionnaire de sécurité est installé ou non. De nombreuses JVM fournissent une durée de vie par défaut de moins de 60 secondes. Si c'est le cas pour la JVM que vous utilisez et que vous n'avez pas recours à un gestionnaire de sécurité, vous pouvez ignorer le reste de cette rubrique. Pour de plus amples informations sur les responsables de la sécurité dans Oracle, veuillez consulter The Security Manager dans la documentation Oracle.

Pour modifier la durée de vie de la JVM, définissez la valeur de la propriété `networkaddress.cache.ttl`. Utilisez l'une des méthodes suivantes selon vos besoins :

- Pour définir globalement la valeur de la propriété pour toutes les applications qui utilisent la JVM, définissez `networkaddress.cache.ttl` dans le fichier `$JAVA_HOME/jre/lib/security/java.security`.

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

- Pour définir la propriété localement pour votre application uniquement, définissez `networkaddress.cache.ttl` dans le code d'initialisation de votre application avant que les connexions réseau ne soient établies.

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

Facturation d'une instance de base de données pour Amazon RDS

Les instances Amazon RDS sont facturées en fonction des composants suivants :

- Heures des instances de base de données (par heure) – En fonction de la classe de l'instance de base de données (par exemple, db.t2.small or db.m4.large). La tarification est indiquée selon une base horaire, mais les factures sont calculées à la seconde près et affichent les heures sous une forme décimale. L'utilisation de RDS est facturée par tranches d'une seconde, avec un minimum de 10 minutes. Pour plus d'informations, consultez Classes d'instances de base de données (p. 6).
- Stockage (par Gio, tous les mois) – Capacité de stockage provisionnée pour votre instance de base de données. Si vous dimensionnez votre capacité de stockage provisionnée dans le mois, votre facture est ajustée au prorata. Pour plus d'informations, consultez Stockage d'instance de base de données Amazon RDS (p. 30).
- Demandes d'E/S (par 1 million de demandes par mois) – Nombre total de demandes de stockage d'E/S effectuées au cours d'un cycle de facturation pour le stockage magnétique Amazon RDS uniquement.
- IOPS provisionnées (par IOPS par mois) – Taux d'IOPS provisionnées, quels que soient les IOPS consommées, pour le stockage SSD des IOPS provisionnés Amazon RDS uniquement. Le stockage provisionné pour les volumes EBS est facturé par tranches d'une seconde, avec un minimum de 10 minutes.
- Stockage de sauvegarde (par Gio par mois) – Le stockage de sauvegarde est le stockage associé à vos sauvegardes de base de données automatisées et tout instantané de base de données active que vous avez pris. Augmenter votre période de rétention des sauvegardes ou prendre des instantanés de base de données supplémentaires augmente le stockage de sauvegarde consommé par votre base de données. La facturation à la seconde ne s'applique pas au stockage de sauvegarde (mesuré en Go/mois).

  Pour plus d'informations, consultez Sauvegarde et restauration d'une instance de base de données Amazon RDS (p. 317).
- Transfert de données (par Go) – Transfert de données entrant et sortant de votre instance de données depuis ou vers Internet et d'autres régions AWS.

Amazon RDS propose les options d'achat suivantes pour vous permettre d'optimiser vos coûts en fonction de vos besoins :

- Instances à la demande – Paiement à l'heure pour les heures d'instance de base de données que vous utilisez. La tarification est indiquée selon une base horaire, mais les factures sont calculées à la seconde près et affichent les heures sous une forme décimale. L'utilisation de RDS est facturée par tranches d'une seconde, avec un minimum de 10 minutes.
- Instances réservées – Réservez une instance de base de données pour un à trois ans, et bénéficiez d'une remise considérable par rapport à la tarification des instances de base de données à la demande. Grâce aux instances réservées, vous pouvez lancer, supprimer, démarrer ou arrêter plusieurs instances pendant une heure, puis obtenir l'avantage d'instance réservé pour toutes les instances.

Pour plus d'informations sur la tarification de Amazon RDS, consultez la page produit de Amazon RDS.

Rubriques

- Instances de base de données à la demande pour Amazon RDS (p. 48)
- Instances de base de données réservées à Amazon RDS (p. 48)

Instances de base de données à la demande pour Amazon RDS

Les instances de base de données à la demande Amazon RDS sont facturées en fonction de la classe de l'instance de base de données (par exemple, db.t2.small ou db.m4.large). Pour plus d'informations sur la tarification de Amazon RDS, consultez la page produit de Amazon RDS.

La facturation commence pour une instance de base de données dès que cette dernière est disponible. La tarification est indiquée selon une base horaire, mais les factures sont calculées à la seconde et affichent les heures au format décimal. L'utilisation d'Amazon RDS est facturée à la seconde avec un minimum de 10 minutes. Dans le cas d'une modification de configuration pouvant être facturée, comme le dimensionnement de la capacité de calcul ou de stockage, un minimum de 10 minutes vous est facturé. La facturation continue jusqu'à la résiliation de l'instance de base de données, qui a lieu lorsque vous supprimez cette dernière ou si elle échoue.

Si vous ne souhaitez plus être facturé pour votre instance de base de données, vous devez l'arrêter ou la supprimer afin d'éviter d'être facturé pour des heures d'instance de base de données supplémentaires. Pour plus d'informations sur les états des instances de base de données pour lesquelles vous êtes facturé, consultez Statut d'instance de bases de données (p. 386).

Instances de base de données arrêtées

Pendant que votre instance de base de données est arrêtée, le stockage provisionné vous est facturé, y compris les IOPS provisionnés. Le stockage de sauvegarde vous est également facturé, notamment le stockage des instantanés manuels et des sauvegardes automatisées dans la fenêtre de conservation que vous avez spécifiée. Les heures de l'instance de base de données ne vous sont pas facturées.

Instances de base de données multi-AZ

Si vous spécifiez que votre instance de base de données doit être un déploiement multi-AZ, vous êtes facturé en fonction du tarif multi-AZ publié sur la page de tarification d'Amazon RDS.

Instances de base de données réservées à Amazon RDS

En utilisant des instances de base de données réservées, vous pouvez réserver une instance de base de données pour une durée d'un an ou de trois ans. Ce type d'instance est beaucoup plus économique que les instances de bases de données à la demande. Les instances de bases de données réservées ne sont pas des instances physiques, mais correspondent à une remise sur la facturation appliquée à l'utilisation de certaines instances de bases de données à la demande dans votre compte. Les remises associées aux instances de bases de données réservées varient en fonction du type d'instance et de la région AWS.

En règle générale, pour utiliser des instances de bases de données réservées, commencez par recueillir des informations sur les offres disponibles, achetez l'offre qui vous convient, puis consultez le détail des instances de bases de données réservées existantes.

Présentation des instances de base de données réservées

Lorsque vous achetez une instance de base de données réservée dans Amazon RDS, vous achetez la garantie d'obtenir un tarif réduit sur un type d'instance de bases de données spécifique pour la durée de l'instance de base de données réservée. Pour utiliser une instance de base de données réservée Amazon RDS, créez une instance de bases de données, tout comme vous le feriez pour une instance à la demande. L'instance de bases de données que vous créez doit correspondre aux spécifications de l'instance de base de données réservée. Si les spécifications de la nouvelle instance de bases de données coïncident avec une instance de base de données réservée existante dans votre compte, vous êtes facturé au tarif réduit correspondant à cette dernière. Dans le cas contraire, l'instance de bases de données est facturée selon le tarif à la demande.

Pour plus d'informations sur les instances de bases de données réservées, ainsi que sur leur tarification, consultez Instances réservées Amazon RDS.

Types d'offres

Trois types d'instances de base de données réservées sont disponibles : sans paiement initial, avec paiement initial partiel et avec paiement initial total. Vous pouvez donc optimiser vos coûts Amazon RDS en vous basant sur votre utilisation prévue.

Sans frais initiaux

Cette option vous permet d'accéder à des instances de base de données réservées sans paiement initial. Les instances de bases de données réservées sans frais initiaux n'impliquent aucun paiement initial et sont facturées selon un taux horaire réduit pendant toute la durée de l'engagement, quelle que soit l'utilisation. Cette option est uniquement disponible dans le cadre d'une réservation d'un an.

Frais initiaux partiels

Cette option exige qu'une partie des instances de base de données réservées soit payée d'avance. Les heures restantes pendant la période sont facturées à un taux réduit, quelle que soit l'utilisation. Cette option remplace l'option précédente d'utilisation intensive.

Tous les frais initiaux

Le paiement complet est effectué en totalité au début de la période, sans aucun autre coût pour le reste de la réservation, quel que soit le nombre d'heures utilisé.

Si vous utilisez une facturation consolidée, tous les comptes de l'organisation sont traités comme s'il s'agissait d'un seul compte. Cela signifie que tous les comptes de l'organisation peuvent bénéficier d'un surplus d'heures correspondant aux instances de base de données réservées qui sont achetées par un autre compte. Pour plus d'informations sur la facturation consolidée, consultez Instances de base de données réservées Amazon RDS dans le Guide de l'utilisateur AWS Billing and Cost Management.

Instances de base de données réservées de taille flexible

Lorsque vous achetez une instance de base de données réservée, vous devez spécifier la classe d'instance, par exemple, db.m4.large. Pour plus d'informations sur les classes d'instance , consultez Classes d'instances de base de données (p. 6).

Si vous devez augmenter la capacité d'une instance de base de données, l'instance réservée est automatiquement appliquée à l'instance de base de données que vous avez dimensionnée. En d'autres termes, les instances de base de données réservées sont appliquées automatiquement aux classes d'instances de bases de données, quelle que soit leur taille. Des instances de bases de donnée réservées de taille flexible sont disponibles pour les instances de bases de données ayant les mêmes région AWS et moteur de base de données. Des instances de bases de données réservées de taille flexible peuvent uniquement être mises à l'échelle dans leur type de classe d'instance. Par exemple, une instance de base de données réservée pour une db.m4.large peut être appliquée à une db.m4.xlarge, mais pas à

une db.m5.large, car db.m4 et db.m5 sont des types de classe d'instance différents. Les avantages des instances de base de données réservées s'appliquent également aux configurations à une seule ou plusieurs zones de disponibilité. La flexibilité signifie que vous pouvez vous déplacer librement d'une configuration à une autre dans le même type de classe d'instance de base de données. Par exemple, vous pouvez passer d'un déploiement mono-AZ exécuté sur une classe d'instance de base de données de grande taille à un déploiement multi-AZ exécuté sur deux classes d'instance de base de données de petite taille.

Des instances de base de données réservées de taille flexible sont disponibles pour les moteurs de base de données Amazon RDS suivants :

- MariaDB
- MySQL
- Oracle, Réutilisez vos licences
- PostgreSQL

Pour obtenir des détails sur l'utilisation d'instances réservées de taille flexible avec Aurora, consultez Instances de base de données réservées à Aurora.

Les unités normalisées permettent de comparer l'utilisation pour différentes tailles d'instances de base de données réservées. Par exemple, une unité d'utilisation sur deux instances de bases de données db.m3.large équivaut à huit unités normalisées d'utilisation sur une instance db.m3.small. Le tableau suivant indique le nombre d'unités normalisées pour chaque taille d'instance de bases de données.

Taille d'instance	Unités normalisées pour une seule zone de disponibilité	Unités normalisées pour plusieurs zones de disponibilité
micro	0.5	1
petit	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
32xlarge	256	512

Par exemple, supposons que vous achetez une instance de base de données réservée `db.t2.medium` et que deux instances `db.t2.small` sont exécutées dans votre compte dans la même région AWS. Dans ce cas, l'avantage de facturation est appliqué entièrement à ces deux instances.

De même, si une instance `db.t2.large` est exécutée dans votre compte dans la même région AWS, l'avantage de facturation est appliqué à 50 % de l'utilisation de l'instance de bases de données.

Exemple de facturation d'une instance de base de données réservée

Le prix d'une instance de base de données réservée n'inclut pas les coûts récurrents associés au stockage, aux sauvegardes et aux E/S. L'exemple suivant illustre le coût total mensuel pour une instance de base de données réservée :

- Classe d'instance de base de données db.r4.large multi-AZ réservée Amazon RDS MySQL dans la région USA Est (Virginie du Nord) avec l'option No Upfront (aucuns frais initiaux) au coût de 0,12 USD pour l'instance, soit 90 USD par mois
- 400 Gio de stockage Volume à usage général SSD (GP2) au coût de 0,115 par Gio et par mois, soit 45,60 USD par mois
- 600 Gio de stockage de sauvegarde au coût de 0,095 USD, soit 19 USD par mois (400 Gio gratuits)

Ajoutez toutes ces options (90 USD + 45,60 USD + 19 USD) à l'instance de base de données réservée : le coût total mensuel est de 154,60 USD.

Si vous choisissez d'utiliser une instance de base de données à la demande au lieu d'une instance de base de données réservée, une classe d'instance de base de données db.r4.large multi-AZ Amazon RDS MySQL dans la région USA Est (Virginie du Nord) coûte de 0,1386 USD par heure, soit

101,18 USD par mois. Pour une instance de base de données à la demande, ajoutez toutes ces options (101,18 USD + 45,60 USD + 19 USD) ; le coût total mensuel est de 165,78 USD.

> **Note**
>
> Les prix indiqués ici sont des exemples et ne correspondent pas aux prix réels.
> Pour plus d'informations sur la tarification de Amazon RDS, consultez la page produit de Amazon RDS.

Suppression d'une instance de base de données réservée

Les conditions d'une instance de base de données réservée impliquent un engagement d'un an ou de trois ans. Il n'est pas possible d'annuler une instance de base de données réservée. Toutefois, vous pouvez supprimer une instance de base de données à laquelle s'applique une remise d'instance de base de données réservée. Le processus de suppression d'une instance de base de données couverte par ce type de remise est le même que pour n'importe quelle autre instance de bases de données.

Le paiement initial effectué pour une instance de bases de données réservée réserve les ressources pour votre utilisation. Étant donné que ces ressources vous sont réservées, vous êtes facturé que vous les utilisiez ou non.

Si vous supprimez une instance de base de données à laquelle s'applique une remise d'instance de base de données réservée, vous pouvez lancer toute autre instance de bases de données dont les spécifications sont compatibles. Dans ce cas, vous conservez le tarif réduit jusqu'à la fin de la période de réservation (d'un ou de trois ans).

Console

Les procédures suivantes montrent comment utiliser les instances de base de données réservées avec AWS Management Console.

Pour obtenir la tarification et les informations relatives aux offres d'instances de bases de données réservées disponibles

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Instances réservées.
3. Choisissez Purchase Reserved DB Instance (Instance de base de données réservée à l'achat).
4. Pour Description du produit, choisissez le moteur de base de données et le type de licence.
5. Pour Classe d'instance de base de données, choisissez la classe d'instance de base de données.
6. Pour Multi-AZ deployment (Déploiement multi-AZ), choisissez si vous souhaitez un déploiement multi-AZ ou non.
7. Pour Durée, choisissez la durée pendant laquelle vous souhaitez que l'instance de base de données soit réservée.
8. Pour Type d'offre, choisissez le type d'offre.

   Les informations relatives à la tarification s'affichent après la sélection du type d'offre.

   > **Important**
   >
   > Choisissez Annuler pour éviter d'acheter l'instance de base de données réservée et d'avoir à payer des frais.

Une fois que vous disposez des informations requises sur les offres d'instances de bases de données réservées disponibles, vous pouvez utiliser ces informations pour acheter une offre, comme le montre la procédure suivante.

Pour acheter une instance de base de données réservée

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Instances réservées.
3. Choisissez Purchase Reserved DB Instance (Instance de base de données réservée à l'achat).
4. Pour Description du produit, choisissez le moteur de base de données et le type de licence.
5. Pour Classe d'instance de base de données, choisissez la classe d'instance de base de données.
6. Pour Multi-AZ deployment (Déploiement multi-AZ), choisissez si vous souhaitez un déploiement multi-AZ ou non.
7. Pour Durée, choisissez la durée pendant laquelle vous souhaitez que l'instance de base de données soit réservée.
8. Pour Type d'offre, choisissez le type d'offre.

   Comme l'illustre l'image ci-dessous, les informations relatives à la tarification s'affichent après la sélection du type d'offre.

Purchase Reserved DB Instances
Choose from the options below, then enter the number of DB instances you wish to reserve with this order. When you are done, click the Continue button.
Options
Product description
aurora-mysql
DB instance class
db.r4.4xlarge — 16 vCPU, 122 GiB RAM
Multi AZ deployment
Multi-AZ deployment model is not applicable for this database engine and edition
Yes
No
Term
1 year
Offering type
All Upfront
Reserved Id (optional)
Optional tag to track your reservation
Number of DB instances
1
Pricing details
One-time payment (per instance)
Total one-time payment*
*Additional taxes may apply
Normalized units per hour info
32
Usage charges*
USD (hourly)
*Additional taxes may apply
This hourly rate is charged for every hour for each instance in the Reserved Instance term you purchase, regardless of instance usage
Charges for your usage will appear on your monthly bill.
Cancel
Continue

9. (Facultatif) Afin de faciliter le suivi des instances de base de données réservées que vous achetez, vous pouvez leur attribuer un identifiant de votre choix. Dans Reserved Id (ID réservé), tapez un identifiant pour l'instance de bases de données réservée.
10. Choisissez Continue.

    Comme vous pouvez le constater ci-dessous, la boîte de dialogue Purchase Reserved DB Instance (Instance de base de données réservée à l'achat) affiche un résumé des attributs de l'instance de bases de données réservée que vous avez sélectionnée, ainsi que la somme due.

11. Sur la page de confirmation, vérifiez l'instance de bases de données réservée. Si les informations sont correctes, choisissez Acheter pour acheter l'instance de bases de données réservée.

    Dans le cas contraire, choisissez Retour pour la modifier.

Une fois que vous avez acheté une instance de bases de données réservée, suivez la procédure ci-dessous afin d'en consulter le détail.

Pour plus d'informations sur les instances de base de données réservées pour votre compte AWS

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet Navigation, choisissez Instances réservées.

   Les instances de bases de données réservées pour votre compte s'affichent. Pour afficher des informations détaillées sur une instance de base de données réservée particulière, choisissez cette instance dans la liste. Vous pouvez alors consulter des informations détaillées sur cette instance dans le volet de détails au bas de la console.

AWS CLI

Les exemples suivants montrent comment utiliser les instances de base de données réservées avec l'AWS CLI.

Example Affichage des informations relatives aux offres d'instances de base de données réservées disponibles

Pour obtenir des informations relatives aux offres d'instances de bases de données réservées disponibles, appelez la commande `describe-reserved-db-instances-offerings` de l'AWS CLI.

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

Cet appel vous renvoie des informations semblables à ce qui suit :

```
OFFERING  OfferingId                            Class         Multi-AZ  Duration  Fixed
 Price  Usage Price  Description  Offering Type
OFFERING  438012d3-4052-4cc7-b2e3-8d3372e0e706  db.m1.large   y         1y        1820.00
 USD  0.368 USD    mysql        Partial  Upfront
OFFERING  649fd0c8-cf6d-47a0-bfa6-060f8e75e95f  db.m1.small   n         1y         227.50
 USD  0.046 USD    mysql        Partial  Upfront
OFFERING  123456cd-ab1c-47a0-bfa6-12345667232f  db.m1.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.m1.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.m1.xlarge  n         1y        4242.00
 USD   2.42 USD    mysql        No       Upfront
```

Une fois que vous disposez des informations requises sur les offres d'instances de bases de données réservées disponibles, vous pouvez utiliser ces informations pour acheter une offre, comme le montre l'exemple suivant.

Example Acheter une instance de base de données réservée

Pour acheter une instance de bases de données réservée, exécutez la commande `purchase-reserved-db-instances-offering` de l'AWS CLI avec les paramètres suivants :

- `--reserved-db-instances-offering-id` – identifiant de l'offre que vous souhaitez acheter. Reportez-vous à l'exemple précédent pour obtenir l'ID de l'offre.

- `--reserved-db-instance-id` – vous pouvez attribuer l'identifiant de votre choix aux instances de base de données réservées que vous achetez pour en faciliter le suivi.

L'exemple suivant montre l'achat d'une offre particulière d'instance de bases de données réservée, *649fd0c8-cf6d-47a0-bfa6-060f8e75e95f*, avec l'attribution de l'identifiant *MyReservation*.

Pour Linux, macOS ou Unix :

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

Pour Windows :

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

La commande renvoie un résultat semblable à ce qui suit :

```
RESERVATION  ReservationId      Class        Multi-AZ  Start Time                Duration
 Fixed Price  Usage Price  Count  State            Description  Offering Type
RESERVATION  MyReservation      db.m1.small  y         2011-12-19T00:30:23.247Z  1y
 455.00 USD   0.092 USD    1      payment-pending  mysql        Partial  Upfront
```

Comme le montre l'exemple ci-dessous, une fois que vous avez acheté une instance de bases de données réservée, vous pouvez en consulter le détail.

Example Affichage des informations relatives à vos instances de base de données réservées

Pour afficher des informations sur les instances de bases de données réservées pour votre compte AWS, appelez la commande `describe-reserved-db-instances` de l'AWS CLI.

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

La commande renvoie un résultat semblable à ce qui suit :

```
RESERVATION  ReservationId     Class        Multi-AZ  Start Time                Duration
 Fixed Price  Usage Price  Count  State    Description  Offering Type
RESERVATION  MyReservation     db.m1.small  y         2011-12-09T23:37:44.720Z  1y
 455.00 USD   0.092 USD    1      retired  mysql        Partial  Upfront
```

API RDS

Les exemples suivants montrent comment utiliser les instances de base de données réservées avec l'API RDS.

Example Affichage des informations relatives aux offres d'instances de base de données réservées disponibles

Pour afficher des informations sur les offres d'instances de bases de données réservées disponibles, appelez la fonction `DescribeReservedDBInstancesOfferings` de l'API Amazon RDS.

```
https://rds.us-east-1.amazonaws.com/
```

```
?Action=DescribeReservedDBInstancesOfferings
&SignatureMethod=HmacSHA256
&SignatureVersion=4
&Version=2014-09-01
&X-Amz-Algorithm=AWS4-HMAC-SHA256
&X-Amz-Credential=AKIADQKE4SARGYLE/20140411/us-east-1/rds/aws4_request
&X-Amz-Date=20140411T203327Z
&X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
&X-Amz-Signature=545f04acffeb4b80d2e778526b1c9da79d0b3097151c24f28e83e851d65422e2
```

Cet appel vous renvoie des informations semblables à ce qui suit :

```
<DescribeReservedDBInstancesOfferingsResponse xmlns="http://rds.amazonaws.com/
doc/2014-10-31/">
  <DescribeReservedDBInstancesOfferingsResult>
    <ReservedDBInstancesOfferings>
      <ReservedDBInstancesOffering>
        <Duration>31536000</Duration>
        <OfferingType>Partial Upfront</OfferingType>
        <CurrencyCode>USD</CurrencyCode>
        <RecurringCharges/>
        <FixedPrice>1820.0</FixedPrice>
        <ProductDescription>mysql</ProductDescription>
        <UsagePrice>0.368</UsagePrice>
        <MultiAZ>true</MultiAZ>
        <ReservedDBInstancesOfferingId>438012d3-4052-4cc7-b2e3-8d3372e0e706</
ReservedDBInstancesOfferingId>
        <DBInstanceClass>db.m1.large</DBInstanceClass>
      </ReservedDBInstancesOffering>
      <ReservedDBInstancesOffering>
        <Duration>31536000</Duration>
        <OfferingType>Partial Upfront</OfferingType>
        <CurrencyCode>USD</CurrencyCode>
        <RecurringCharges/>
        <FixedPrice>227.5</FixedPrice>
        <ProductDescription>mysql</ProductDescription>
        <UsagePrice>0.046</UsagePrice>
        <MultiAZ>false</MultiAZ>
        <ReservedDBInstancesOfferingId>649fd0c8-cf6d-47a0-bfa6-060f8e75e95f</
ReservedDBInstancesOfferingId>
        <DBInstanceClass>db.m1.small</DBInstanceClass>
      </ReservedDBInstancesOffering>
    </ReservedDBInstancesOfferings>
  </DescribeReservedDBInstancesOfferingsResult>
  <ResponseMetadata>
    <RequestId>5e4ec40b-2978-11e1-9e6d-771388d6ed6b</RequestId>
  </ResponseMetadata>
</DescribeReservedDBInstancesOfferingsResponse>
```

Une fois que vous disposez des informations requises sur les offres d'instances de bases de données réservées disponibles, vous pouvez utiliser ces informations pour acheter une offre, comme le montre l'exemple suivant.

Example Acheter une instance de base de données réservée

Pour acheter une instance de bases de données réservée, appelez l'opération d'API Amazon RDS `PurchaseReservedDBInstancesOffering` avec les paramètres suivants :

- `--reserved-db-instances-offering-id` – identifiant de l'offre que vous souhaitez acheter. Reportez-vous à l'exemple précédent pour obtenir l'ID de l'offre.
- `--reserved-db-instance-id` – vous pouvez attribuer l'identifiant de votre choix aux instances de base de données réservées que vous achetez pour en faciliter le suivi.

L'exemple suivant montre l'achat d'une offre particulière d'instance de bases de données réservée, *649fd0c8-cf6d-47a0-bfa6-060f8e75e95f*, avec l'attribution de l'identifiant *MyReservation*.

```
https://rds.us-east-1.amazonaws.com/
   ?Action=PurchaseReservedDBInstancesOffering
   &ReservedDBInstanceId=MyReservation
   &ReservedDBInstancesOfferingId=438012d3-4052-4cc7-b2e3-8d3372e0e706
   &DBInstanceCount=10
   &SignatureMethod=HmacSHA256
   &SignatureVersion=4
   &Version=2014-09-01
   &X-Amz-Algorithm=AWS4-HMAC-SHA256
   &X-Amz-Credential=AKIADQKE4SARGYLE/20140415/us-east-1/rds/aws4_request
   &X-Amz-Date=20140415T232655Z
   &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
   &X-Amz-Signature=c2ac761e8c8f54a8c0727f5a87ad0a766fbb0024510b9aa34ea6d1f7df52fb11
```

Cet appel vous renvoie des informations semblables à ce qui suit :

```
<PurchaseReservedDBInstancesOfferingResponse xmlns="http://rds.amazonaws.com/
doc/2014-10-31/">
  <PurchaseReservedDBInstancesOfferingResult>
    <ReservedDBInstance>
      <OfferingType>Partial Upfront</OfferingType>
      <CurrencyCode>USD</CurrencyCode>
      <RecurringCharges/>
      <ProductDescription>mysql</ProductDescription>
      <ReservedDBInstancesOfferingId>649fd0c8-cf6d-47a0-bfa6-060f8e75e95f</
ReservedDBInstancesOfferingId>
      <MultiAZ>true</MultiAZ>
      <State>payment-pending</State>
      <ReservedDBInstanceId>MyReservation</ReservedDBInstanceId>
      <DBInstanceCount>10</DBInstanceCount>
      <StartTime>2011-12-18T23:24:56.577Z</StartTime>
      <Duration>31536000</Duration>
      <FixedPrice>123.0</FixedPrice>
      <UsagePrice>0.123</UsagePrice>
      <DBInstanceClass>db.m1.small</DBInstanceClass>
    </ReservedDBInstance>
  </PurchaseReservedDBInstancesOfferingResult>
  <ResponseMetadata>
    <RequestId>7f099901-29cf-11e1-bd06-6fe008f046c3</RequestId>
  </ResponseMetadata>
</PurchaseReservedDBInstancesOfferingResponse>
```

Comme le montre l'exemple ci-dessous, une fois que vous avez acheté une instance de bases de données réservée, vous pouvez en consulter le détail.

Example Affichage des informations relatives à vos instances de base de données réservées

Pour plus d'informations sur les instances de base de données réservées pour votre compte AWS, appelez l'opération d'API Amazon RDS`DescribeReservedDBInstances`.

```
https://rds.us-west-2.amazonaws.com/
   ?Action=DescribeReservedDBInstances
   &SignatureMethod=HmacSHA256
   &SignatureVersion=4
   &Version=2014-09-01
   &X-Amz-Algorithm=AWS4-HMAC-SHA256
   &X-Amz-Credential=AKIADQKE4SARGYLE/20140420/us-west-2/rds/aws4_request
   &X-Amz-Date=20140420T162211Z
   &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
```

```
&X-Amz-Signature=3312d17a4c43bcd209bc22a0778dd23e73f8434254abbd7ac53b89ade3dae88e
```

L'API renvoie un résultat semblable à ce qui suit :

```
<DescribeReservedDBInstancesResponse xmlns="http://rds.amazonaws.com/doc/2014-10-31/">
  <DescribeReservedDBInstancesResult>
    <ReservedDBInstances>
      <ReservedDBInstance>
        <OfferingType>Partial Upfront</OfferingType>
        <CurrencyCode>USD</CurrencyCode>
        <RecurringCharges/>
        <ProductDescription>mysql</ProductDescription>
        <ReservedDBInstancesOfferingId>649fd0c8-cf6d-47a0-bfa6-060f8e75e95f</
ReservedDBInstancesOfferingId>
        <MultiAZ>false</MultiAZ>
        <State>payment-failed</State>
        <ReservedDBInstanceId>MyReservation</ReservedDBInstanceId>
        <DBInstanceCount>1</DBInstanceCount>
        <StartTime>2010-12-15T00:25:14.131Z</StartTime>
        <Duration>31536000</Duration>
        <FixedPrice>227.5</FixedPrice>
        <UsagePrice>0.046</UsagePrice>
        <DBInstanceClass>db.m1.small</DBInstanceClass>
      </ReservedDBInstance>
      <ReservedDBInstance>
        <OfferingType>Partial Upfront</OfferingType>
        <CurrencyCode>USD</CurrencyCode>
        <RecurringCharges/>
        <ProductDescription>mysql</ProductDescription>
        <ReservedDBInstancesOfferingId>649fd0c8-cf6d-47a0-bfa6-060f8e75e95f</
ReservedDBInstancesOfferingId>
        <MultiAZ>false</MultiAZ>
        <State>payment-failed</State>
        <ReservedDBInstanceId>MyReservation</ReservedDBInstanceId>
        <DBInstanceCount>1</DBInstanceCount>
        <StartTime>2010-12-15T01:07:22.275Z</StartTime>
        <Duration>31536000</Duration>
        <FixedPrice>227.5</FixedPrice>
        <UsagePrice>0.046</UsagePrice>
        <DBInstanceClass>db.m1.small</DBInstanceClass>
      </ReservedDBInstance>
    </ReservedDBInstances>
  </DescribeReservedDBInstancesResult>
  <ResponseMetadata>
    <RequestId>23400d50-2978-11e1-9e6d-771388d6ed6b</RequestId>
  </ResponseMetadata>
</DescribeReservedDBInstancesResponse>
```

Configuration pour Amazon RDS

Effectuez les tâches décrites dans cette section pour configurer Amazon Relational Database Service (Amazon RDS) pour la première fois. Si vous possédez déjà un compte AWS, que vous connaissez déjà les exigences de Amazon RDS et que vous préférez utiliser toutes les valeurs par défaut pour les groupes de sécurité IAM et VPC, vous pouvez passer directement à Mise en route (p. 4).

Ce que vous devez savoir sur Amazon Web Services (AWS) :

- Lorsque vous vous inscrivez à AWS, votre compte AWS a automatiquement accès à tous les services AWS, y compris Amazon RDS. Toutefois, seuls les services que vous utilisez vous sont facturés.
- Avec Amazon RDS, vous ne payez que pour les instances RDS qui sont actives. L'instance de base de données Amazon RDS que vous créez est en ligne (elle ne s'exécute pas dans un environnement de test (sandbox)). Vous devez payer les frais d'utilisation standard d'Amazon RDS pour l'instance jusqu'à ce que vous la mettiez hors service. Pour plus d'informations sur les tarifs d'utilisation relatifs à Amazon RDS, consultez la page de présentation du produit Amazon RDS.

Rubriques

- Inscrivez-vous à AWS (p. 62)
- Création d'un utilisateur IAM (p. 62)
- Déterminer les exigences (p. 64)
- Créer un groupe de sécurité qui autorise l'accès à votre instance de base de données dans votre VPC (p. 66)

Inscrivez-vous à AWS

Si vous possédez déjà un compte AWS, passez à la section suivante : Création d'un utilisateur IAM (p. 62).

Si tel n'est pas le cas, utilisez la procédure suivante pour en créer un. Si vous êtes un nouveau client AWS, vous pouvez démarrer gratuitement avec Amazon RDS. Pour de plus amples informations, veuillez consulter Niveau d'offre gratuite AWS.

Pour créer un nouveau compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

Création d'un utilisateur IAM

Après que vous avez créé un compte AWS et que vous vous êtes connecté à la AWS Management Console, vous pouvez créer un utilisateur AWS Identity and Access Management (IAM). Au lieu de vous connecter avec votre compte racine AWS, nous vous recommandons d'utiliser un utilisateur administratif IAM avec Amazon RDS.

Pour cela, vous pouvez créer un nouvel utilisateur IAM et lui accorder des autorisations d'administrateur. Vous pouvez aussi utiliser un utilisateur IAM existant à un groupe IAM avec les autorisations administratives Amazon RDS. Vous pouvez alors accéder à AWS depuis une URL spéciale à l'aide des informations d'identification de l'utilisateur IAM.

Si vous êtes inscrit à AWS, mais que vous n'avez pas créé d'utilisateur IAM pour vous-même, vous pouvez le faire avec la console IAM.

Pour créer un administrateur pour vous-même et ajouter l'utilisateur à un groupe d'administrateurs (console)

1. Connectez-vous à la console IAM en tant que propriétaire du compte en choisissant utilisateur racine et en saisissant l'adresse e-mail de votre compte AWS. Sur la page suivante, saisissez votre mot de passe.

   > **Note**
   >
   > Nous vous recommandons vivement de respecter la bonne pratique qui consiste à avoir recours à l'utilisateur **`Administrator`** IAM ci-dessous et à mettre en sécurité les informations d'identification de l'utilisateur racine. Connectez-vous en tant qu'utilisateur racine pour effectuer certaines tâches de gestion des comptes et des services.

2. Dans le panneau de navigation, choisissez Utilisateurs, puis Add user (Ajouter un utilisateur).
3. Dans User name (Nom d'utilisateur), entrez **`Administrator`**.
4. Cochez la case en regard de AWS Management Console access. Puis, sélectionnez Custom password (Mot de passe personnalisé, et entrez votre nouveau mot de passe dans la zone de texte.
5. Par défaut, AWS oblige le nouvel utilisateur à créer un nouveau mot de passe lors de sa première connexion. Décochez la case en regard de User must create a new password at next sign-in (L'utilisateur doit créer un nouveau mot de passe à sa prochaine connexion) pour autoriser le nouvel utilisateur à réinitialiser son mot de passe une fois qu'il s'est connecté.
6. Choisissez Next: Permissions (Suivant : Autorisations).
7. Sous Set permissions (Accorder des autorisations), choisissez Add user to group (Ajouter un utilisateur au groupe).
8. Choisissez Create group.
9. Dans la boîte de dialogue Create group (Créer un groupe), pour Group name (Nom du groupe), tapez **`Administrators`**.
10. Choisissez Filter policies (Filtrer les stratégies), puis sélectionnez AWS managed -job function (Fonction -job gérée par) pour filtrer le contenu de la table.
11. Dans la liste des stratégies, cochez la case AdministratorAccess. Choisissez ensuite Create group.

    > **Note**
    >
    > Vous devez activer l'accès des rôles et utilisateurs IAM à la facturation avant de pouvoir utiliser les autorisations `AdministratorAccess` pour accéder à la console AWS Billing and Cost Management. Pour ce faire, suivez les instructions de l'étape 1 du didacticiel portant sur comment déléguer l'accès à la console de facturation.

12. De retour dans la liste des groupes, activez la case à cocher du nouveau groupe. Choisissez Refresh si nécessaire pour afficher le groupe dans la liste.
13. Choisissez Next: Tags (Suivant : Balises).
14. (Facultatif) Ajoutez des métadonnées à l'utilisateur en associant les balises sous forme de paires clé-valeur. Pour plus d'informations sur l'utilisation des balises dans IAM, consultez Balisage des entités IAM dans le IAM Guide de l'utilisateur.
15. Choisissez Next: Review pour afficher la liste des membres du groupe à ajouter au nouvel utilisateur. Une fois que vous êtes prêt à continuer, choisissez Create user.

Vous pouvez utiliser ce même processus pour créer d'autres groupes et utilisateurs et pour accorder à vos utilisateurs l'accès aux ressources de votre compte AWS. Pour en savoir plus sur l'utilisation des stratégies afin de limiter les autorisations d'accès des utilisateurs à certaines ressources AWS, consultez Gestion des accès et Exemples de stratégies.

Pour vous connecter avec les identifiants de ce nouvel utilisateur IAM, vous devez d'abord vous déconnecter de la AWS Management Console. Utilisez ensuite l'URL suivante, où *votre_id_compte_aws* est votre numéro de compte AWS sans les tirets. Par exemple, si votre numéro de compte AWS est `1234-5678-9012`, votre ID de compte AWS est `123456789012`.

```
https://your_aws_account_id.signin.aws.amazon.com/console/
```

Saisissez le nom utilisateur et le mot de passe IAM que vous venez de créer. Lorsque vous êtes connecté, la barre de navigation affiche « votre_nom_utilisateur @ votre_id_de_compte_aws ».

Si vous ne voulez pas que l'URL de votre page de connexion contienne votre ID de compte AWS, vous pouvez créer un alias de compte. Depuis le tableau de bord IAM, sélectionnez Customize (Personnaliser) et saisissez un alias, par exemple le nom de votre société. Pour vous connecter après avoir créé un alias de compte, utilisez l'URL suivante.

```
https://your_account_alias.signin.aws.amazon.com/console/
```

Pour contrôler le lien de connexion des utilisateurs IAM de votre compte, ouvrez la console IAM et vérifiez le lien sous AWS Account Alias sur le tableau de bord.

Vous pouvez également créer des clés d'accès pour votre compte AWS. Vous pouvez ensuite utiliser ces clés d'accès pour accéder à AWS via l'AWS Command Line Interface (AWS CLI) ou via l'API Amazon RDS. Pour de plus amples informations, veuillez consulter Accès par programme, Installation de AWS CLI, et Référence de l'API Amazon RDS.

Déterminer les exigences

La fondation de base d'Amazon RDS est l'instance de base de données. Dans une instance de base de données, vous pouvez créer vos bases de données. Une instance de base de données fournit une adresse réseau appelée point de terminaison. Vos applications utilisent ce point de terminaison pour se connecter à votre instance de base de données. Lorsque vous créez une instance de base de données, vous spécifiez des détails tels que le stockage, la mémoire, le moteur et la version de la base de données, la configuration réseau, la sécurité et les périodes de maintenance. Votre contrôlez l'accès réseau à une instance de base de données via un groupe de sécurité.

Avant de créer une instance de base de données et un groupe de sécurité, vous devez connaître les besoins en termes d'instances de base de données et de réseau. Voici quelques éléments importants à prendre en compte :

- Exigences en matière de ressources– Quelles sont les exigences de votre application ou de votre service en termes de mémoire et de processeur ? Vous utilisez ces paramètres pour déterminer plus facilement la classe d'instance de base de données à utiliser. Pour obtenir les caractéristiques des classes des instances de bases de données, consultez Classes d'instances de base de données (p. 6).
- VPC, sous-réseau et groupe de sécurité– Votre instance de base de données se trouve le plus probablement dans un cloud privé virtuel (VPC). Pour vous connecter à votre instance de base de données, vous devez configurer des règles de groupes de sécurité. Ces règles sont configurées différemment selon le type de VPC que vous utilisez : VPC et comment vous l'utilisez dans un VPC par défaut, un VPC défini par l'utilisateur ou en dehors d'un VPC.

  > **Note**
  >
  > Certains comptes hérités n'utilisent pas de VPC. Si vous accédez à une nouvelle région AWS ou que vous êtes un nouvel utilisateur de RDS (après 2013), vous allez plus probablement créer une instance de base de données au sein d'un VPC.

  Pour savoir comment déterminer si votre compte possède un VPC par défaut dans une région AWS particulière, consultez Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611).

La liste suivante décrit les règles pour chaque option de VPC :

- VPC par défaut – Si votre compte AWS possède un VPC par défaut dans la région AWS actuelle, ce VPC est configuré pour prendre en charge des instances de bases de données. Si vous spécifiez le VPC par défaut lorsque vous créez l'instance de base de données, procédez comme suit :
  - Créez un groupe de sécurité VPC autorisant les connexions de l'application ou du service à l'instance de base de données Amazon RDS contenant la base de données. Utilisez l'option API Amazon EC2 ou l'option Groupe de sécurité de la console VPC pour créer des groupes de sécurité VPC. Pour plus d'informations, consultez Étape 4 : Créer un groupe de sécurité VPC (p. 1626).
  - Spécifiez le groupe de sous-réseaux DB par défaut. S'il s'agit de la première instance de base de données que vous créez dans cette région AWS, Amazon RDS créé le groupe de sous-réseau DB par défaut au moment de la création de l'instance de base de données.
- VPC défini par l'utilisateur– Si vous souhaitez spécifier un VPC défini par l'utilisateur lorsque vous créez une instance de base de données, tenez compte de ce qui suit :
  - Assurez-vous de créer un groupe de sécurité VPC autorisant les connexions de l'application ou du service à l'instance de base de données Amazon RDS contenant la base de données. Utilisez l'option API Amazon EC2 ou l'option Groupe de sécurité de la console VPC pour créer des groupes de sécurité VPC. Pour plus d'informations, consultez Étape 4 : Créer un groupe de sécurité VPC (p. 1626).
  - Le VPC doit respecter certaines exigences afin d'héberger des instances de bases de données. Il doit notamment comporter au moins deux sous-réseaux, dans deux zones de disponibilités distinctes. Pour plus d'informations, consultez VPC Amazon Virtual Private Cloud et Amazon RDS (p. 1610).
  - Assurez-vous de spécifier un groupe de sous-réseaux DB définissant les sous-réseaux de ce VPC pouvant être utilisés par l'instance de base de données. Pour plus d'informations, consultez la section Groupe de sous-réseau DB de Utilisation d'une instance de base de données dans un VPC (p. 1621).
- Aucun VPC – Si votre compte AWS ne possède pas de VPC par défaut et que vous ne spécifiez pas de VPC défini par l'utilisateur, créez un groupe de sécurité de base de données. Un groupe de sécurité de base de données autorise les connexions à partir d'appareils et d'instances Amazon RDS exécutant les applications ou les utilitaires qui accèdent aux bases de données dans l'instance de base de données. Pour plus d'informations, consultez Utilisation des groupes de sécurité DB (plateforme EC2-Classic) (p. 1596).

- Haute disponibilité : Avez-vous besoin de la prise en charge du basculement ? Sur Amazon RDS, un déploiement multi-AZ crée une instance de base de données principale et une instance de base de données de secours secondaire dans une autre zone de disponibilité pour la prise en charge du basculement. Nous recommandons les déploiements multi-AZ pour les charges de travail de production afin de maintenir une haute disponibilité. À des fins de développement et de test, vous pouvez utiliser un déploiement qui n'est pas multi-AZ. Pour plus d'informations, consultez Haute disponibilité (multi-AZ) pour Amazon RDS (p. 43).
- Stratégies IAM : Votre compte AWS comporte-t-il des stratégies accordant les autorisations nécessaires pour exécuter les opérations Amazon RDS ? Si vous vous connectez à AWS à l'aide des informations d'identification IAM, votre compte IAM doit disposer des stratégies IAM qui accordent les autorisations requises pour exécuter les opérations Amazon RDS. Pour plus d'informations, consultez Identity and Access Management dans Amazon RDS (p. 1536).
- Ports ouverts : Sur quel port TCP/IP votre base de données écoute-t-elle ? Dans certaines entreprises, le pare-feu peut bloquer les connexions vers le port par défaut de votre moteur de base de données. Si le pare-feu de votre entreprise bloque le port par défaut, choisissez un autre port pour la nouvelle instance de base de données. Lorsque vous créez une instance de base de données qui écoute sur un port spécifié par vos soins, vous pouvez changer de port en modifiant l'instance de base de données.
- Région AWS : Dans quelle région AWS souhaitez-vous créer votre base de données ? La proximité entre votre base de données et votre application ou le service Web service permet de réduire la latence du réseau.

- Sous-système de disque de base de données : Quels sont vos besoins en termes de stockage ? Amazon RDS propose trois types de stockage :
  - Magnétique (stockage standard)
  - Usage général (SSD)
  - IOPS provisionnées (PIOPS)

  Le stockage magnétique offre un stockage économique qui convient parfaitement aux applications avec des exigences en termes d'E/S modérées ou émises en rafales. Le stockage à usage général reposant sur SSD, également appelé gp2, fournit un accès plus rapide que le stockage sur disque. Le stockage IOPS provisionnées est conçu pour satisfaire les besoins des charges de travail gourmandes en E/S, notamment les charges de travail de base de données qui sont sensibles aux performances de stockage et à l'homogénéité du débit d'E/S. Pour plus d'informations sur le stockage Amazon RDS, consultez Stockage d'instance de base de données Amazon RDS (p. 30).

Lorsque vous disposez de toutes les informations nécessaires pour créer le groupe de sécurité et l'instance de base de données, passez à l'étape suivante.

Créer un groupe de sécurité qui autorise l'accès à votre instance de base de données dans votre VPC

Les groupes de sécurité VPC permettent l'accès aux instances de base de données dans un VPC. Ils font office de pare-feu pour l'instance de base de données associée, en contrôlant le trafic entrant et le trafic sortant au niveau de l'instance. Par défaut, les instances de base de données sont créées avec un pare-feu et un groupe de sécurité par défaut protégeant l'instance de base de données.

Avant de pouvoir vous connecter à votre instance de base de données, vous devez ajouter des règles à un groupe de sécurité qui vous permettent de vous connecter. Utilisez vos informations réseau et de configuration pour créer les règles autorisant l'accès à votre instance de base de données.

> **Note**
>
> Si votre instance de base de données héritée a été créée avant mars 2013 et qu'elle ne se trouve pas dans un VPC, il se peut qu'elle ne soit pas associée à des groupes de sécurité. Si votre instance de base de données a été créée après cette date, il se peut qu'elle se trouve dans un VPC par défaut.

Prenons l'exemple d'une application qui a accès à une base de données sur votre instance de base de données dans un VPC. Dans ce cas, vous devez ajouter une règle TCP personnalisée qui spécifie la plage de ports et les adresses IP utilisées par votre application pour accéder à la base de données. Si vous possédez une application sur une instance Amazon EC2, vous pouvez utiliser le groupe de sécurité qui est configuré pour l'instance Amazon EC2.

Pour créer un groupe de sécurité VPC

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le coin supérieur droit de la AWS Management Console, sélectionnez la région AWS dans laquelle vous souhaitez créer votre groupe de sécurité VPC et l'instance DB. Dans la liste des ressources Amazon VPC de cette région AWS, vous devez voir que vous possédez au moins un VPC et plusieurs sous-réseaux. Si ce n'est pas le cas, cela signifie que vous ne disposez pas de VPC par défaut dans cette région AWS.
3. Dans le volet de navigation, choisissez Groupes de sécurité.
4. Sélectionnez Create Security Group.

5. Dans la fenêtre Créer un groupe de sécurité, renseignez les valeurs Balise de nom, Nom du groupe et Description pour votre groupe de sécurité. Pour VPC, choisissez le VPC dans lequel vous souhaitez créer votre instance de base de données. Choisissez Yes, Create.
6. Le groupe de sécurité VPC que vous avez créé doit encore être sélectionné. Si tel n'est pas le cas, choisissez-le dans la liste. Le volet des détails situé en bas de la fenêtre de la console affiche les détails du groupe de sécurité, ainsi que des onglets pour utiliser les règles entrantes et sortantes. Choisissez l'onglet Règles entrantes.
7. Sous l'onglet Inbound Rules, choisissez Edit.
   a. Pour Type, choisissez Custom TCP Rule.
   b. Pour Plage de ports, saisissez le numéro du port à utiliser pour votre instance de base de données.
   c. Pour Source, choisissez un nom de groupe de sécurité ou tapez la plage d'adresses IP (valeur CIDR) à partir de laquelle vous accédez à l'instance. Si vous choisissez Mon IP, l'accès à l'instance de base de données est autorisé à partir de l'adresse IP détectée dans votre navigateur.
8. Choisissez Ajouter une autre règle si vous devez ajouter d'autres adresses IP ou des plages de ports différentes.
9. (Facultatif) Utilisez l'onglet Règles sortantes pour ajouter des règles pour le trafic sortant. Par défaut, tous les trafics sortant sont autorisés.

Vous pouvez utiliser le groupe de sécurité VPC que vous venez de créer comme groupe de sécurité pour votre instance de base de données lors de sa création. Si votre instance de base de données n'est pas destinée à être située dans un VPC, consultez Utilisation des groupes de sécurité DB (plateforme EC2-Classic) (p. 1596) pour créer un groupe de sécurité DB à utiliser lors de la création de votre instance de base de données.

> **Note**
>
> Si vous utilisez un VPC par défaut, un groupe de sous-réseaux par défaut couvrant l'ensemble des sous-réseaux du VPC a déjà été créé pour vous. Lorsque vous créez une instance de base de données, vous pouvez sélectionner le VPC par défaut et utiliser par défaut en regard de DB Subnet Group (Groupe de sous-réseaux de base de données).

Une fois que vous avez terminé la configuration, vous pouvez lancer une instance de base de données en utilisant votre configuration et votre groupe de sécurité. Pour plus d'informations sur la création d'une instance de base de données, consultez la documentation appropriée indiquée dans le tableau suivant.

Moteur de base de données	Documentation
MariaDB	Création d'une instance de base de données MariaDB et connexion à une base de données sur une instance de base de données MariaDB (p. 69)
Microsoft SQL Server	Création d'une instance de base de données Microsoft SQL Server et connexion à une instance de base de données (p. 76)
MySQL	Création d'une instance de base de données MySQL et connexion à une base de données sur une instance de base de données MySQL (p. 85)
Oracle	Création d'une instance de base de données Oracle et connexion à une base de données sur une instance de base de données Oracle (p. 93)
PostgreSQL	Création d'une instance de base de données PostgreSQL et connexion à une base de données sur une instance de base de données PostgreSQL (p. 99)

Note

Si vous ne parvenez pas à vous connecter à une instance de base de données après l'avoir créée, veuillez consulter les informations de dépannage dans Impossible de se connecter à l'instance de base de données Amazon RDS (p. 1639).

Mise en route avec Amazon RDS

Les exemples ci-dessous décrivent comment créer une instance de base de données et comment vous y connecter à l'aide d'Amazon Relational Database Service (Amazon RDS). Vous pouvez créer une instance de base de données qui utilise MariaDB, MySQL, Microsoft SQL Server, Oracle ou PostgreSQL.

> Important
>
> Avant de pouvoir créer une instance de base de données ou de vous y connecter, vous devez réaliser les tâches de la section Configuration pour Amazon RDS (p. 62).

La création d'une instance de base de données et la connexion à une base de données d'une instance est légèrement différente pour chacun des moteurs de bases de données. Choisissez l'un des moteurs de base de données suivants que vous souhaitez utiliser pour en savoir plus sur la création et la connexion à l'instance de base de données. Une fois que vous avez assuré la création de votre instance de base de données, et la connexion à cette dernière, des instructions sont fournies pour vous aider à supprimer l'instance de base de données.

Rubriques

- Création d'une instance de base de données MariaDB et connexion à une base de données sur une instance de base de données MariaDB (p. 69)
- Création d'une instance de base de données Microsoft SQL Server et connexion à une instance de base de données (p. 76)
- Création d'une instance de base de données MySQL et connexion à une base de données sur une instance de base de données MySQL (p. 85)
- Création d'une instance de base de données Oracle et connexion à une base de données sur une instance de base de données Oracle (p. 93)
- Création d'une instance de base de données PostgreSQL et connexion à une base de données sur une instance de base de données PostgreSQL (p. 99)
- Didacticiel : Créer un serveur web et une instance de base de données Amazon RDS (p. 109)

Création d'une instance de base de données MariaDB et connexion à une base de données sur une instance de base de données MariaDB

La manière la plus simple de créer une instance de base de données MariaDB consiste à utiliser la console Amazon RDS. Une fois que vous avez créé l'instance de base de données, vous pouvez utiliser des outils de ligne de commande, tels que mysql ou des outils graphiques standard, tels que HeidiSQL pour vous connecter à une base de données sur l'instance de base de données.

> Important
>
> Avant de pouvoir créer une instance de base de données ou de vous y connecter, vous devez réaliser les tâches de la section Configuration pour Amazon RDS (p. 62).

Rubriques

- Création d'une instance de base de données MariaDB (p. 70)
- Connexion à une base de données sur une instance de base de données exécutant le moteur de base de données MariaDB (p. 74)
- Suppression d'une instance DB (p. 76)

Création d'une instance de base de données MariaDB

La fondation de base d'Amazon RDS est l'instance de base de données. Il s'agit de l'environnement dans lequel vous exécutez vos bases de données MariaDB.

Console

Vous pouvez créer une instance de base de données exécutant MariaDB à l'aide d'AWS Management Console, avec l'option Easy Create (Création facile) activée ou désactivée. Lorsque l'option Easy Create (Création facile) est activée, vous spécifiez uniquement le type de moteur, la taille et l'identifiant d'instance de base de données. Easy Create (Création facile) utilise les paramètres par défaut pour les autres options de configuration. Lorsque l'option Easy Create (Création facile) est désactivée, vous spécifiez davantage d'options de configuration lors de la création d'une base de données, notamment en matière de disponibilité, de sécurité, de sauvegardes et de maintenance.

Dans cet exemple, vous utilisez Easy Create (Création facile) pour créer une instance de base de données exécutant le moteur de base de données MariaDB avec une classe d'instance de base de données db.t2.micro.

> **Note**
>
> Pour de plus amples informations sur la création d'instances de base de données avec l'option Easy Create (Création facile) désactivée, veuillez consulter Création d'une instance de base de données Amazon RDS (p. 146).

Pour créer une instance de base de données MariaDB avec l'option Easy Create (Création facile) activée

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le coin supérieur droit de la console Amazon RDS, choisissez la région AWS dans laquelle vous voulez créer l'instance de base de données.
3. Dans la panneau de navigation, choisissez Databases (Bases de données).
4. Choisissez Create database (Créer une base de données) et veillez à choisir Easy Create (Création facile).

5. Dans Configuration, choisissez MariaDB.
6. Pour DB instance size (Taille de l'instance de base de données), choisissez Free tier (Offre gratuite).
7. Pour DB instance identifier (Identifiant d'instance de base de données), saisissez un nom pour l'instance de base de données, ou conservez le nom par défaut.
8. Pour Master username (Identifiant principal), saisissez un nom pour l'utilisateur principal, ou conservez le nom par défaut.

   La page Create database (Créer une base de données) doit ressembler à l'image suivante.

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 conf configuration options can be changed database is created.

Configuration

Engine type Info

- Amazon Aurora
- MySQL
- MariaDB
- PostgreSQL
- Oracle
- Microsoft SQ

DB instance size

- Production
  db.r4.xlarge
  4 vCPUs
  30.5 GiB RAM
  500 GiB
- Dev/Test
  db.r4.large
  2 vCPUs
  15.25 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 cross all DB instances owned by your AWS account Region.

database-1

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1

9. Pour utiliser un mot de passe principal généré automatiquement pour l'instance de base de données, vérifiez que la case Auto generate a password (Générer un mot de passe automatiquement) est cochée.

   Pour entrer votre mot de passe principal, décochez la case Auto generate a password (Générer un mot de passe automatiquement), puis entrez le même mot de passe dans les champs Mot de passe principal et Confirmer le mot de passe.

10. (Facultatif) Ouvrez View default settings for Easy Create (Afficher les paramètres par défaut pour Création facile).

   Vous pouvez examiner les paramètres par défaut utilisés quand l'option Easy Create (Création facile) est activée. Si vous voulez modifier un ou plusieurs paramètres pendant la création de la base de données, choisissez Standard Create (Création standard) pour les définir. La colonne Editable after database creation (Modifiable après création de la base de données indique les options que vous pouvez modifier après la création de la base de données. Pour modifier un paramètre dont la valeur est No (Non) dans cette colonne, utilisez Standard Create (Création standard). Pour les paramètres dont la valeur est Yes (Oui) dans cette colonne, vous pouvez utiliser Standard Create (Création standard) ou modifier l'instance de base de données après l'avoir créée pour modifier ces paramètres.

11. Choisissez Create database (Créer une base de données).

   Si vous choisissez de générer un mot de passe automatiquement, le bouton View credential details (Afficher les informations d'identification) apparaît sur la page Databases (Bases de données).

   Pour afficher l'identifiant principal et le mot de passe pour l'instance de base de données, choisissez View credential details (Afficher les informations d'identification).

   Pour vous connecter à l'instance de base de données en tant qu'utilisateur principal, utilisez l'identifiant et le mot de passe affichés.

   > **Important**
   >
   > Vous ne pourrez pas afficher le mot de passe de l'utilisateur principal de nouveau. Si vous ne l'enregistrez pas, il sera peut-être nécessaire de le modifier. Si vous devez changer le mot de passe de l'utilisateur principal une fois l'instance de base de données disponible, vous pouvez le faire en modifiant l'instance de base de données. Pour de plus amples informations

sur la modification d'une instance de base de données, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

12. Pour Databases (Bases de données), choisissez le nom de la nouvelle instance de base de données MariaDB.

    Sur la console RDS, les détails de la nouvelle instance de base de données s'affichent. L'instance de base de données a le statut creating (création en cours) jusqu'à ce qu'elle soit créée et prête à l'emploi. Lorsque l'état devient available (disponible), vous pouvez vous connecter à l'instance de base de données. En fonction de la quantité de stockage et de la classe d'instance de base de données, la mise à disposition de la nouvelle instance peut prendre jusqu'à 20 minutes.

Connexion à une base de données sur une instance de base de données exécutant le moteur de base de données MariaDB

Une fois qu'Amazon RDS a provisionné votre instance de base de données, vous pouvez utiliser n'importe quelle application cliente SQL standard pour vous connecter à une base de données sur l'instance de base de données. Dans cet exemple, vous vous connectez à une base de données sur une instance de base de données MariaDB en utilisant l'outil de ligne de commande mysql. HeidiSQL est une application basée sur l'interface utilisateur graphique que vous pouvez utiliser pour la connexion. Pour en savoir plus, consultez la page Télécharger HeidiSQL. Pour plus d'informations sur l'utilisation de MariaDB, consultez la documentation MariaDB.

Pour vous connecter à une base de données sur une instance de base de données en utilisant l'outil de ligne de commande **`mysql`**

1. Trouvez le point de terminaison (nom DNS) et le numéro de port pour votre instance de base de données.

   a. Ouvrez la console RDS et choisissez Bases de données pour afficher une liste de vos instances de bases de données.

   b. Choisissez le nom de l'instance de base de données MariaDB pour afficher ses détails.

   c. Dans l'onglet Connectivity & security (Connectivité et sécurité), copiez le point de terminaison. Notez également le numéro du port. Vous avez besoin du point de terminaison et du numéro de port pour vous connecter à l'instance de base de données.

2. Saisissez la commande suivante dans une invite de commande sur un ordinateur client afin de vous connecter à une base de données sur une instance de base de données MariaDB. Remplacez le nom DNS (point de terminaison) de votre instance de base de données pour *<endpoint>*, l'identifiant principal que vous avez utilisé pour *<mymasteruser>*, et fournissez le mot de passe principal que vous avez utilisé lorsqu'un mot de passe vous a été demandé.

```
PROMPT> mysql -h <endpoint> -P 3306 -u <mymasteruser>  -p
```

Après avoir entré le mot de passe pour l'utilisateur, le résultat suivant devrait normalement s'afficher.

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 272
Server version: 5.5.5-10.0.17-MariaDB-log MariaDB Server

Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.
```

```
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql >
```

Pour de plus amples informations sur la connexion à une instance de base de données MariaDB, veuillez consulter Connexion à une instance de base de données exécutant le moteur de base de données MariaDB (p. 556). Pour de plus amples informations sur les problèmes de connexion, veuillez consulter Impossible de se connecter à l'instance de base de données Amazon RDS (p. 1639).

Suppression d'une instance DB

Une fois que vous êtes connecté à l'exemple d'instance de base de données que vous avez créée, vous devez supprimer l'instance de base de données afin qu'elle ne vous soit plus facturée.

Pour supprimer une instance de base de données sans instantané de base de données final

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez l'instance de base de données que vous voulez supprimer.
4. Pour Actions, choisissez Supprimer.
5. Pour Créer un instantané final ?, choisissez Non, puis confirmez.
6. Sélectionnez Delete.

Création d'une instance de base de données Microsoft SQL Server et connexion à une instance de base de données

La fondation de base d'Amazon RDS est l'instance de base de données. Votre instance de base de données Amazon RDS est similaire à votre serveur Microsoft SQL Server sur site. Après avoir créé votre instance de base de données SQL Server, vous pouvez lui ajouter une ou plusieurs bases de données personnalisées.

> Important
>
> Vous devez avoir un compte AWS avant de créer une instance de base de données. Si vous n'avez pas de compte AWS, ouvrez https://aws.amazon.com/, puis choisissez Créer un compte AWS.

Dans cette rubrique, vous allez créer un exemple d'instance de base de données SQL Server. Vous allez ensuite vous connecter à l'instance de base de données et exécuter une requête simple. Pour finir, vous allez supprimer l'exemple d'instance de base de données.

Création d'un exemple d'instance de base de données SQL Server

L'instance de base de données est l'environnement dans lequel vous exécutez vos bases de données Microsoft SQL Server.

Console

Vous pouvez créer une instance de base de données exécutant Microsoft SQL Server à l'aide d'AWS Management Console, avec l'option Easy Create (Création facile) activée ou désactivée. Lorsque l'option Easy Create (Création facile) est activée, vous spécifiez uniquement le type de moteur, la taille et l'identifiant d'instance de base de données. Easy Create (Création facile) utilise les paramètres par défaut pour les autres options de configuration. Lorsque l'option Easy Create (Création facile) est désactivée, vous spécifiez davantage d'options de configuration lors de la création d'une base de données, notamment en matière de disponibilité, de sécurité, de sauvegardes et de maintenance.

Dans cet exemple, vous utilisez Easy Create (Création facile) pour créer une instance de base de données exécutant le moteur de base de données Microsoft SQL Server avec une classe d'instance de base de données db.t2.micro.

> Note
>
> Pour de plus amples informations sur la création d'instances de base de données avec l'option Easy Create (Création facile) désactivée, veuillez consulter Création d'une instance de base de données Amazon RDS (p. 146).

Pour créer une instance de base de données Microsoft SQL Server avec l'option Easy Create (Création facile) activée

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le coin supérieur droit de la console Amazon RDS, choisissez la région AWS dans laquelle vous voulez créer l'instance de base de données.
3. Dans la panneau de navigation, choisissez Databases (Bases de données).
4. Choisissez Create database (Créer une base de données) et veillez à choisir Easy Create (Création facile).

5. Dans Configuration, choisissez Microsoft SQL Server.
6. Pour DB instance size (Taille de l'instance de base de données), choisissez Free tier (Offre gratuite).
7. Pour DB instance identifier (Identifiant d'instance de base de données), saisissez un nom pour l'instance de base de données, ou conservez le nom par défaut.
8. Pour Master username (Identifiant principal), saisissez un nom pour l'utilisateur principal, ou conservez le nom par défaut.

   La page Create database (Créer une base de données) doit ressembler à l'image suivante.

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 con
  configuration options can be change
  database is created.

Configuration

Engine type Info

- Amazon Aurora
- MySQL
- MariaDB
- PostgreSQL
- Oracle
- Microsoft S

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
- 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 cross all DB instances owned by your AWS account
Region.

database-1

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1

9. Pour utiliser un mot de passe principal généré automatiquement pour l'instance de base de données, vérifiez que la case Auto generate a password (Générer un mot de passe automatiquement) est cochée.

   Pour entrer votre mot de passe principal, décochez la case Auto generate a password (Générer un mot de passe automatiquement), puis entrez le même mot de passe dans les champs Mot de passe principal et Confirmer le mot de passe.

10. (Facultatif) Ouvrez View default settings for Easy Create (Afficher les paramètres par défaut pour Création facile).

   Vous pouvez examiner les paramètres par défaut utilisés quand l'option Easy Create (Création facile) est activée. Si vous voulez modifier un ou plusieurs paramètres pendant la création de la base de données, choisissez Standard Create (Création standard) pour les définir. La colonne Editable after database creation (Modifiable après création de la base de données indique les options que vous pouvez modifier après la création de la base de données. Pour modifier un paramètre dont la valeur est No (Non) dans cette colonne, utilisez Standard Create (Création standard). Pour les paramètres dont la valeur est Yes (Oui) dans cette colonne, vous pouvez utiliser Standard Create (Création standard) ou modifier l'instance de base de données après l'avoir créée pour modifier ces paramètres.

11. Choisissez Create database (Créer une base de données).

   Si vous choisissez de générer un mot de passe automatiquement, le bouton View credential details (Afficher les informations d'identification) apparaît sur la page Databases (Bases de données).

   Pour afficher l'identifiant principal et le mot de passe pour l'instance de base de données, choisissez View credential details (Afficher les informations d'identification).

   Pour vous connecter à l'instance de base de données en tant qu'utilisateur principal, utilisez l'identifiant et le mot de passe affichés.

   > **Important**
   >
   > Vous ne pourrez pas afficher le mot de passe de l'utilisateur principal de nouveau. Si vous ne l'enregistrez pas, il sera peut-être nécessaire de le modifier. Si vous devez changer le mot de passe de l'utilisateur principal une fois l'instance de base de données disponible, vous pouvez le faire en modifiant l'instance de base de données. Pour de plus amples informations

sur la modification d'une instance de base de données, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

12. Pour Databases (Bases de données), choisissez le nom de la nouvelle instance de base de données Microsoft SQL Server.

    Sur la console RDS, les détails de la nouvelle instance de base de données s'affichent. L'instance de base de données a le statut creating (création en cours) jusqu'à ce qu'elle soit créée et prête à l'emploi. Lorsque l'état devient available (disponible), vous pouvez vous connecter à l'instance de base de données. En fonction de la quantité de stockage et de la classe d'instance de base de données, la mise à disposition de la nouvelle instance peut prendre jusqu'à 20 minutes.

Connexion à votre exemple d'instance de base de données SQL Server

Au cours de cette procédure, vous vous connectez à votre exemple d'instance de base de données à l'aide de Microsoft SQL Server Management Studio (SSMS).

Avant que vous ne commenciez, votre base de données doit avoir le statut Available (Disponible). Si son statut est Creating (En cours de création) ou Backup-up (Sauvegarde), attendez que celui-ci devienne Available (Disponible). Le statut se met à jour sans que vous ayez besoin d'actualiser la page. Ce processus peut prendre jusqu'à 20 minutes.

Vérifiez également que SSMS est installé. Vous pouvez également vous connecter à SQL Server sur RDS avec d'autres outils tels qu'un module complémentaire pour votre environnement de développement ou d'autres outils de base de données. Toutefois, ce didacticiel couvre uniquement l'utilisation de SSMS. Pour télécharger une version autonome de SSMS, consultez Download SQL Server Management Studio (SSMS) dans la documentation Microsoft.

Pour vous connecter à une instance de base de données à l'aide de SSMS

1. Trouvez le numéro de port et le nom DNS pour votre instance de base de données.

   a. Ouvrez la console RDS et choisissez Bases de données pour afficher une liste de vos instances de bases de données.

   b. Survolez le nom sample-instance, qui apparaît en bleu, avec le curseur de votre souris. Le curseur de la souris se transforme alors en icône de sélection (par exemple, une main avec un doigt pointé). Le nom de l'instance de base de données est également souligné.

      Cliquez sur le nom de l'instance de base de données pour la sélectionner. L'écran affiche alors les informations sur l'instance de base de données que vous avez choisie.

   c. Dans l'onglet Connectivity (Connectivité), qui s'ouvre par défaut, copiez le point de terminaison. Le Endpoint (Point de terminaison) ressemble à ce qui suit : `sample-instance.abc2defghije.us-west-2.rds.amazonaws.com`. Notez également le numéro de port. Le port par défaut pour SQL Server est 1433. Si le vôtre est différent, notez-le.

2. Démarrez SQL Server Management Studio.

   La boîte de dialogue Connect to Server (Se connecter à un serveur) s'affiche.

3. Fournissez les informations relatives à votre exemple d'instance de base de données.

   a. Pour Server type (Type de serveur), choisissez Database Engine (Moteur de base de données).

   b. Pour Server name (Nom du serveur), entrez le nom DNS, suivi d'une virgule et du numéro de port (le port par défaut est 1433). Par exemple, le nom du serveur doit se présenter comme suit.

   ```
   sample-instance.abc2defghije.us-west-2.rds.amazonaws.com,1433
   ```

   c. Pour Authentication (Authentification), choisissez SQL Server Authentication (Authentification SQL Server).

   d. Pour Login (Connexion), saisissez le nom d'utilisateur que vous avez choisi d'utiliser pour votre exemple d'instance de base de données. Ce nom est également appelé « nom d'utilisateur principal ».

   e. Pour Password (Mot de passe), saisissez le mot de passe que vous avez choisi auparavant pour votre exemple d'instance de base de données. Ce nom est également appelé « mot de passe d'utilisateur principal ».

4. Choisissez Connect (Se connecter).

   Après quelques instants, SSMS se connecte à votre instance de base de données.

   Si vous ne pouvez pas vous connecter à votre instance de base de données, consultez Résolution des problèmes de connexion à votre instance de base de données SQL Server (p. 624).

Exploration de votre exemple d'instance de base de données SQL Server

Cette procédure est la continuation de la procédure précédente et permet d'explorer votre exemple d'instance de base de données à l'aide de Microsoft SQL Server Management Studio (SSMS).

Pour explorer une instance de base de données à l'aide de SSMS

1. Votre instance de base de données SQL Server est fournie avec les bases de données système intégrées standard de SQL Server (master, model, msdb et tempdb). Pour explorer les bases de données système, effectuez les opérations suivantes :

   a. Dans SSMS, dans le menu View (Afficher), choisissez Object Explorer (Navigateur d'objet).

   b. Développez votre instance de base de données, développez Databases (Bases de données), puis System Databases (Bases de données système) comme indiqué ci-dessous.

2. Votre instance de base de données SQL Server est également accompagnée d'une base de données nommée `rdsadmin`. Amazon RDS utilise cette base de données pour stocker les objets dont il se sert pour gérer votre base de données. La base de données `rdsadmin` inclut également des procédures stockées que vous pouvez exécuter pour effectuer des tâches avancées.
3. Vous pouvez maintenant commencer à créer vos propres bases de données et à exécuter des requêtes sur votre instance de base de données et vos bases de données comme d'habitude. Pour exécuter une requête de test sur votre exemple d'instance de base de données, procédez comme suit :

   a. Dans SSMS, dans le menu Fichier, pointez sur Nouveau, puis choisissez Query with Current Connection (Requête avec la connexion actuelle).

   b. Entrez la requête SQL suivante.

   ```
   select @@VERSION
   ```

   c. Exécutez la requête. SSMS renvoie la version SQL Server de votre instance de base de données Amazon RDS.

Suppression de votre exemple d'instance de base de données

Une fois que vous avez fini d'explorer l'exemple d'instance de base de données que vous avez créée, vous devez supprimer l'instance de base de données afin qu'elle ne vous soit plus facturée.

Pour supprimer une instance de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez le bouton en regard de sample-instance (ou du nom de votre exemple d'instance de données).
4. Choisissez Delete (Supprimer) à partir de Actions ci-dessus (à gauche du bouton orange Create database [Créer une base de données]).

   Si le message This database has deletion protection option enabled (L'option de protection contre la suppression est activée pour cette base de données), procédez comme suit :

   - Sélectionnez Modify (Modifier).
   - Sur la carte Deletion protection (Protection contre la suppression) (au bas de la page), décochez la case Enable deletion protection (Activer la protection contre la suppression). Choisissez ensuite Continue (Continuer).

- Sur la carte Scheduling of modifications (Planification des modifications), choisissez Apply immediately (Appliquer immédiatement). Choisissez ensuite Modify DB Instance (Modifier l'instance de base de données).
- Faites une nouvelle tentative de suppression de l'instance en choisissant Delete (Supprimer) à partir du menu Actions.

5. Décochez la case pour Create final snapshot (Créer un instantané final). Il ne s'agit pas d'une base de données de production, vous n'avez donc pas besoin d'en enregistrer une copie.
6. Vérifiez que vous avez sélectionné la bonne base de données à supprimer. Le nom « sample-instance » s'affiche dans le titre de l'écran : Delete sample-instance instance? (Supprimer l'instance sample-instance ?)

   Si vous ne reconnaissez pas le nom de votre exemple d'instance dans le titre, choisissez Cancel (Annuler) et recommencez.
7. Pour confirmer que vous souhaitez supprimer définitivement la base de données dont le nom figure dans le titre de cet écran, procédez comme suit :

   - Cochez la case pour confirmer : I acknowledge that upon instance deletion, automated backups, including system snapshots and point-in-time recovery, will no longer be available (Je reconnais qu'en cas de suppression d'une instance, les sauvegardes automatisées, y compris les instantanés système et les restaurations ponctuelles, ne seront plus disponibles).
   - Entrez « **`delete me`** » dans la case To confirm deletion, type delete me into the field (Pour confirmer la suppression, entrez « delete me » dans le champ).
   - Sélectionnez Delete (Supprimer). Cette action ne peut pas être annulée.

   La base de données affiche le statutDeleting (En cours de suppression) jusqu'à ce que la suppression soit terminée.

Création d'une instance de base de données MySQL et connexion à une base de données sur une instance de base de données MySQL

La manière la plus simple de créer une instance de base de données consiste à utiliser la AWS Management Console. Une fois que vous avez créé l'instance de base de données, vous pouvez utiliser des utilitaires MySQL standard tels que MySQL Workbench pour vous connecter à une base de données sur l'instance de base de données.

> **Important**
>
> Avant de pouvoir créer une instance de base de données ou de vous y connecter, vous devez réaliser les tâches de la section Configuration pour Amazon RDS (p. 62).

Rubriques

- Création d'une instance de base de données MySQL (p. 86)
- Connexion à une base de données sur une instance de base de données exécutant le moteur de base de données MySQL (p. 90)
- Suppression d'une instance DB (p. 92)

Création d'une instance de base de données MySQL

La fondation de base d'Amazon RDS est l'instance de base de données. Il s'agit de l'environnement dans lequel vous exécutez vos bases de données MySQL.

Console

Vous pouvez créer une instance de base de données exécutant MySQL à l'aide d'AWS Management Console, avec l'option Easy Create (Création facile) activée ou désactivée. Lorsque l'option Easy Create (Création facile) est activée, vous spécifiez uniquement le type de moteur, la taille et l'identifiant d'instance de base de données. Easy Create (Création facile) utilise les paramètres par défaut pour les autres options de configuration. Lorsque l'option Easy Create (Création facile) est désactivée, vous spécifiez davantage d'options de configuration lors de la création d'une base de données, notamment en matière de disponibilité, de sécurité, de sauvegardes et de maintenance.

Dans cet exemple, vous utilisez Easy Create (Création facile) pour créer une instance de base de données exécutant le moteur de base de données MySQL avec une classe d'instance de base de données db.t2.micro.

> **Note**
>
> Pour de plus amples informations sur la création d'instances de base de données avec l'option Easy Create (Création facile) désactivée, veuillez consulter Création d'une instance de base de données Amazon RDS (p. 146).

Pour créer une instance de base de données MySQL avec l'option Easy Create (Création facile) activée

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le coin supérieur droit de la console Amazon RDS, choisissez la région AWS dans laquelle vous voulez créer l'instance de base de données.
3. Dans la panneau de navigation, choisissez Databases (Bases de données).
4. Choisissez Create database (Créer une base de données) et veillez à choisir Easy Create (Création facile).

5. Dans Configuration, choisissez MySQL.
6. Pour DB instance size (Taille de l'instance de base de données), choisissez Free tier (Offre gratuite).
7. Pour DB instance identifier (Identifiant d'instance de base de données), saisissez un nom pour l'instance de base de données, ou conservez le nom par défaut.
8. Pour Master username (Identifiant principal), saisissez un nom pour l'utilisateur principal, ou conservez le nom par défaut.

   La page Create database (Créer une base de données) doit ressembler à l'image suivante.

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 con configuration options can be change database is created.

Configuration

Engine type Info

- Amazon Aurora
- MySQL
- MariaDB
- PostgreSQL
- Oracle
- Microsoft S

DB instance size

- Production
  db.r5.xlarge
  4 vCPUs
  32 GiB RAM
  500 GiB
- Dev/Test
  db.r5.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 cross all DB instances owned by your AWS accoun Region.

database-1

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1

9. Pour utiliser un mot de passe principal généré automatiquement pour l'instance de base de données, activez la fonction Auto generate a password (Générer un mot de passe automatiquement).

   Pour entrer votre mot de passe principal, désactivez la fonction Auto generate a password (Générer un mot de passe automatiquement), puis entrez un mot de passe identique dans les champs Mot de passe principal et Confirmer le mot de passe.

10. (Facultatif) Ouvrez View default settings for Easy Create (Afficher les paramètres par défaut pour Création facile).

    Vous pouvez examiner les paramètres par défaut utilisés quand l'option Easy Create (Création facile) est activée. Si vous voulez modifier un ou plusieurs paramètres pendant la création de la base de données, choisissez Standard Create (Création standard) pour les définir. La colonne Editable after database creation (Modifiable après création de la base de données indique les options que vous pouvez modifier après la création de la base de données. Pour modifier un paramètre dont la valeur est No (Non) dans cette colonne, utilisez Standard Create (Création standard). Pour les paramètres associés à la valeur Yes (Oui) dans cette colonne, vous pouvez utiliser Standard Create (Création standard) ou modifier l'instance de base de données après l'avoir créée pour modifier ces paramètres.

11. Choisissez Create database (Créer une base de données).

    Si vous choisissez de générer un mot de passe automatiquement, le bouton View credential details (Afficher les informations d'identification) sur la page Databases (Bases de données).

    Pour afficher l'identifiant principal et le mot de passe pour l'instance de base de données, choisissez View credential details (Afficher les informations d'identification).

    Vous pouvez utiliser l'identifiant et le mot de passe affichés pour vous connecter à l'instance de base de données en tant qu'utilisateur principal.

    > **Important**
    >
    > Vous ne pourrez pas afficher le mot de passe de l'utilisateur principal de nouveau. Si vous ne l'enregistrez pas, il sera peut-être nécessaire de le modifier. Si vous devez changer le mot de passe de l'utilisateur principal une fois l'instance de base de données disponible, vous pouvez le faire en modifiant l'instance de base de données. Pour de plus amples informations sur la modification d'une instance de base de données, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

12. Dans la liste Databases (Bases de données), choisissez le nom de la nouvelle instance de base de données MySQL.

    Sur la console RDS, les détails de la nouvelle instance de base de données s'affichent. L'instance de base de données a le statut creating (création en cours) jusqu'à ce qu'elle soit créée et prête à l'emploi. Lorsque l'état devient available (disponible), vous pouvez vous connecter à l'instance de base de données. En fonction de la quantité de stockage et de la classe d'instance de base de données, la mise à disposition de la nouvelle instance peut prendre jusqu'à 20 minutes.

Connexion à une base de données sur une instance de base de données exécutant le moteur de base de données MySQL

Une fois qu'Amazon RDS a provisionné votre instance de base de données, vous pouvez utiliser n'importe quelle application cliente SQL standard pour vous connecter à une base de données sur l'instance de base de données. Dans cet exemple, vous vous connectez à une base de données sur une instance de base de données MySQL en utilisant des commandes de surveillance MySQL. Vous pouvez utiliser MySQL Workbench comme application basée sur la GUI pour la connexion. Pour plus d'informations, accédez à la page Download MySQL Workbench (Télécharger MySQL Workbench). Pour plus d'informations sur l'utilisation de MySQL, consultez la documentation MySQL. Pour de plus amples informations sur l'installation de MySQL (y compris le client MySQL), veuillez consulter Installing and Upgrading MySQL.

Pour vous connecter à une base de données sur une instance de base de données en utilisant la surveillance MySQL

1. Trouvez le point de terminaison (nom DNS) et le numéro de port pour votre instance de base de données.

   a. Ouvrez la console RDS et choisissez Bases de données pour afficher une liste de vos instances de bases de données.

   b. Choisissez le nom de l'instance de base de données MySQL pour afficher ses détails.

   c. Dans l'onglet Connectivity & security (Connectivité et sécurité), copiez le point de terminaison. Notez également le numéro du port. Vous avez besoin du point de terminaison et du numéro de port pour vous connecter à l'instance de base de données.

2. Téléchargez un client SQL que vous pouvez utiliser pour vous connecter à l'instance de base de données.

   Vous pouvez vous connecter à une instance de base de données MySQL Amazon RDS en utilisant des outils tels que l'utilitaire de ligne de commande MySQL. Pour de plus amples informations sur l'utilisation du client MySQL, veuillez consulter mysql - The MySQL Command-Line Client dans la documentation MySQL. MySQL Workbench est une application basée sur l'interface utilisateur graphique que vous pouvez utiliser pour la connexion. Pour plus d'informations, consultez la page Télécharger MySQL Workbench.

3. Connectez-vous à une base de données sur une instance de base de données MySQL. Par exemple, saisissez la commande suivante dans une invite de commande sur un ordinateur client afin de vous connecter à une base de données sur une instance de base de données MySQL en utilisant le client MySQL. Remplacez le nom DNS de votre instance de base de données pour `<endpoint>`, le nom d'utilisateur principal que vous avez utilisé pour `<mymasteruser>` et fournissez le mot de passe principal que vous avez utilisé lorsqu'un mot de passe vous a été demandé.

```
PROMPT> mysql -h <endpoint> -P 3306 -u <mymasteruser> -p
```

Après avoir entré le mot de passe pour l'utilisateur, le résultat suivant devrait normalement s'afficher.

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 350
Server version: 5.6.40-log MySQL Community Server (GPL)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

Si vous ne pouvez pas vous connecter à votre instance de base de données MySQL, deux causes courantes d'échec de connexion à une nouvelle instance de base de données sont :

- L'instance de base de données a été créée grâce à un groupe de sécurité qui interdit les connexions depuis l'appareil ou l'instance Amazon EC2 où l'application ou l'utilitaire MySQL s'exécute. Si l'instance de base de données a été créée à l'intérieur d'un VPC, elle doit avoir un groupe de sécurité VPC qui autorise les connexions. Si l'instance de base de données a été créée à l'extérieur d'un VPC, elle doit avoir un groupe de sécurité de bases de données qui autorise les connexions. Pour plus d'informations, consultez VPC Amazon Virtual Private Cloud et Amazon RDS (p. 1610).
- L'instance de base de données a été créée à l'aide du port par défaut 3306, et votre entreprise dispose de règles de pare-feu bloquant les connexions à ce port depuis les appareils de votre réseau d'entreprise. Pour corriger le problème, recréez l'instance avec un port différent.

Pour plus d'informations sur la connexion à votre instance de base de données MySQL, consultez Connexion à une instance de base de données exécutant le moteur de base de données MySQL (p. 793). Pour de plus amples informations sur les problèmes de connexion, veuillez consulter Impossible de se connecter à l'instance de base de données Amazon RDS (p. 1639).

Suppression d'une instance DB

Une fois que vous êtes connecté à l'exemple d'instance de base de données que vous avez créée, vous devez supprimer l'instance de base de données afin qu'elle ne vous soit plus facturée.

Pour supprimer une instance de base de données sans instantané de base de données final

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez l'instance de base de données que vous souhaitez supprimer.
4. Pour Actions, choisissez Supprimer.
5. Pour Créer un instantané final ?, choisissez Non, puis confirmez.
6. Sélectionnez Delete.

Création d'une instance de base de données Oracle et connexion à une base de données sur une instance de base de données Oracle

La fondation de base d'Amazon RDS est l'instance de base de données. Votre instance de base de données Amazon RDS est similaire à votre base de données Oracle sur site.

> **Important**
>
> Vous devez avoir un compte AWS avant de créer une instance de base de données. Si vous n'avez pas de compte AWS, ouvrez https://aws.amazon.com/, puis choisissez Créer un compte AWS.

Dans cette rubrique, vous allez créer un exemple d'instance de base de données Oracle. Vous allez ensuite vous connecter à l'instance de base de données et exécuter une requête simple. Pour finir, vous allez supprimer l'exemple d'instance de base de données.

Création d'un exemple d'instance de base de données Oracle

Il s'agit de l'instance de base de données dans laquelle vous exécutez vos bases de données Oracle.

Console

Vous pouvez créer une instance de base de données exécutant Oracle à l'aide d'AWS Management Console, avec l'option Easy Create (Création facile) activée ou désactivée. Lorsque l'option Easy Create (Création facile) est activée, vous spécifiez uniquement le type de moteur, la taille et l'identifiant d'instance de base de données. Easy Create (Création facile) utilise les paramètres par défaut pour les autres options de configuration. Lorsque l'option Easy Create (Création facile) est désactivée, vous spécifiez davantage d'options de configuration lors de la création d'une base de données, notamment en matière de disponibilité, de sécurité, de sauvegardes et de maintenance.

Dans cet exemple, vous utilisez Easy Create (Création facile) pour créer une instance de base de données exécutant le moteur de base de données Oracle avec une classe d'instance de base de données db.t2.micro.

> **Note**
>
> Pour de plus amples informations sur la création d'instances de base de données avec l'option Easy Create (Création facile) désactivée, veuillez consulter Création d'une instance de base de données Amazon RDS (p. 146).

Pour créer une instance de base de données Oracle avec l'option Easy Create (Création facile) activée

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le coin supérieur droit de la console Amazon RDS, choisissez la région AWS dans laquelle vous voulez créer l'instance de base de données.
3. Dans la panneau de navigation, choisissez Databases (Bases de données).
4. Choisissez Create database (Créer une base de données) et veillez à choisir Easy Create (Création facile).

5. Dans Configuration, choisissez Oracle.
6. Pour DB instance size (Taille de l'instance de base de données), choisissez Free tier (Offre gratuite). Si Free tier (Offre gratuite) n'est pas disponible, choisissez Dev/Test (Développement/Test).
7. Pour Identifiant de l'instance DB, entrez un nom pour l'instance de base de données ou conservez le nom par défaut.
8. Pour Master username (Identifiant principal), saisissez un nom pour l'utilisateur principal, ou conservez le nom par défaut.

   La page Create database (Créer une base de données) doit ressembler à l'image suivante.

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 conf
  configuration options can be change
  database is created.

Configuration

Engine type Info

- Amazon Aurora
- MySQL
- MariaDB
- PostgreSQL
- Oracle
- Microsoft SQ

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 cross all DB instances owned by your AWS account
Region.

database-1

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1
characters or hyphens (1 to 15 for SQL Server). First character must be a letter. Can't contain two consecutive hy

9. Pour utiliser un mot de passe principal généré automatiquement pour l'instance de base de données, vérifiez que la case Auto generate a password (Générer un mot de passe automatiquement) est cochée.

   Pour entrer votre mot de passe principal, décochez la case Auto generate a password (Générer un mot de passe automatiquement), puis entrez le même mot de passe dans les champs Mot de passe principal et Confirmer le mot de passe.

10. (Facultatif) Ouvrez View default settings for Easy Create (Afficher les paramètres par défaut pour Création facile).

   Vous pouvez examiner les paramètres par défaut utilisés quand l'option Easy Create (Création facile) est activée. Si vous voulez modifier un ou plusieurs paramètres pendant la création de la base de données, choisissez Standard Create (Création standard) pour les définir. La colonne Editable after database creation (Modifiable après création de la base de données indique les options que vous pouvez modifier après la création de la base de données. Pour modifier un paramètre dont la valeur est No (Non) dans cette colonne, utilisez Standard Create (Création standard). Pour les paramètres dont la valeur est Yes (Oui) dans cette colonne, vous pouvez utiliser Standard Create (Création standard) ou modifier l'instance de base de données après l'avoir créée pour modifier ces paramètres.

11. Choisissez Create database (Créer une base de données).

   Si vous avez utilisé un mot de passe généré automatiquement, le bouton View credential details (Afficher les informations d'identification) apparaît sur la page Databases (Bases de données).

   Pour afficher l'identifiant principal et le mot de passe pour l'instance de base de données, choisissez View credential details (Afficher les informations d'identification).

   Pour vous connecter à l'instance de base de données en tant qu'utilisateur principal, utilisez l'identifiant et le mot de passe affichés.

   > **Important**
   >
   > >Vous ne pourrez pas afficher le mot de passe de l'utilisateur principal de nouveau. Si vous ne l'enregistrez pas, il sera peut-être nécessaire de le modifier. Si vous devez changer le mot de passe de l'utilisateur principal une fois l'instance de base de données disponible, vous pouvez le faire en modifiant l'instance de base de données. Pour de plus amples informations

sur la modification d'une instance de base de données, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

12. Pour Databases (Bases de données), choisissez le nom de la nouvelle instance de base de données Oracle.

    Sur la console RDS, les détails de la nouvelle instance de base de données s'affichent. L'instance de base de données a le statut creating (création en cours) jusqu'à ce qu'elle soit créée et prête à l'emploi. Lorsque l'état devient available (disponible), vous pouvez vous connecter à l'instance de base de données. En fonction de la quantité de stockage et de la classe d'instance de base de données, la mise à disposition de la nouvelle instance peut prendre jusqu'à 20 minutes.

Connexion à votre exemple d'instance de base de données Oracle

Après qu'Amazon RDS a provisionné votre instance de base de données, vous pouvez utiliser n'importe quelle application cliente SQL standard pour vous connecter à l'instance de base de données. Au cours de cette procédure, vous vous connectez à votre exemple d'instance de base de données en utilisant l'utilitaire de ligne de commande Oracle sqlplus. Pour télécharger une version autonome de cet utilitaire, consultez SQL*Plus User's Guide and Reference (Guide et référence de l'utilisateur SQL*Plus).

Se connecter à une instance de base de données à l'aide de SQL*Plus

1. Trouvez le point de terminaison (nom DNS) et le numéro de port pour votre instance de base de données.

   a. Ouvrez la console RDS et choisissez Bases de données pour afficher une liste de vos instances de bases de données.

   b. Choisissez le nom de l'instance de base de données Oracle pour afficher ses détails.

   c. Dans l'onglet Connectivity & security (Connectivité et sécurité), copiez le point de terminaison. Notez également le numéro du port. Vous avez besoin du point de terminaison et du numéro de port pour vous connecter à l'instance de base de données.

2. Saisissez la commande suivante sur une ligne à partir d'une invite de commande pour vous connecter à votre instance de bases de données à l'aide de l'utilitaire sqlplus. La valeur `Host` correspond au point de terminaison de l'instance de base de données et la valeur `Port` est le port que vous avez affecté à cette instance. La valeur `SID` pour Oracle est le nom de la base de données de l'instance de base de données que vous avez spécifié lors de la création de l'instance de base de données, pas le nom de l'instance de base de données.

```
PROMPT>sqlplus 'mydbusr@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=endpoint)(PORT=1521))
(CONNECT_DATA=(SID=ORCL)))'
```

Vous devez visualiser des résultats similaires à ce qui suit.

```
SQL*Plus: Release 11.1.0.7.0 - Production on Wed May 25 15:13:59 2011

SQL>
```

Pour de plus amples informations sur la connexion à l'instance de base de données, veuillez consulter Connexion à une instance de base de données Oracle (p. 961). Pour de plus amples informations sur les problèmes de connexion, veuillez consulter Impossible de se connecter à l'instance de base de données Amazon RDS (p. 1639).

Suppression de votre exemple d'instance de base de données

Une fois que vous avez fini d'explorer l'exemple d'instance de base de données que vous avez créée, vous devez supprimer l'instance de base de données afin qu'elle ne vous soit plus facturée.

Pour supprimer une instance de base de données sans instantané de base de données final

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez l'instance de base de données que vous souhaitez supprimer.
4. Pour Actions, choisissez Supprimer.
5. Pour Créer un instantané final ?, choisissez Non, puis confirmez.
6. Sélectionnez Delete.

Création d'une instance de base de données PostgreSQL et connexion à une base de données sur une instance de base de données PostgreSQL

La manière la plus simple de créer une instance de base de données consiste à utiliser la console RDS. Une fois que vous avez créé l'instance de base de données, vous pouvez utiliser des utilitaires de client SQL standard tels que pgAdmin pour vous connecter à l'instance de base de données. Dans cet exemple, vous créez une instance de base de données exécutant le moteur de base de données PostgreSQL appelé database-1, avec une classe d'instance de base de données db.t2.micro et 20 gibioctets (GiO) de stockage.

> **Important**
>
> Vous devez réaliser les tâches de la section Configuration pour Amazon RDS (p. 62) avant de créer une instance de base de données ou de vous y connecter.

Rubriques

- Création d'une instance de base de données PostgreSQL (p. 100)
- Connexion à une instance de base de données PostgreSQL (p. 104)
- Suppression d'une instance DB (p. 108)

Création d'une instance de base de données PostgreSQL

La fondation de base d'Amazon RDS est l'instance de base de données. Il s'agit de l'environnement dans lequel vous exécutez vos bases de données PostgreSQL.

Console

Vous pouvez créer une instance de base de données exécutant PostgreSQL à l'aide d'AWS Management Console, avec l'option Easy Create (Création facile) activée ou désactivée. Lorsque l'option Easy Create (Création facile) est activée, vous spécifiez uniquement le type de moteur, la taille et l'identifiant d'instance de base de données. Easy Create (Création facile) utilise les paramètres par défaut pour les autres options de configuration. Lorsque l'option Easy Create (Création facile) est désactivée, vous spécifiez davantage d'options de configuration lors de la création d'une base de données, notamment en matière de disponibilité, de sécurité, de sauvegardes et de maintenance.

Dans cet exemple, vous utilisez Easy Create (Création facile) pour créer une instance de base de données exécutant le moteur de base de données PostgreSQL avec une classe d'instance de base de données db.t2.micro.

> **Note**
>
> Pour de plus amples informations sur la création d'instances de base de données avec l'option Easy Create (Création facile) désactivée, veuillez consulter Création d'une instance de base de données Amazon RDS (p. 146).

Pour créer une instance de base de données PostgreSQL avec l'option Easy Create (Création facile) activée

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le coin supérieur droit de la console Amazon RDS, choisissez la région AWS dans laquelle vous voulez créer l'instance de base de données.
3. Dans la panneau de navigation, choisissez Databases (Bases de données).
4. Choisissez Create database (Créer une base de données) et veillez à choisir Easy Create (Création facile).

5. Dans Configuration, choisissez PostgreSQL.
6. Pour DB instance size (Taille de l'instance de base de données), choisissez Free tier (Offre gratuite).
7. Pour DB instance identifier (Identifiant d'instance de base de données), saisissez un nom pour l'instance de base de données, ou conservez le nom par défaut.
8. Pour Master username (Identifiant principal), saisissez un nom pour l'utilisateur principal, ou conservez le nom par défaut.

   La page Create database (Créer une base de données) doit ressembler à l'image suivante.

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 conf
  configuration options can be changed
  database is created.

Configuration

Engine type Info

- Amazon Aurora
- MySQL
- MariaDB
- PostgreSQL
- Oracle
- Microsoft SQ

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
- 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 cross all DB instances owned by your AWS account
Region.

database-1

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1

9. Pour utiliser un mot de passe principal généré automatiquement pour l'instance de base de données, vérifiez que la case Auto generate a password (Générer un mot de passe automatiquement) est cochée.

   Pour entrer votre mot de passe principal, décochez la case Auto generate a password (Générer un mot de passe automatiquement), puis entrez le même mot de passe dans les champs Mot de passe principal et Confirmer le mot de passe.

10. (Facultatif) Ouvrez View default settings for Easy Create (Afficher les paramètres par défaut pour Création facile).

   Vous pouvez examiner les paramètres par défaut utilisés quand l'option Easy Create (Création facile) est activée. Si vous voulez modifier un ou plusieurs paramètres pendant la création de la base de données, choisissez Standard Create (Création standard) pour les définir. La colonne Editable after database creation (Modifiable après création de la base de données indique les options que vous pouvez modifier après la création de la base de données. Pour modifier un paramètre dont la valeur est No (Non) dans cette colonne, utilisez Standard Create (Création standard). Pour les paramètres dont la valeur est Yes (Oui) dans cette colonne, vous pouvez utiliser Standard Create (Création standard) ou modifier l'instance de base de données après l'avoir créée pour modifier ces paramètres.

11. Choisissez Create database (Créer une base de données).

   Si vous choisissez de générer un mot de passe automatiquement, le bouton View credential details (Afficher les informations d'identification) apparaît sur la page Databases (Bases de données).

   Pour afficher l'identifiant principal et le mot de passe pour l'instance de base de données, choisissez View credential details (Afficher les informations d'identification).

   Pour vous connecter à l'instance de base de données en tant qu'utilisateur principal, utilisez l'identifiant et le mot de passe affichés.

   > **Important**
   >
   > Vous ne pourrez pas afficher le mot de passe de l'utilisateur principal de nouveau. Si vous ne l'enregistrez pas, il sera peut-être nécessaire de le modifier. Si vous devez changer le mot de passe de l'utilisateur principal une fois l'instance de base de données disponible, vous pouvez le faire en modifiant l'instance de base de données. Pour de plus amples informations

sur la modification d'une instance de base de données, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

12. Pour Databases (Bases de données), choisissez le nom de la nouvelle instance de base de données PostgreSQL.

    Sur la console RDS, les détails de la nouvelle instance de base de données s'affichent. L'instance de base de données a le statut creating (création en cours) jusqu'à ce qu'elle soit créée et prête à l'emploi. Lorsque l'état devient available (disponible), vous pouvez vous connecter à l'instance de base de données. En fonction de la quantité de stockage et de la classe d'instance de base de données, la mise à disposition de la nouvelle instance peut prendre jusqu'à 20 minutes.

Connexion à une instance de base de données PostgreSQL

Après qu'Amazon RDS a provisionné votre instance de base de données, vous pouvez utiliser n'importe quelle application cliente SQL standard pour vous connecter à l'instance. Le groupe de sécurité que vous avez assigné à l'instance de base de données lors de sa création doit autoriser l'accès à l'instance de base de données. Si vous avez des difficultés à vous connecter à l'instance de base de données, le problème concerne le plus souvent les règles d'accès que vous avez définies dans le groupe de sécurité assigné à l'instance de base de données.

Cette section illustre deux façons de se connecter à une instance de base de données PostgreSQL. Le premier exemple utilise pgAdmin, célèbre outil open source d'administration et de développement pour PostgreSQL. Vous pouvez télécharger et utiliser pgAdmin sans avoir une instance locale de PostgreSQL sur votre ordinateur client. Le second exemple utilise psql, utilitaire de ligne de commande qui fait partie d'une installation PostgreSQL. Pour utiliser psql, vous devez avoir installé PostgreSQL sur votre ordinateur client ou avoir installé le client psql sur votre ordinateur.

Dans cet exemple, vous vous connectez à une instance de base de données PostgreSQL à l'aide de pgAdmin.

Utilisation de pgAdmin pour se connecter à une instance de base de données PostgreSQL

Pour vous connecter à une instance de base de données PostgreSQL avec pgAdmin

1. Trouvez le point de terminaison (nom DNS) et le numéro de port pour votre instance de base de données.

a. Ouvrez la console RDS et choisissez Bases de données pour afficher une liste de vos instances de bases de données.

b. Choisissez le nom de l'instance de base de données PostgreSQL pour afficher ses détails.

c. Dans l'onglet Connectivity & security (Connectivité et sécurité), copiez le point de terminaison. Notez également le numéro du port. Vous avez besoin du point de terminaison et du numéro de port pour vous connecter à l'instance de base de données.

2. Installez pgAdmin depuis http://www.pgadmin.org/. Vous pouvez télécharger et utiliser pgAdmin sans avoir une instance locale de PostgreSQL sur votre ordinateur client.
3. Lancez l'application pgAdmin sur votre ordinateur client.
4. Choisissez Add Server (Ajouter un serveur) dans le menu File (Fichier).
5. Dans la boîte de dialogue New Server Registration (Nouvelle inscription de serveur), entrez le point de terminaison de l'instance de base de données (par exemple, `database-1.c6c8dntfzzhgv0.us-`

`west-1.rds.amazonaws.com`) dans la zone Host (Hôte). N'incluez pas les deux points ou le numéro du port comme illustré dans la console Amazon RDS (`database-1.c6c8dntfzzhgv0.us-west-1.rds.amazonaws.com:5432`).

Entrez le port que vous avez attribué à l'instance de base de données dans la zone Port. Saisissez l'identifiant et le mot de passe que vous avez entrés lorsque vous avez créé l'instance de base de données, respectivement dans les zones Username (Identifiant) et Password (Mot de passe).

6. Choisissez OK.
7. Dans l'Object browser (Navigateur d'objet), développez Server Groups (Groupes de serveur). Choisissez le serveur (l'instance de base de données) que vous avez créé, puis sélectionnez le nom de la base de données.

8. Choisissez l'icône de plug-in et choisissez Console PSQL. La fenêtre de la commande psql s'ouvre pour la base de données par défaut que vous avez créée.

9. Utilisez la fenêtre de commande pour entrer les commandes SQL ou psql. Entrez `\q` pour fermer la fenêtre.

Utilisation de psql pour se connecter à une instance de base de données PostgreSQL

Si PostgreSQL est installé sur votre ordinateur client, vous pouvez utiliser une instance locale de psql pour vous connecter à une instance de base de données PostgreSQL. Pour vous connecter à votre instance de base de données PostgreSQL avec psql, vous devez fournir les informations sur l'hôte et les informations d'identification d'accès.

Le format suivant permet de se connecter à une instance de base de données PostgreSQL sur Amazon RDS.

```
psql --host=DB_instance_endpoint --port=port --username=master_user_name --password --
dbname=database_name
```

Par exemple, la commande suivante se connecte à une base de données appelée `mypgdb` sur une instance de base de données PostgreSQL appelée `mypostgresql` à l'aide d'informations d'identification fictives.

```
psql --host=database-1.c6c8dntfzzhgv0.us-west-1.rds.amazonaws.com --port=5432 --
username=awsuser --password --dbname=postgres
```

Dépannage des problèmes de connexion

Le problème qui intervient le plus fréquemment lorsque vous tentez de vous connecter à une base de données sur une instance de base de données concerne les règles d'accès du groupe de sécurité assigné à l'instance de base de données. Si vous avez utilisé le groupe de sécurité de bases de données par défaut lorsque vous avez créé l'instance de base de données, ce groupe de sécurité ne dispose vraisemblablement pas des règles qui vous autorisent à accéder à l'instance. Pour plus d'informations sur les groupes de sécurité Amazon RDS, consultez Contrôle d'accès par groupe de sécurité (p. 1590).

L'erreur la plus courante est « could not connect to server: Connection timed out » (impossible de se connecter au serveur : connexion expirée). Si vous recevez cette erreur, vérifiez que le nom d'hôte est le point de terminaison de l'instance de base de données et que le numéro de port est correct. Vérifiez que le groupe de sécurité affecté à l'instance de base de données possède les règles nécessaires pour autoriser l'accès via tout pare-feu que votre connexion peut traverser.

Suppression d'une instance DB

Une fois que vous êtes connecté à l'exemple d'instance de base de données que vous avez créée, vous devez supprimer l'instance de base de données afin qu'elle ne vous soit plus facturée.

Pour supprimer une instance de base de données sans instantané de base de données final

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez l'instance de base de données que vous souhaitez supprimer.
4. Pour Actions, choisissez Supprimer.
5. Pour Créer un instantané final ?, choisissez Non, puis confirmez.
6. Sélectionnez Delete.

Didacticiel : Créer un serveur web et une instance de base de données Amazon RDS

Ce didacticiel vous aide à installer un serveur web Apache avec PHP et à créer une base de données MySQL. Le serveur web s'exécute sur une instance Amazon EC2 à l'aide d'Amazon Linux et la base de données MySQL est une instance de base de données MySQL Amazon RDS. L'instance Amazon EC2 et l'instance de base de données s'exécutent tous deux dans un Virtual Private Cloud (VPC) basé sur le service Amazon VPC.

> **Important**
>
> La création d'un compte AWS n'entraîne pas de frais. Toutefois, au cours de ce didacticiel, des coûts peuvent être générés par l'utilisation des ressources AWS. Vous pouvez supprimer ces ressources après avoir terminé le didacticiel si elles ne sont plus nécessaires.
>
> **Note**
>
> Ce didacticiel s'applique à Amazon Linux et peut ne pas fonctionner pour d'autres versions de Linux telles qu'Ubuntu.

Dans le didacticiel qui suit, vous allez spécifier le VPC, les sous-réseaux et les groupes de sécurité lors de la création de l'instance de base de données. Vous les spécifierez également lors de la création de l'instance EC2 pour héberger votre serveur web. Le VPC, les sous-réseaux et les groupes de sécurité sont nécessaires à la communication entre l'instance de base de données et le serveur web. Une fois que le VPC est configuré, ce didacticiel vous montre comment créer l'instance de base de données et comment installer le serveur web. Vous connectez votre serveur web à votre instance de base de données dans le VPC à l'aide du point de terminaison de l'instance de base de données point de terminaison du .

1. Effectuez les tâches définies dans Didacticiel : créer un Amazon VPC à utiliser avec une instance de base de données (p. 1629).

   Avant de commencer ce didacticiel, assurez-vous de disposer d'un VPC avec des sous-réseaux public et privé, ainsi que les groupes de sécurité correspondants. Si vous ne possédez pas ces éléments, effectuez les tâches suivantes dans le didacticiel :

   a. Créer un VPC avec des sous-réseaux publics et privés (p. 1630)
   b. Création de sous-réseaux supplémentaires (p. 1631)
   c. Créer un groupe de sécurité VPC pour un serveur web public (p. 1631)
   d. Créer un groupe de sécurité VPC pour une instance de base de données privée (p. 1632)
   e. Création d'un groupe de sous-réseaux DB (p. 1633)
2. Créez une instance de base de données. (p. 110)
3. Créer une instance EC2 et installer un serveur web (p. 121)

Le diagramme suivant affiche la configuration obtenue au terme de ce didacticiel.

Créez une instance de base de données.

Au cours de cette étape, vous allez créer une instance de base de données MySQL Amazon RDS qui conserve les données utilisées par une application web.

> **Important**
>
> Avant de commencer cette étape, assurez-vous de disposer d'un VPC avec des sous-réseaux public et privé, ainsi que les groupes de sécurité correspondants. Si vous ne disposez pas de ces éléments, consultez Didacticiel : créer un Amazon VPC à utiliser avec une instance de base de données (p. 1629). Suivez les étapes dans Créer un VPC avec des sous-réseaux publics et privés (p. 1630), Création de sous-réseaux supplémentaires (p. 1631), Créer un groupe de sécurité VPC pour un serveur web public (p. 1631) et Créer un groupe de sécurité VPC pour une instance de base de données privée (p. 1632).

> **Note**
>
> Une nouvelle interface de la console est disponible pour la création de bases de données. Selon la console que vous utilisez, choisissez les instructions Nouvelle console ou Console d'origine. Les instructions Nouvelle console sont ouvertes par défaut.

Nouvelle console

Pour lancer une instance de base de données MySQL

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le coin supérieur droit d'AWS Management Console, choisissez la région AWS dans laquelle vous voulez créer l'instance de base de données. Cet exemple utilise la région USA Ouest (Oregon).
3. Dans le panneau de navigation, choisissez Databases (Bases de données).
4. Choisissez Create database (Créer une base de données).
5. Sur la page Create database (Créer une base de données), présentée ci-après, vérifiez que l'option Standard Create (Création standard) est activée, puis choisissez MySQL.

6. Dans la section Modèles, choisissez Offre gratuite.
7. Dans la section Settings (Paramètres), définissez les valeurs suivantes :
   - DB Instance Identifier (Identifiant d'instance DB) – **`tutorial-db-instance`**

- Master Username (Identifiant principal) – **`tutorial_user`**
- Auto generate a password (Générer un mot de passe automatiquement) – Désactivez l'option
- Master password (Mot de passe principal) – Choisissez un mot de passe.
- Confirm password (Confirmer le mot de passe) – Saisissez à nouveau le mot de passe.

8. Dans la section DB instance size (Taille de l'instance de base de données), définissez les valeurs suivantes :

   - Classe à capacité extensible (inclut les classes t)
   - db.t2.micro

9. Dans les sections Storage (Stockage) et Availability & durability (Disponibilité et durabilité), utilisez les valeurs par défaut.
10. Dans la section Connectivity (Connectivité), ouvrez Additional connectivity configuration (Configuration de la connectivité supplémentaire) et définissez les valeurs suivantes :

    - Virtual Private Cloud (VPC) : choisissez un VPC existant avec des sous-réseaux publics et privés, tels que `tutorial-vpc` (*`l'identifiant`* du vpc) créé dans Créer un VPC avec des sous-réseaux publics et privés (p. 1630)

      Note

      Le VPC doit avoir des sous-réseaux dans des zones de disponibilité différentes.
    - Groupe de sous-réseaux – Le groupe de sous-réseaux de base de données pour le VPC, tel que `tutorial-db-subnet-group` créé dans Création d'un groupe de sous-réseaux DB (p. 1633)
    - Accès public : Non
    - Groupes de sécurité VPC existants : choisissez un groupe de sécurité VPC existant configuré pour un accès privé, tel que `tutorial-db-securitygroup` créé dans Créer un groupe de sécurité VPC pour une instance de base de données privée (p. 1632).

      Supprimez les autres groupes de sécurité, tels que le groupe de sécurité par défaut, en cliquant sur le signe X qui lui est associé.
    - Port de base de données – 3306

11. Ouvrez la section Additional configuration (Configuration supplémentaire), puis entrez **`sample`** pour Initial database name (Nom de la base de données initiale). Conservez les paramètres par défaut pour les autres options.
12. Pour créer votre instance de base de données MySQL RDS, choisissez Créer une base de données.

    Votre nouvelle instance de base de données apparaît dans la liste Databases (Bases de données) avec l'état Creating (Création en cours).
13. Attendez que le Status (État) de votre instance de base de données affiche Available (Disponible). Sélectionnez ensuite le nom de l'instance de base de données pour afficher les détails.
14. Dans la section Connectivity & security (Connectivité et sécurité), affichez le Endpoint (Point de terminaison) et le Port de l'instance de base de données.

Notez le point de terminaison et le port de votre instance de base de données. Vous utilisez ces informations pour connecter votre serveur web à votre instance de base de données.

Pour vous assurer que votre instance de base de données est aussi sécurisée que possible, vérifiez que les sources extérieures au VPC ne peuvent pas se connecter à cette dernière.

15. Terminé Créer une instance EC2 et installer un serveur web (p. 121)

Console d'origine

Pour lancer une instance de base de données MySQL

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le coin supérieur droit d'AWS Management Console, choisissez la région AWS dans laquelle vous voulez créer l'instance de base de données. Cet exemple utilise la région USA Ouest (Oregon).
3. Dans la panneau de navigation, choisissez Databases (Bases de données).

   Si le panneau de navigation est fermé, choisissez l'icône de menu en haut à gauche pour l'ouvrir.
4. Choisissez Create database (Créer une base de données) pour ouvrir la page Sélectionner un moteur.
5. Sur la page Sélectionner le moteur, illustré ci-après, choisissez MySQL, puis Suivant.

6. Sur la page Choose use case (Choisir le cas d'utilisation), choisissez Offre gratuite – MySQL, puis Suivant.
7. Sur la page Spécification de détails de base de données, illustrée ci-dessous, définissez les valeurs suivantes :

   - Modèle de licence : Utilisez la valeur par défaut.
   - Version du moteur de base de données : Utilisez la valeur par défaut.
   - Classe d'instance de base de données : `db.t2.micro`

- Déploiement multi-AZ : `No`
- Type de stockage : `General Purpose (SSD)`
- Stockage alloué : `20 GiB`
- Identifiant d'instance DB : `tutorial-db-instance`
- Identifiant principa l: `tutorial_user`
- Mot de passe principal : Choisissez un mot de passe.
- Confirmer le mot de passe : Saisissez à nouveau le mot de passe.

Specify DB details

Instance specifications

Estimate your monthly costs for the DB Instance using the AWS Simple Monthly Calculator.

DB engine
MySQL Community Edition

License model info
general-public-license

DB engine version info
mysql 5.6.37

Known Issues/Limitations
Review the Known Issues/Limitations to learn about potential compatibility issues with specific database versions.

Free tier
The Amazon RDS Free Tier provides a single db.t2.micro instance as well as up to 20 GB of storage, allowing new AWS customers to gain hands-on experience with Amazon RDS. Learn more about the RDS Free Tier and the instance restrictions here.

Only enable options eligible for RDS Free Usage Tier info

DB instance class info
db.t2.small — 1 vCPU, 2 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
General Purpose (SSD)

Allocated storage
20 GB
(Minimum: 20 GB, Maximum: 16384 GB) Higher allocated storage may improve IOPS performance.

Provisioning less than 100 GB of General Purpose (SSD) storage for high throughput workloads could result in higher latencies upon exhaustion of the initial General Purpose (SSD) IO credit balance. Click here for more details.

Settings

DB instance identifier info
Specify a name that is unique for all DB instances owned by your AWS account in the current region.
tutorial-db-instance
DB instance identifier is case insensitive, but stored as all lower-case, as in "mydbinstance".

Master username info
Specify an alphanumeric string that defines the login ID for the master user.
tutorial_user
Master Username must start with a letter.

Master password info
••••••••
Master Password must be at least eight characters long, as in "mypassword".

Confirm password info
••••••••

Cancel Previous Next

8. Choisissez Suivant et définissez les valeurs suivantes sur la page Configure advanced settings (Configurer les paramètres avancés) :

   - Virtual Private Cloud (VPC) : Choisissez un VPC existant avec des sous-réseaux publics et privés, tels que `tutorial-vpc` (*`identifiant`*-vpc) créé dans Créer un VPC avec des sous-réseaux publics et privés (p. 1630)

     Note

     Le VPC doit avoir des sous-réseaux dans des zones de disponibilité différentes.

   - Groupe de sous-réseaux : Le groupe de sous-réseaux de base de données pour le VPC, tel que `tutorial-db-subnet-group` créé dans Création d'un groupe de sous-réseaux DB (p. 1633)
   - Accessibilité publique : Non
   - Zone de disponibilité : Aucune préférence
   - Groupes de sécurité VPC : choisissez un groupe de sécurité VPC existant configuré pour un accès privé, tel que `tutorial-db-securitygroup` créé dans Créer un groupe de sécurité VPC pour une instance de base de données privée (p. 1632).

     Supprimez les autres groupes de sécurité, tels que le groupe de sécurité par défaut, en cliquant sur le signe X qui lui est associé.

   - Nom de base de données : `sample`

   Conservez les paramètres par défaut pour les autres options.

9. Pour créer votre instance de base de données MySQL RDS, choisissez Créer une base de données.
10. Sur la page suivante, choisissez Afficher les détails d'instances de bases de données pour afficher votre instance de base de données.
11. Attendez que l'état de votre nouvelle instance de base de données indique qu'elle est disponible. Faites défiler ensuite jusqu'à la section Connect (Se connecter), illustrée ci-après.

Notez le point de terminaison et le port de votre instance de base de données. Vous utilisez ces informations pour connecter votre serveur web à votre instance de base de données.

Pour vous assurer que votre instance de base de données est aussi sécurisée que possible, vérifiez que les sources extérieures au VPC ne peuvent pas se connecter à cette dernière.

12. Terminé Créer une instance EC2 et installer un serveur web (p. 121)

Créer une instance EC2 et installer un serveur web

Dans cette étape, vous allez créer un serveur web pour vous connecter à l'instance de base de données Amazon RDS que vous avez créée dans Créez une instance de base de données. (p. 110).

Lancer une instance EC2

En premier lieu, vous allez créer une instance Amazon EC2 dans le sous-réseau public de votre VPC.

Pour lancer une instance EC2

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Choisissez Tableau de bord EC2, puis Lancer une instance, comme illustré ci-dessous.

3. Choisissez l'AMI Amazon Linux, comme indiqué ci-après.

Important

Ne choisissez pas l'AMI Amazon Linux car elle ne dispose pas des packages logiciels requis pour ce didacticiel.

4. Choisissez le type d'instance t2.micro, comme illustré ci-dessous, puis choisissez Suivant : Configurer les détails d'instance.

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
General purpose	t3a.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
General purpose	t3a.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes
General purpose	t3a.medium	2	4	EBS only	Yes	Up to 5 Gigabit	Yes
General purpose	t3a.large	2	8	EBS only	Yes	Up to 5 Gigabit	Yes

5. Sur la page Configurer les détails d'instance, illustrée ci-dessous, spécifiez les valeurs suivantes et conservez les valeurs par défaut des autres paramètres :

   - Réseau : Choisissez le VPC avec des sous-réseaux publics et privés que vous avez choisi pour l'instance de base de données, tel que `vpc-`*`identifier`* `| tutorial-vpc` créé dans Créer un VPC avec des sous-réseaux publics et privés (p. 1630).

- Subnet (Sous-réseau) : Choisissez un sous-réseau public existant, tel que `subnet-identifier | Tutorial public | us-west-2a` créé dans Créer un groupe de sécurité VPC pour un serveur web public (p. 1631).
- Attribuer automatiquement l'adresse IP publique : choisissez Enable (Activer).

6. Choisissez Next: Add Storage.
7. Sur la page Add Storage (Ajouter le stockage), conservez les valeurs par défaut et choisissez Next: Add Tags (Étape suivante : ajouter des balises).
8. Sur la page Add Tags (Ajouter des balises), illustrée ci-après, choisissez Add Tag (Ajouter une balise), puis tapez **`Name`** pour Clé et **`tutorial-web-server`** pour Valeur.

9. Choisissez Suivant : Configurer le groupe de sécurité.
10. Sur la page Configurez le groupe de sécurité, illustrée ci-dessous, choisissez Sélectionnez un groupe de sécurité existant. Choisissez ensuite un groupe de sécurité existant, tel que `tutorial-securitygroup` créé dans Créer un groupe de sécurité VPC pour un serveur web public (p. 1631). Assurez-vous que le groupe de sécurité que vous choisissez inclut des règles entrantes pour l'accès SSH (Secure Shell) et HTTP.

11. Choisissez Review and Launch.
12. Sur la page Review Instance Launch (Examiner le lancement d'instance), illustrée ci-dessous, vérifiez vos paramètres, puis choisissez Launch (Lancer).

13. Sur la page Select an existing key pair or create a new key pair (Sélectionner une paire de clés existante ou en créer une), illustrée ci-dessous, choisissez Create a new key pair (Créer une paire de clés) et choisissez `tutorial-key-pair` comme nom de cette paire de clés. Choisissez Download Key Pair (Télécharger la paire de clés), puis enregistrez le fichier de paire de clés sur votre ordinateur local. Vous utilisez ce fichier de paire de clés pour vous connecter à votre instance EC2.

14. Pour lancer votre instance EC2, choisissez Launch Instances (Lancer les instances). Sur la page Launch Status (Statut de lancement), illustrée ci-dessous, notez l'identifiant de votre nouvelle instance EC2, tel que : `i-0288d65fd4470b6a9`.

15. Pour rechercher votre instance, choisissez Afficher les instances.
16. Attendez que le paramètre État de l'instance de votre instance stipule En cours d'exécution, avant de continuer.

Installer un serveur Web Apache avec PHP

Ensuite, vous allez vous connecter à votre instance EC2 et installer le serveur web.

> **Note**
>
> Ce didacticiel est conçu pour fonctionner avec une instance de base de données MySQL version 5.6. Si vous utilisez une instance de base de données MySQL 8.0 à la place, vous devez définir les paramètres suivants sur les valeurs spécifiées dans un groupe de paramètres de base de données créé par le client :
>
> - `character_set_server` – `utf8`
> - `collation_server` – `utf8_general_ci`
>
> Les valeurs par défaut de ces paramètres provoquent l'échec de la connexion à la base de données. D'autres valeurs de paramètre peuvent également corriger le problème. Pour de plus

amples informations sur la définition des paramètres, veuillez consulter Utilisation de groupes de paramètres de base de données (p. 225).
Après avoir réinitialisé les paramètres, modifiez votre instance de base de données pour utiliser le groupe de paramètres de base de données, puis redémarrez l'instance de base de données. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243) et Redémarrage d'une instance de base de données (p. 272).

Pour vous connecter à votre instance EC2 et installer le serveur Web Apache avec PHP

1. Connectez-vous à l'instance EC2 que vous avez précédemment créée en suivant la procédure spécifiée dans Connexion à l'instance Linux.
2. Obtenez les dernières corrections de bogues et mises à jour de sécurité en mettant à jour le logiciel sur votre instance EC2. Pour ce faire, exécutez la commande suivante.

   Note

   L'option `-y` installe les mises à jour sans demander de confirmation. Pour examiner les mises à jour avant de les installer, omettez cette option.

```
[ec2-user ~]$ sudo yum update -y
```

3. Une fois les mises à jour terminées, installez le serveur web Apache avec le package logiciel PHP à l'aide de la commande `yum install`. Cette commande installe plusieurs packages logiciels et les dépendances connexes au même moment.

```
[ec2-user ~]$ sudo yum install -y httpd24 php56 php56-mysqlnd
```

   Si vous obtenez le message d'erreur `No package package-name available`, votre instance n'a pas été lancée avec l'AMI Amazon Linux. Vous utilisez peut-être l'AMI Amazon Linux 2 à la place. Vous pouvez afficher votre version d'Amazon Linux avec la commande suivante

```
cat /etc/system-release
```

   Pour plus d'informations, consultez Mise à jour du logiciel de l'instance.
4. Démarrez le serveur web avec la commande illustrée ci-dessous.

```
[ec2-user ~]$ sudo service httpd start
```

   Vous pouvez vérifier que votre serveur web est correctement installé et démarré. Pour ce faire, saisissez le nom DNS (Domain Name System) public de votre instance EC2 dans la barre d'adresse d'un navigateur web, par exemple : `http://ec2-42-8-168-21.us-west-1.compute.amazonaws.com`. Si votre serveur Web est en cours d'exécution, vous voyez la page de test Apache.

   Si la page de test Apache ne s'affiche pas, vérifiez vos règles entrantes pour le groupe de sécurité du VPC que vous avez créé dans Didacticiel : créer un Amazon VPC à utiliser avec une instance de base de données (p. 1629). Assurez-vous que vos règles entrantes incluent une règle autorisant l'accès HTTP (port 80) à l'adresse IP que vous utilisez pour vous connecter au serveur web.

   Note

   La page de test Apache apparaît uniquement en l'absence de contenu dans le répertoire racine des documents, `/var/www/html`. Après l'ajout de contenu dans le répertoire racine des documents, votre contenu apparaît à l'adresse DNS publique de votre instance EC2 à la place de la page de test Apache.

5. Configurez le serveur web pour qu'il démarre à chaque redémarrage du système à l'aide de la commande `chkconfig`.

```
[ec2-user ~]$ sudo chkconfig httpd on
```

Pour autoriser `ec2-user` à gérer les fichiers dans le répertoire racine par défaut pour votre serveur Web Apache, modifiez l'appartenance et les autorisations du répertoire `/var/www`. Dans ce didacticiel, vous ajoutez un groupe nommé `www` à votre instance EC2. Ensuite, vous donnez à ce groupe la propriété du répertoire `/var/www` et ajoutez des autorisations d'écriture pour le groupe. Tous les membres de ce groupe peuvent alors ajouter, supprimer et modifier des fichiers pour le serveur Web.

Pour définir les autorisations sur les fichiers pour le serveur Web Apache

1. Ajoutez le groupe `www` à votre instance EC2 à l'aide de la commande suivante.

```
[ec2-user ~]$ sudo groupadd www
```

2. Ajoutez l'utilisateur `ec2-user` au groupe `www`.

```
[ec2-user ~]$ sudo usermod -a -G www ec2-user
```

3. Pour actualiser vos autorisations et inclure le nouveau groupe `www`, déconnectez-vous.

```
[ec2-user ~]$ exit
```

4. Reconnectez-vous et vérifiez que le groupe `www` existe à l'aide de la commande `groups`.

```
[ec2-user ~]$ groups
ec2-user wheel www
```

5. Remplacez le groupe propriétaire du répertoire `/var/www` et de son contenu par le groupe `www`.

```
[ec2-user ~]$ sudo chgrp -R www /var/www
```

6. Modifiez les autorisations des répertoires `/var/www` et de ses sous-répertoires pour ajouter des autorisations d'écriture de groupe et définir l'ID de groupe sur les sous-répertoires créés à l'avenir.

```
[ec2-user ~]$ sudo chmod 2775 /var/www
[ec2-user ~]$ find /var/www -type d -exec sudo chmod 2775 {} +
```

7. Modifiez de façon récursive les autorisations pour les fichiers figurant dans le répertoire `/var/www` et ses sous-répertoires pour ajouter des autorisations d'écriture de groupe.

```
[ec2-user ~]$ find /var/www -type f -exec sudo chmod 0664 {} +
```

Connecter le serveur web Apache à l'instance de base de données

Ensuite, vous allez ajouter du contenu à votre serveur web Apache qui se connecte à votre instance de base de données Amazon RDS.

Pour ajouter du contenu au serveur web Apache qui se connecte à votre instance de base de données

1. Alors que vous êtes encore connecté à votre instance EC2, remplacez le répertoire par `/var/www` et créez un sous-répertoire nommé `inc`.

```
[ec2-user ~]$ cd /var/www
[ec2-user ~]$ mkdir inc
[ec2-user ~]$ cd inc
```

2. Créez un fichier dans le répertoire `inc` nommé `dbinfo.inc`, puis modifiez le fichier en appelant nano (ou l'éditeur de votre choix).

```
[ec2-user ~]$ >dbinfo.inc
[ec2-user ~]$ nano dbinfo.inc
```

3. Ajoutez le contenu suivant au fichier `dbinfo.inc`. Ici, *`db_instance_endpoint`* est le point de terminaison de l'instance de base de données, sans le port, et le *`mot de passe maître`* est le mot de passe maître de votre instance de base données.

   Note

   Nous vous recommandons de placer les informations de nom d'utilisateur et de mot de passe dans un dossier ne faisant pas partie de la racine du document de votre serveur web. Vous réduisez ainsi la possibilité d'exposer vos informations de sécurité.

```
<?php

define('DB_SERVER', 'db_instance_endpoint');
define('DB_USERNAME', 'tutorial_user');
define('DB_PASSWORD', 'master password');
define('DB_DATABASE', 'sample');

?>
```

4. Enregistrez et fermez le fichier `dbinfo.inc`.
5. Remplacez le répertoire par `/var/www/html`.

```
[ec2-user ~]$ cd /var/www/html
```

6. Créez un fichier dans le répertoire `html` nommé `SamplePage.php`, puis modifiez le fichier en appelant nano (ou l'éditeur de votre choix).

```
[ec2-user ~]$ >SamplePage.php
[ec2-user ~]$ nano SamplePage.php
```

7. Ajoutez le contenu suivant au fichier `SamplePage.php` :

   Note

   Nous vous recommandons de placer les informations de nom d'utilisateur et de mot de passe dans un dossier ne faisant pas partie de la racine du document de votre serveur web. Vous réduisez ainsi la possibilité d'exposer vos informations de sécurité.

```
<?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. Enregistrez et fermez le fichier `SamplePage.php`.
9. Vérifiez que votre serveur web se connecte avec succès à votre instance de base de données en ouvrant un navigateur web et en accédant à une page `http://`*`EC2 instance endpoint`*`/SamplePage.php`, par exemple : `http://ec2-55-122-41-31.us-west-2.compute.amazonaws.com/SamplePage.php`.

Vous pouvez utiliser `SamplePage.php` pour ajouter des données à votreinstance de base de données. Les données que vous ajoutez sont ensuite affichées sur la page. Pour vérifier que les données ont été insérées dans la table, vous pouvez installer MySQL sur l'instance Amazon EC2, connectez-vous à l'instance de base de données et interrogez la table.

Pour vérifier que la sécurité de votre instance de base de données est assurée, contrôlez que les sources extérieures du VPC ne peuvent pas se connecter à votre instance de base de données.

Après avoir testé votre serveur Web et votre base de données, vous devez supprimer votre instance de base de données et votre instance Amazon EC2.

- Pour supprimer votre instance de base de données, suivez les instructions de la section Suppression d'une instance de base de données (p. 313). Vous n'avez pas besoin de créer un instantané final.
- Pour résilier une instance Amazon EC2, suivez les instructions de la page Résilier votre instance dans le Guide de l'utilisateur Amazon EC2.

Didacticiels

Les didacticiels suivants vous montrent comment exécuter les tâches courantes qui utilisent Amazon RDS:

- Didacticiel : créer un Amazon VPC à utiliser avec une instance de base de données (p. 1629)
- Didacticiel : Créer un serveur web et une instance de base de données Amazon RDS (p. 109)
- Didacticiel : restaurer une instance de base de données à partir d'un instantané de base de données (p. 368)

Pour plus d'informations sur la formation, consultez Formation et certification AWS.

Bonnes pratiques relatives à Amazon RDS.

Découvrez les bonnes pratiques d'utilisation de Amazon RDS. A mesure que de nouvelles bonnes pratiques seront identifiées, nous mettrons à jour cette section.

Rubriques

- Directives opérationnelles de base Amazon RDS (p. 135)
- Recommandations RAM d'une instance de base de données (p. 136)
- Utilisation de la surveillance améliorée pour identifier les problèmes de système d'exploitation (p. 136)
- Utilisation des métriques pour identifier les problèmes de performances (p. 137)
- Bonnes pratiques pour utiliser les moteurs de stockage MySQL (p. 141)
- Bonnes pratiques pour utiliser les moteurs de stockage MariaDB (p. 142)
- Bonnes pratiques d'utilisation d'Oracle (p. 142)
- Bonnes pratiques pour utiliser les moteurs de stockage PostgreSQL (p. 142)
- Bonnes pratiques pour l'utilisation de SQL Server (p. 144)
- Utilisation des groupes de paramètres DB (p. 145)
- Vidéo de présentation des nouvelles fonctionnalités et des bonnes pratiques pour Amazon RDS (p. 145)

> **Note**
>
> Pour obtenir des recommandations communes pour Amazon RDS, consultez Utilisation des recommandations Amazon RDS (p. 389).

Directives opérationnelles de base Amazon RDS

Voici les directives opérationnelles de base que toute personne doit suivre lorsqu'elle utilise Amazon RDS. Notez que le contrat de niveau de service (SLA) Amazon RDS exige que vous suiviez ces directives :

- Surveillez l'utilisation de votre mémoire, de votre UC et de votre espace de stockage. Amazon CloudWatch peut être configuré pour vous informer quand vos habitudes d'utilisation changent ou quand vous atteignez le maximum votre capacité de développement, afin que vous puissiez maintenir les performances et la disponibilité du système.
- Augmentez la capacité de votre instance de base de données lorsque vous atteignez la limite de stockage. Vous devrez disposer de capacités de mémoire et de stockage supplémentaires pour vous adapter aux hausses imprévues des besoins de vos applications.
- Activez les sauvegardes automatiques et configurez-les pour qu'elles s'exécutent pendant la plus faible I/O par seconde en écriture de la journée. C'est à ce moment qu'une sauvegarde perturbe le moins l'utilisation de votre base de données.
- Si la charge de travail de votre base de données exige plus d'I/O que vous avez provisionné, la récupération suite à un basculement ou un échec de la base de données est lente. Pour augmenter la capacité d'I/O d'une instance de base de données, procédez comme suit :
  - Migrez vers une classe d'instance de base de données différente avec une forte capacité d'E/S.

  - Passez du stockage magnétique au stockage à usage général ou au stockage à IOPS provisionnées, suivant l'augmentation dont vous avez besoin. Pour plus d'informations sur les types de stockage disponibles, consultez Types de stockage Amazon RDS (p. 30).

    Si vous passez au stockage à IOPS provisionnées, veillez que vous utilisez également une classe d'instance de base de données optimisée pour les IOPS provisionnées. Pour plus d'informations sur les IOPS provisionnées, consultez Stockage SSD d'I/O par seconde provisionnées (p. 33).
  - Si vous utilisez déjà un stockage d'IOPS provisionnées, allouez un débit supplémentaire.
- Si votre application cliente met en cache les données DNS (Domain Name Service) de vos instances de base de données, définissez une valeur durée de vie (TTL) de moins de 30 secondes. Étant donné que l'adresse IP sous-jacente d'une instance de base de données peut changer suite à un basculement, la mise en cache des données DNS pour une durée prolongée peut entraîner des échecs de connexion si votre application tente de se connecter à une adresse IP qui n'est plus en service.
- Testez le basculement pour votre instance de base de données afin de connaître la durée du processus pour votre cas d'utilisation spécifique et veiller à ce que l'application qui accède à votre instance de base de données puisse automatiquement se connecter à la nouvelle instance de base de données suite au basculement.

Recommandations RAM d'une instance de base de données

Une bonne pratique Amazon RDS en matière de performances consiste à attribuer suffisamment de RAM pour que votre ensemble de travail réside presque totalement en mémoire. L'ensemble de travail est les données et les index fréquemment utilisés sur votre instance. Plus vous utilisez l'instance de base de données, plus l'ensemble de travail se développera.

Pour savoir si votre ensemble de travail est presque totalement en mémoire, vérifiez les métriques d'E/S par seconde en lecture (avec Amazon CloudWatch) pendant que l'instance de base de données est en chargement. La valeur d'I/O par seconde en lecture doit être faible et stable. Si l'augmentation de la classe d'instance de base de données—pour une classe avec plus de RAM—entraîne une chute spectaculaire de ReadIOPS, cela signifie que votre ensemble de travail n'était pas encore totalement en mémoire. Continuez à augmenter jusqu'à ce que la valeur d'I/O par seconde en lecture ne chute plus de façon spectaculaire suite à une opération de dimensionnement, ou qu'elle soit réduite au minimum. Pour plus d'informations sur la supervision des métriques d'une instance de base de données, consultez Affichage des métriques d'instances de base de données (p. 384).

Utilisation de la surveillance améliorée pour identifier les problèmes de système d'exploitation

Lorsque la surveillance améliorée est activée, Amazon RDS fournit des métriques en temps réel pour le système d'exploitation sur lequel votre instance de base de données s'exécute. Vous pouvez afficher les métriques pour votre instance de base de données à l'aide de la console, ou utiliser la sortie JSON de surveillance améliorée d'Amazon CloudWatch Logs dans le système de surveillance de votre choix. Pour plus d'informations sur la surveillance améliorée, consultez Surveillance améliorée (p. 394)

Utilisation des métriques pour identifier les problèmes de performances

Pour identifier les problèmes de performances causés par des ressources insuffisantes et d'autres goulots d'étranglement courants, vous pouvez surveiller les métriques disponibles pour votre instance de base de données Amazon RDS.

Consultation des métriques de performances

Vous devez régulièrement surveiller les métriques de performances pour observer les valeurs moyennes, maximum et minimum pour différents intervalles de temps. De cette façon, vous pouvez identifier quand les performances se dégradent. Vous pouvez également configurer des alarmes Amazon CloudWatch pour des seuils de métriques spécifiques, afin d'être alerté lorsqu'ils sont atteints.

Pour résoudre les problèmes de performances, il est important de comprendre les performances de base du système. Lorsque vous configurez une nouvelle instance de base de données et l'exécutez avec une charge de travail typique, vous devez capturer les valeurs moyennes, maximum et minimum de toutes les métriques de performances à un nombre d'intervalles différents (par exemple, une heure, 24 heures, une semaine, deux semaines) pour vous faire une idée. Cela permet de comparer l'activité pendant les heures pleines et les heures creuses. Vous pouvez ensuite utiliser ces informations pour identifier quand les performances chutent sous les niveaux standard.

Pour consulter les métriques de performances

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, sélectionnez Bases de données, choisissez une instance de base de données.
3. Choisissez Surveillance. Les huit premières métriques de performances s'affichent. Les métriques affichent par défaut les informations pour le jour même.
4. Utilisez les boutons numérotés en haut à droite pour parcourir les autres métriques, ou choisissez Adjust the settings (Ajuster les paramètres) pour consulter d'autres métriques.
5. Choisissez une métrique de performances pour régler l'intervalle de temps afin de consulter d'autres données que celles du jour même. Vous pouvez changer les valeurs Statistic (Statistique), Time Range (Plage de temps) et Period (Période) pour régler les informations affichées. Par exemple, pour consulter les valeurs maximales d'une métrique pour chaque jour des deux dernières semaines, configurez Statistic (Statistique) sur Maximum, Time Range (Plage de temps) sur Last 2 Weeks (Dernières 2 semaines) et Period (Période) sur Day (Jour).

   Note

   Si vous changez les valeurs Statistic (Statistique), Time Range (Plage de temps) et Period (Période), elles seront modifiées pour toutes les métriques. Les valeurs mises à jour restent inchangées tout au long de votre session ou jusqu'à ce que vous les modifiiez de nouveau.

Vous pouvez également consulter les métriques de performances à l'aide de l'interface de ligne de commande ou de l'API. Pour plus d'informations, consultez Affichage des métriques d'instances de base de données (p. 384).

Pour définir une alarme CloudWatch

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.

2. Dans le panneau de navigation, sélectionnez Bases de données, choisissez une instance de base de données.
3. Choisissez Logs & events (Journaux et événements).
4. Dans la section Alarmes CloudWatch, choisissez Créer une alarme.

5. Pour Envoyer des notifications, choisissez Oui et pour Envoyer des notifications à, choisissez New email or SMS topic (Nouvel e-mail ou nouvelle rubrique SMS).
6. Dans Nom de la rubrique, entrez un nom pour la notification, et pour Avec ces destinataires, entrez une liste séparée par des virgules d'adresses e-mail et de numéros de téléphone.
7. Pour Métrique, choisissez la statistique et la métrique d'alarme à définir.
8. Pour Seuil, indiquez si la métrique doit être supérieure, inférieure ou égale au seuil, et définissez la valeur du seuil.
9. Pour Période d'évaluation, choisissez la période d'évaluation de l'alarme et pour période(s) consécutive(s) de, choisissez la durée pendant laquelle le seuil doit avoir été atteint pour déclencher l'alarme.
10. Pour Name of alarm (Nom de l'alarme), entrez un nom pour l'alarme.
11. Sélectionnez Create Alarm.

L'alarme apparaît dans la section Alarmes CloudWatch.

Évaluation des métriques de performances

Une instance de base de données possède un nombre de catégories différentes de métriques, et la manière de déterminer les valeurs acceptables dépend de la métrique.

Processeur

- Utilisation du processeur : pourcentage de capacité de traitement informatique utilisée.

Mémoire

- Mémoire libérable : combien de RAM est disponible sur l'instance de base de données, en octets. La ligne rouge des métriques de l'onglet Monitoring est marqué à 75 % pour les métriques d'UC, de mémoire et de stockage. Si la consommation de la mémoire de l'instance franchit régulièrement cette ligne, cela indique que vous devez vérifier votre charge de travail ou mettre à niveau votre instance.
- Usage du swap : combien d'espace de swap est utilisé par l'instance de base de données, en octets.

Espace disque

- Espace de stockage libre : combien d'espace disque n'est pas utilisé actuellement par l'instance de base de données, en octets.

Opérations d'entrée/sortie

- E/S par seconde en lecture, E/S par seconde en écriture : le nombre moyen d'opérations de lecture ou d'écriture sur disque par seconde.
- Latence de lecture, latence d'écriture : la durée moyenne d'une opération de lecture ou d'écriture en millisecondes.
- Débit de lecture, débit d'écriture : le nombre moyen d'octets lus depuis un disque ou écrits sur un disque par seconde.
- Longueur de la file d'attente : le nombre d'opérations d'E/S qui attendent d'être écrites sur un disque ou lues depuis un disque.

Trafic réseau

- Débit réseau reçu, débit réseau transmis : la vitesse du trafic réseau vers et depuis l'instance de base de données en octets par seconde.

Connexions de la base de données

- Connexions DB : le nombre de sessions client qui sont connectées à l'instance de base de données.

Pour des descriptions individuelles plus détaillées des métriques de performances disponibles, veuillez consulter Surveillance avec Amazon CloudWatch (p. 376).

En général, les valeurs acceptables pour les métriques de performances dépendent de vos données de référence et de l'activité de votre application. Enquêtez sur les écarts cohérents ou tendanciels de vos données de référence. Voici quelques conseils sur les types spécifiques de métriques :

- Forte utilisation de l'UC et de la RAM – Des valeurs importantes de l'utilisation de l'UC et de la RAM peuvent être appropriées, pourvu qu'elles soient attendues et conformes aux objectifs pour votre application (comme le débit ou la simultanéité).
- Utilisation de l'espace disque – Enquêtez sur l'utilisation de l'espace disque si l'espace utilisé est constamment égal ou supérieur à 85 pour cent de l'espace disque total. Voyez s'il est possible de supprimer des données de l'instance ou d'archiver des données sur un système différent pour libérer de l'espace.
- Trafic réseau – Pour le trafic réseau, discutez avec votre administrateur pour connaître le débit attendu pour votre domaine réseau et votre connexion Internet. Enquêtez sur le trafic réseau si le débit est constamment inférieur à vos attentes.
- Connexions de la base de données – Envisagez de limiter les connexions de la base de données si vous constatez un nombre important de connexions utilisateur conjointement avec une baisse des performances de l'instance et des temps de réponse. Le bon nombre de connexions utilisateur pour votre instance de base de données dépendra de votre classe d'instance et de la complexité des opérations exécutées. Vous pouvez déterminer le nombre de connexions de la base de données en associant votre instance de base de données à un groupe de paramètres dans lequel le paramètre Connexions utilisateur est configuré sur un autre chiffre que 0 (illimité). Vous pouvez utiliser un groupe de paramètres existant ou en créer un nouveau. Pour plus d'informations, consultez Utilisation de groupes de paramètres de base de données (p. 225).
- Métriques IOPS – Les valeurs attendues pour les métriques d'IOPS par seconde dépendent de la spécification du disque et de la configuration du serveur, donc utilisez vos données de référence pour

connaître les caractéristiques typiques. Enquêtez si les valeurs sont constamment différentes de vos données de référence. Pour de meilleures performances d'I/O par seconde, veillez à ce que votre ensemble de travail typique puisse être chargé en mémoire pour minimiser les opérations de lecture et écriture.

Si vous rencontrez des problèmes avec les métriques de performances, l'une des premières choses à faire pour améliorer les choses est de régler les requêtes les plus utilisées et onéreuses pour réduire la pression exercée sur les ressources système. Pour plus d'informations, consultez Réglage des requêtes (p. 140)

Si vos requêtes sont réglées et que le problème persiste, envisagez de mettre à jour votre Amazon RDS Classes d'instances de base de données (p. 6) vers une classe contenant plus de ressources (processeur, RAM, espace disque, bande passante réseau, capacité d'I/O) qui sont liées au problème que vous rencontrez.

Réglage des requêtes

L'un des meilleurs moyens d'améliorer les performances d'une instance de base de données est de régler les requêtes les plus communément utilisées et exigeantes en ressources pour les rendre moins onéreuses à exécuter.

Réglage des requêtes MySQL

Veuillez consulter Optimisation des déclarations SELECT dans la documentation MySQL pour plus d'informations sur l'écriture des requêtes afin d'améliorer les performances. Vous pouvez également consulter MySQL Performance Tuning and Optimization Resources (Ressources d'optimisation et de réglage de performance MySQL) pour des ressources supplémentaires de réglage des requêtes.

Réglage des requêtes Oracle

Consultez Database SQL Tuning Guide (Guide de réglage Database SQL) dans la documentation Oracle pour plus d'informations sur l'écriture et l'analyse des requêtes afin d'améliorer les performances.

Réglage des requêtes SQL Server

Consultez Analyzing a Query (Analyse d'une requête) dans la documentation SQL Server afin d'améliorer les requêtes pour les instances de base de données SQL Server. Vous pouvez également utiliser les vues de gestion dynamique (DMV) liées à l'exécution, l'index et aux I/O décrites dans la documentation Dynamic Management Views and Functions (Fonctions et vues de gestion dynamique) pour résoudre vos problèmes de requêtes SQL Server.

Un aspect courant du réglage de requête est la création d'index efficaces. Vous pouvez utiliser Assistant de réglage du moteur de base de données afin d'obtenir des améliorations potentielles d'index pour votre instance de base de données. Pour plus d'informations, consultez Analyse de la charge de travail d'une base de données sur une instance de base de données Amazon RDS avec l'Assistant Paramétrage SQL Server (p. 762).

Réglage des requêtes PostgreSQL

Consultez Using EXPLAIN (Utilisation de EXPLAIN) dans la documentation PostgreSQL pour savoir comment analyser un plan de requête. Vous pouvez utiliser ces informations pour modifier une requête ou des tables sous-jacentes afin d'améliorer les performances des requêtes. Vous pouvez également consulter Controlling the Planner with Explicit JOIN Clauses (Contrôler le planificateur avec des clauses JOIN explicites) pour obtenir des astuces sur la façon dont vous pouvez spécifier des jointures dans votre requête afin d'améliorer les performances.

Réglage des requêtes MariaDB

Consultez Query Optimizations (Optimisations de requêtes) dans la documentation MariaDB pour plus d'informations sur l'écriture des requêtes afin d'améliorer les performances.

Bonnes pratiques pour utiliser les moteurs de stockage MySQL

Sur une instance de base de données MySQL, observez les limites de création de table suivantes :

- Vous êtes limité à 10 000 tables si vous utilisez un stockage sur volumes d'IOPS provisionnées ou un stockage à usage général et que l'instance de base de données a une taille de 200 Gio ou plus.
- Vous êtes limité à 1000 tables si vous utilisez un stockage magnétique ou un stockage à usage général et que l'instance de base de données a une taille inférieure à 200 Gio.

Nous vous recommandons ces limites, car la quantité des tables augmente de façon significative le temps de récupération après un basculement ou une défaillance de la base de données. Si vous avez besoin de créer plus de tables que le nombre recommandé, configurez le paramètre `innodb_file_per_table` sur 0. Pour plus d'informations, consultez Utilisation des tablespaces InnoDB pour améliorer les temps de récupération sur incident (p. 882) et Utilisation de groupes de paramètres de base de données (p. 225).

Pour les instances de base de données MySQL qui utilisent la version 5.7 ou ultérieure, vous pouvez dépasser ces limites de création des tables grâce aux progrès faits en termes de récupération d'incident InnoDB. Cependant, nous vous recommandons de faire attention en raison de l'impact potentiel de la création d'un grand nombre de tables sur les performances.

Sur une instance de base de données MySQL, évitez que les tables de votre base de données deviennent trop volumineuses. Bien que la limite du stockage général soit de 64 Tio,les limites de stockage alloué réduisent la taille maximale d'un fichier de table MySQL à 64 To. Partitionnez vos tables volumineuses pour que la taille des fichiers soit inférieure à la limite de 16 To. Cette approche peut également améliorer les performances et le temps de récupération. Pour plus d'informations, consultez Limites de taille des fichiers MySQL dans Amazon RDS (p. 898).

Les fonctions de restauration à un instant dans le passé et de restauration d'instantané d'Amazon RDS pour MySQL nécessitent un moteur de stockage tolérant aux incidents et sont prises en charge uniquement pour le moteur de stockage InnoDB. Bien que MySQL prenne en charge plusieurs moteurs de stockage avec diverses capacités, toutes ne sont pas optimisées pour la récupération sur incident et la durabilité des données. Par exemple, le moteur de stockage MyISAM ne prend pas en charge une récupération sur incident fiable et peut empêcher la restauration à un instant dans le passé ou la restauration de instantané de fonctionner comme prévu. Cela peut entraîner la perte ou la corruption de données lors du redémarrage de MySQL après un incident.

InnoDB est le moteur de stockage recommandé et pris en charge pour les instances de base de données MySQL sur Amazon RDS. Les instances InnoDB peuvent également être migrées vers Aurora, au contraire des instances MySQL. Toutefois, les performances de MyISAM sont meilleures qu'InnoDB si vous avez besoin de capacités intenses de recherche en texte intégral. Si vous choisissez d'utiliser MyISAM avec Amazon RDS, suivre les étapes décrites dans Sauvegardes automatiques avec moteurs de stockage MySQL non pris en charge (p. 326) peut être utile dans certaines situations pour la fonctionnalité de restauration d'instantané.

Si vous souhaitez convertir les tables MyISAM existantes en tables InnoDB, vous pouvez utiliser le processus décrit dans la documentation MySQL. MyISAM et InnoDB ont des forces et des faiblesses différentes, vous devriez donc commencer par évaluer de façon exhaustive l'impact de ce basculement sur vos applications.

De plus, Federated Storage Engine n'est pour l'instant pas pris en charge par Amazon RDS pour MySQL.

Bonnes pratiques pour utiliser les moteurs de stockage MariaDB

Les fonctions de restauration à un instant dans le passé et de restauration d'instantané d'Amazon RDS pour MariaDB nécessitent un moteur de stockage tolérant aux incidents. Bien que MariaDB prenne en charge plusieurs moteurs de stockage avec diverses capacités, toutes ne sont pas optimisées pour la récupération sur incident et la durabilité des données. Par exemple, bien qu'Aria soit un remplacement sûr en cas d'incident pour MyISAM, il peut empêcher une restauration à un instant dans le passé ou la restauration de snapshot de fonctionner comme prévu. Cela peut entraîner la perte ou la corruption de données lors du redémarrage de MariaDB après un incident. InnoDB (pour la version 10.2 et les versions suivantes) et XtraDB (pour les versions 10.0 et 10.1) sont les moteurs de stockage recommandés et pris en charge pour les instances de base de données MariaDB sur Amazon RDS. Si vous choisissez d'utiliser Aria avec Amazon RDS, suivre les étapes décrites dans Sauvegardes automatiques avec moteurs de stockage MariaDB non pris en charge (p. 327) peut être utile dans certaines situations pour la fonctionnalité de restauration d'instantané.

Bonnes pratiques d'utilisation d'Oracle

Pour de plus amples informations sur les bonnes pratiques d'utilisation de Amazon RDS pour Oracle, veuillez consulter Bonnes pratiques pour l'exécution d'une base de données Oracle sur Amazon Web Services.

Un atelier virtuel AWS 2020 comprenait une présentation sur l'exécution de bases de données Oracle de production sur Amazon RDS. Une vidéo de la présentation est disponible ici.

Bonnes pratiques pour utiliser les moteurs de stockage PostgreSQL

Les deux principaux domaines dans lesquels vous pouvez améliorer les performances avec PostgreSQL sur Amazon RDS sont lorsque vous chargez des données dans une instance de base de données ou que vous utilisez la fonction autovacuum de PostgreSQL. Les sections suivantes couvrent certaines pratiques que nous recommandons pour ces domaines en particulier.

Chargement des données dans une instance de base de données PostgreSQL

Lors du chargement des données dans une instance de base de données PostgreSQL Amazon RDS, vous devez modifier les paramètres de l'instance et les valeurs du groupe de paramètres de base de données pour permettre l'importation la plus efficace possible des données dans votre instance de base de données.

Modifiez les paramètres de l'instance de base de données comme suit :

- Désactivez les sauvegardes de l'instance de base de données (affectez la valeur 0 à backup_retention)
- Désactivez le mode multi-AZ

Modifiez votre groupe de paramètres DB pour inclure les paramètres suivants. Vous devez tester les réglages des paramètres pour déterminer les réglages les plus efficaces pour votre instance de base de données :

- Augmentez la valeur du paramètre `maintenance_work_mem`. Pour plus d'informations sur l'utilisation de la ressource PostgreSQL, consultez la documentation sur PostgreSQL.
- Augmentez la valeur des paramètres `checkpoint_segments` et `checkpoint_timeout` pour réduire le nombre d'écritures dans le journal wal.
- Désactivez le paramètre `synchronous_commit` (ne désactivez pas FSYNC).
- Désactivez le paramètre autovacuum de PostgreSQL.
- Assurez-vous qu'aucune des tables que vous importez n'est pas journalisée. Les données stockées dans les tables non journalisées peuvent être perdues lors d'un basculement. Pour de plus amples informations, veuillez consulter CREATE TABLE UNLOGGED

Utilisez les commandes `pg_dump -Fc` (compressé) ou `pg_restore -j` (parallèle) avec ces paramètres.

Une fois l'opération de chargement terminée, réinitialisez votre instance de base de données et les paramètres de base de données à leurs paramètres normaux.

Utilisation de la fonction autovacuum de PostgreSQL

La fonction autovacuum pour les bases de données PostgreSQL est une fonction que nous vous recommandons vivement d'utiliser pour maintenir l'état de votre instance de bases de données PostgreSQL. Autovacuum automatise l'exécution des commandes VACUUM et ANALYZE ; son utilisation est exigée par PostgreSQL, non imposée par Amazon RDS et essentielle pour garantir de bonnes performances. La fonction est activée par défaut pour toutes les nouvelles instances de bases de données PostgreSQL Amazon RDS, et les paramètres de configuration associés sont configurés par défaut de manière appropriée.

Votre administrateur de base de données doit connaître et comprendre cette opération de maintenance. Pour accéder à la documentation PostgreSQL sur la fonction autovacuum, veuillez consulter Routine Vacuuming.

Autovacuum n'est pas une opération « sans utilisation de ressources », mais elle fonctionne en arrière-plan et profite autant que possible aux opérations utilisateur. Lorsqu'elle est activée, la fonction autovacuum vérifie les tables ayant eu un grand nombre de tuples mis à jour ou supprimés. Elle protège également contre la perte de données très anciennes due au renvoi à la ligne de l'ID de transaction. Pour de plus amples informations, veuillez consulter Preventing Transaction ID Wraparound Failures.

Autovacuum ne doit pas être considérée comme une opération aux frais généraux élevés qui peut être réduite pour améliorer les performances. Au contraire, les tables qui mettent à jour et suppriment très rapidement se détériorent vite avec le temps si la fonction autovacuum n'est pas exécutée.

> **Important**
>
> La non-exécution de la fonction autovacuum peut entraîner un arrêt obligatoire ultérieur pour effectuer une opération de nettoyage bien plus intrusive. Lorsqu'une instance de base de données PostgreSQL Amazon RDS devient indisponible en raison d'une faible utilisation d'autovacuum, la base de données PostgreSQL se ferme pour se protéger. À ce stade, Amazon RDS doit effectuer un nettoyage complet en mode utilisateur unique directement sur l'instance de base de données, ce qui peut entraîner un arrêt de plusieurs heures. Nous vous recommandons donc vivement de ne pas désactiver la fonction autovacuum, qui est activée par défaut.

Les paramètres d'autovacuum déterminent sa fréquence et son intensité de travail. Les paramètres `autovacuum_vacuum_threshold` et `autovacuum_vacuum_scale_factor` déterminent le moment où la fonction autovacuum est exécutée. Les paramètres `autovacuum_max_workers`, `autovacuum_nap_time`, `autovacuum_cost_limit` et `autovacuum_cost_delay` déterminent l'intensité de travail d'autovacuum. Pour de plus amples informations sur la fonction autovacuum, son exécution et les paramètres obligatoires, veuillez consulter la documentation PostgreSQL.

La requête suivante indique le nombre de tuples « inactifs » dans une table appelée 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';
```

Les résultats de la requête ressembleront à l'exemple ci-dessous :

```
relname | n_dead_tup | last_vacuum | last_autovacuum
---------+------------+-------------+-----------------
 tasks   |   81430522 |             |
(1 row)
```

Bonnes pratiques pour l'utilisation de SQL Server

Les bonnes pratiques pour un déploiement multi-AZ avec une instance de base de données SQL Server sont les suivantes :

- Utilisez les événements de base de données Amazon RDS pour surveiller les basculements. Par exemple, vous pouvez être notifié par sms ou e-mail en cas de basculement d'une instance de base de données. Pour plus d'informations sur les événements Amazon RDS, consultez Utilisation de la notification d'événement Amazon RDS (p. 467)
- Si votre application met en cache des valeurs DNS, configurez la durée de vie à moins de 30 secondes. La configuration de la durée de vie est une bonne pratique en tant que tel en cas de basculement, car l'adresse IP peut changer et la valeur mise en cache peut ne plus être en service.
- Nous vous recommandons de ne pas activer les modes suivants car ils désactivent la journalisation des transactions, qui est obligatoire pour le déploiement multi-AZ :
  - Mode de récupération simple
  - Mode hors ligne
  - Mode lecture seule
- Testez pour déterminer combien de temps votre instance de base de données met-elle pour basculer. Les délais de basculement peuvent varier en raison du type de base de données, la classe d'instance et le type de stockage utilisé. Vous devez également tester la capacité de votre application à continuer de fonctionner en cas de basculement.
- Pour raccourcir les délais de basculement, vous devez procéder comme suit :
  - Veillez à avoir suffisamment d'IOPS provisionnées allouées pour votre charge de travail. Des I/O inadaptées peuvent augmenter les délais de basculement. La récupération d'une base de données exige des I/O.
  - Utilisez de plus petites transactions. La récupération de la base de données repose sur les transactions, donc si vous pouvez séparer d'importantes transactions en plusieurs transactions plus petites, vos délais de basculement devraient diminuer.
- Pensez que lors d'un basculement, les temps de latence sont élevés. Dans le cadre d'un processus de basculement, Amazon RDS réplique automatiquement vos données vers une nouvelle instance de secours. Cette réplication signifie que de nouvelles données sont copiées dans deux instances de base de données différentes, il se peut donc qu'il y ait une certaine latence jusqu'à ce que l'instance de base de données de secours rattrape la nouvelle instance de base de données principale.
- Déployez vos applications dans toutes les zones de disponibilité. Si une zone de disponibilité tombe en panne, vos applications qui se trouvent dans les autres zones de disponibilité seront toujours disponibles.

Lorsque vous travaillez avec un déploiement multi-AZ de SQL Server, rappelez-vous qu'Amazon RDS crée des réplicas pour toutes les bases de données SQL Server sur votre instance. Si vous ne souhaitez pas que des bases de données spécifiques aient des réplicas secondaires, configurez une instance de base de données séparée qui n'utilise pas de déploiement multi-AZ pour ces bases de données.

Vidéo sur les bonnes pratiques SQL Server Amazon RDS

La conférence AWS re:Invent 2019 incluait une présentation sur les nouvelles fonctionnalités et sur les bonnes pratiques pour travailler avec SQL Server sur Amazon RDS. Une vidéo de la présentation est disponible ici.

Utilisation des groupes de paramètres DB

Nous vous recommandons de tester les modifications apportées aux groupes de paramètres de base de données sur une instance de base de données test avant d'appliquer ces modifications à vos instances de base de données de production. La configuration incorrecte de paramètres de moteur DB dans un groupe de paramètres de base de données peut avoir des effets contraires involontaires, notamment une dégradation de la performance et une instabilité du système. Montrez-vous toujours prudent lorsque vous modifiez des paramètres de moteur DB et sauvegardez votre instance de base de données avant de modifier un groupe de paramètres de base de données.

Pour plus d'informations sur la sauvegarde de votre instance de base de données, consultez Sauvegarde et restauration d'une instance de base de données Amazon RDS (p. 317).

Vidéo de présentation des nouvelles fonctionnalités et des bonnes pratiques pour Amazon RDS

La conférence AWS re:Invent 2019 incluait une présentation sur les nouvelles fonctionnalités et sur les bonnes pratiques pour Amazon RDS pour la surveillance, l’analyse et le réglage des performances d’une base de données utilisant RDS. Une vidéo de la présentation est disponible ici.

Configuration d'une instance de base de données Amazon RDS

Cette section décrit comment configurer votre instance de base de données Amazon RDS. Avant de créer une instance de base de données, choisissez la classe d'instance de base de données qui exécutera l'instance de base de données. Vous devez également déterminer l'emplacement d'exécution de l'instance de base de données en choisissant une région AWS. Créez ensuite l'instance de base de données.

Rubriques

- Création d'une instance de base de données Amazon RDS (p. 146)
- Connexion à une instance de base de données Amazon RDS (p. 169)
- Utilisation de groupes d'options (p. 209)
- Utilisation de groupes de paramètres de base de données (p. 225)

Création d'une instance de base de données Amazon RDS

La composante de base de Amazon RDS est l'instance de base de données dans laquelle vous créez vos bases de données. Vous choisissez les caractéristiques propres au moteur de l'instance de base de données lorsque vous la créez. Vous choisissez également la capacité de stockage, l'UC, la mémoire, etc. de l'instance AWS sur laquelle le serveur de base de données est exécuté.

> Important
>
> Vous devez réaliser les tâches de la section Configuration pour Amazon RDS (p. 62) avant de créer une instance de base de données ou de vous y connecter.

Console

Vous pouvez créer une instance de base de données à l'aide d'AWS Management Console, avec l'option Easy Create (Création facile) activée ou désactivée. Lorsque l'option Easy Create (Création facile) est activée, vous spécifiez uniquement le type de moteur, la taille et l'identifiant d'instance de base de données. Easy Create (Création facile) utilise les paramètres par défaut pour les autres options de configuration. Lorsque l'option Easy Create (Création facile) est désactivée, vous spécifiez davantage d'options de configuration lors de la création d'une base de données, notamment en matière de disponibilité, de sécurité, de sauvegardes et de maintenance.

> Note
>
> Dans la procédure suivante, Standard Create (Création standard) est activé et Easy Create (Création facile) est désactivé. Cette procédure utilise Microsoft SQL Server à titre d'exemple. Pour obtenir des exemples qui utilisent Easy Create (Création facile) pour vous aider à créer et à vous connecter à des exemples d'instances de base de données pour chaque moteur, veuillez consulter Mise en route avec Amazon RDS (p. 69). Pour obtenir un exemple qui utilise la console d'origine pour créer une instance de base de données, veuillez consulter Exemple de console d'origine (p. 165).

Pour créer une instance de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.

2. Dans le coin supérieur droit de la console Amazon RDS, choisissez la région AWS dans laquelle vous voulez créer l'instance de base de données.
3. Dans la panneau de navigation, choisissez Databases (Bases de données).
4. Choisissez Create database (Créer une base de données).
5. Dans Choose a database creation method (Choisir une méthode de création de base de données), sélectionnez Standard Create (Création standard).
6. Dans Engine options (Options de moteur), choisissez le type de moteur : MariaDB, Microsoft SQL Server, MySQL, Oracle ou PostgreSQL. Microsoft SQL Server est illustré ici.

7. Dans Edition (Édition), si vous utilisez Oracle ou SQL Server, choisissez l'édition du moteur de base de données que vous souhaitez utiliser.

   MySQL n'a qu'une seule option pour l'édition, tandis que MariaDB et PostgreSQL n'en ont aucune.
8. Dans Version, choisissez la version du moteur.
9. Dans Templates (Modèles), sélectionnez le modèle qui correspond à votre cas d'utilisation. Si vous choisissez Production, les éléments suivants sont présélectionnés lors d'une étape ultérieure :

   - Option de basculement Multi-AZ
   - Option de stockage IOPS provisionnés
   - Option Enable deletion protection (Activer la protection contre la suppression)

   Ces fonctions sont recommandées pour tous les environnements de production.

   > **Note**
   >
   > Les choix de modèles varient selon l'édition.
10. Pour entrer votre mot de passe principal, procédez comme suit :

    a. Dans la section Settings (Paramètres), ouvrez Credential Settings (Paramètres des informations d'identification).
    b. Décochez la case Auto generate a password (Générer un mot de passe automatiquement).
    c. (Facultatif) Modifiez la valeur du champ Master username (Identifiant principal) et saisissez le même mot de passe dans les champs Master password (Mot de passe principal) et Confirm password (Confirmer le mot de passe).

    Par défaut, la nouvelle instance de base de données utilise un mot de passe généré automatiquement pour l'utilisateur principal.
11. Pour les sections restantes, spécifiez vos paramètres d'instance de base de données. Pour plus d'informations sur chaque paramètre, consultez Paramètres des instances de base de données (p. 151).
12. Choisissez Create database (Créer une base de données).

    Si vous choisissez de générer un mot de passe automatiquement, le bouton View credential details (Afficher les informations d'identification) apparaît sur la page Databases (Bases de données).

    Pour afficher l'identifiant principal et le mot de passe pour l'instance de base de données, choisissez View credential details (Afficher les informations d'identification).

    Pour vous connecter à l'instance de base de données en tant qu'utilisateur principal, utilisez l'identifiant et le mot de passe affichés.

    > **Important**
    >
    > Vous ne pourrez pas afficher le mot de passe de l'utilisateur principal de nouveau. Si vous ne l'enregistrez pas, il sera peut-être nécessaire de le modifier. Si vous devez changer le mot de passe de l'utilisateur principal une fois l'instance de base de données disponible, faites-le en modifiant l'instance de base de données. Pour de plus amples informations sur la modification

d'une instance de base de données, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

13. Pour Databases (Bases de données), choisissez le nom de la nouvelle instance de base de données.

    Sur la console RDS, les détails de la nouvelle instance de base de données s'affichent. L'instance de base de données a le statut creating (création en cours) jusqu'à ce qu'elle soit créée et prête à l'emploi. Lorsque l'état devient available (disponible), vous pouvez vous connecter à l'instance de base de données. En fonction du stockage et de la classe d'instance de base de données alloués, la mise à disposition de la nouvelle instance de base de données peut nécessiter plusieurs minutes.

AWS CLI

Pour créer une instance de base de données à l'aide d'AWS CLI, appelez la commande create-db-instance avec les paramètres suivants. Cet exemple utilise Microsoft SQL Server.

Pour plus d'informations sur chaque paramètre, consultez Paramètres des instances de base de données (p. 151).

- `--db-instance-identifier`
- `--db-instance-class`
- `--db-security-groups`
- `--db-subnet-group`
- `--engine`
- `--master-username`
- `--master-user-password`
- `--allocated-storage`
- `--backup-retention-period`

Example

Pour Linux, macOS ou Unix :

```
aws rds create-db-instance
    --engine sqlserver-se \
    --db-instance-identifier mymsftsqlserver \
    --allocated-storage 250 \
    --db-instance-class db.t3.large \
    --db-security-groups mydbsecuritygroup \
    --db-subnet-group mydbsubnetgroup \
    --master-username masterawsuser \
```

```
    --master-user-password masteruserpassword \
    --backup-retention-period 3
```

Pour Windows :

```
aws rds create-db-instance ^
    --engine sqlserver-se ^
    --db-instance-identifier mydbinstance ^
    --allocated-storage 250 ^
    --db-instance-class db.t3.large ^
    --db-security-groups mydbsecuritygroup ^
    --db-subnet-group mydbsubnetgroup ^
    --master-username masterawsuser ^
    --master-user-password masteruserpassword ^
    --backup-retention-period 3
```

Le résultat produit lors de l'exécution de cette commande est semblable à ce qui suit :

```
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
```

API RDS

Pour créer une instance de base de données à l'aide de l'API Amazon RDS, appelez l'opération CreateDBInstance avec les paramètres suivants. Cet exemple utilise Microsoft SQL Server.

Pour plus d'informations sur chaque paramètre, consultez Paramètres des instances de base de données (p. 151).

- `AllocatedStorage`
- `BackupRetentionPeriod`
- `DBInstanceClass`
- `DBInstanceIdentifier`
- `DBSecurityGroups`
- `DBSubnetGroup`
- `Engine`
- `MasterUsername`
- `MasterUserPassword`

Example

```
https://rds.amazonaws.com/
    ?Action=CreateDBInstance
    &AllocatedStorage=250
    &BackupRetentionPeriod=3
    &DBInstanceClass=db.t3.large
    &DBInstanceIdentifier=mydbinstance
    &DBSecurityGroups.member.1=mysecuritygroup
    &DBSubnetGroup=mydbsubnetgroup
    &Engine=sqlserver-se
    &MasterUserPassword=masteruserpassword
    &MasterUsername=masterawsuser
    &SignatureMethod=HmacSHA256
```

```
&SignatureVersion=4
&Version=2014-10-31
&X-Amz-Algorithm=AWS4-HMAC-SHA256
&X-Amz-Credential=AKIADQKE4SARGYLE/20140305/us-west-1/rds/aws4_request
&X-Amz-Date=20140305T185838Z
&X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
&X-Amz-Signature=b441901545441d3c7a48f63b5b1522c5b2b37c137500c93c45e209d4b3a064a3
```

Paramètres des instances de base de données

Le tableau suivant contient des détails sur les paramètres que vous choisissez lors de la création d'une instance de base de données. Le tableau répertorie également les moteurs de base de données pour lesquels chaque paramètre est pris en charge.

Vous pouvez créer une instance de base de données à l'aide de la console, de la commande d'interface de ligne de commande `create-db-instance` ou de l'opération d'API RDS `CreateDBInstance`.

Paramètre de la console	Description du paramètre	Option de l'interface de ligne de commande et paramètre de l'API RDS	Moteurs de base de données pris en charge

Stockage alloué	Volume de stockage à allouer pour votre instance de base de données (en gigaoctets). Dans certains cas, allouer une quantité de stockage pour votre instance de base de données supérieure à la taille de votre base de données permet d'améliorer les performances d'E/S.
	
	Pour plus d'informations, consultez Stockage d'instance de base de données Amazon RDS (p. 30).
		Option de l'interface de ligne de commande :
		
		`--allocated-storage`
		
		Paramètre de l'API :
		
		`AllocatedStorage`
			Tous

Mise à niveau automatique des versions mineures	Activez Mise à niveau automatique des versions mineures pour permettre à votre instance de base de données de recevoir automatiquement les mises à niveau de la version mineure préférée du moteur de base de données lorsqu'elles sont disponibles. Amazon RDS effectue les mises à niveau automatiques des versions mineures dans la fenêtre de maintenance.	Option de l'interface de ligne de commande :
		
		`--auto-minor-version-upgrade`
		
		`--no-auto-minor-version-upgrade`
		
		Paramètre de l'API :
		
		`AutoMinorVersionUpgrade`
			Tous sauf SQL Server

Zone de disponibilité	Zone de disponibilité de votre instance de base de données. Utilisez la valeur par défaut No Preference (Aucune préférence), sauf si vous souhaitez spécifier une zone de disponibilité.
	
	Pour plus d'informations, consultez Régions, zones de disponibilité et zones locales (p. 39).
		Option de l'interface de ligne de commande :
		
		`--availability-zone`
		
		Paramètre de l'API :
		
		`AvailabilityZone`
			Tous

Paramètre de la console	Description du paramètre	Option de l'interface de ligne de commande et paramètre de l'API RDS	Moteurs de base de données pris en charge

Période de rétention des sauvegardes	Nombre de jours durant lesquels les sauvegardes automatiques de votre instance de base de données doivent être conservées. Pour une instance de base de données importante, définissez cette valeur sur `1` ou une valeur supérieure.
	
	Pour plus d'informations, consultez Utilisation des sauvegardes (p. 317).
		Option de l'interface de ligne de commande :
		
		`--backup-retention-period`
		
		Paramètre de l'API :
		
		`BackupRetentionPeriod`
			Tous

Fenêtre de sauvegarde	Période de temps durant laquelle Amazon RDS effectue automatiquement une sauvegarde de votre instance de base de données. Si vous n'avez pas besoin que votre base de données soit sauvegardée à un moment précis, utilisez la valeur par défaut No Preference (Aucune préférence).
	
	Pour plus d'informations, consultez Utilisation des sauvegardes (p. 317).
		Option de l'interface de ligne de commande :
		
		`--preferred-backup-window`
		
		Paramètre de l'API :
		
		`PreferredBackupWindow`
			Tous

Jeu de caractères	Jeu de caractères pour l'instance de base de données. La valeur par défaut AL32UTF8 pour le jeu de caractères de base de données est pour le jeu de caractères Unicode 5.0 UTF-8 Universal. Vous ne pouvez pas modifier le jeu de caractères de base de données après avoir créé l'instance de base de données.
	
	Le jeu de caractères de base de données est différent du jeu de caractères national, appelé jeu de caractères NCHAR. Contrairement au jeu de caractères de base de données, le jeu de caractères NCHAR spécifie le codage des colonnes des types de données NCHAR (NCHAR, NVARCHAR2 et NCLOB) sans affecter les métadonnées de base de données.
	
	Pour plus d'informations, consultez Jeux de caractères Oracle pris en charge dans Amazon RDS (p. 1010).
		Option de l'interface de ligne de commande :
		
		`--character-set-name`
		
		Paramètre de l'API :
		
		`CharacterSetName`
			Oracle

Paramètre de la console	Description du paramètre	Option de l'interface de ligne de commande et paramètre de l'API RDS	Moteurs de base de données pris en charge

Classement (Collation)	Classement de niveau serveur pour votre instance de base de données.
	
	Pour plus d'informations, consultez Classement de niveau serveur pour Microsoft SQL Server (p. 766).
		Option de l'interface de ligne de commande :
		
		`--character-set-name`
		
		Paramètre de l'API :
		
		`CharacterSetName`
			SQL Server

Copier les balises aux instantanés	Cette option copie les balises de l'instance de base de données dans un instantané de base de données au moment où vous créez un instantané.
	
	Pour plus d'informations, consultez Balisage de ressources Amazon RDS (p. 293).
		Option de l'interface de ligne de commande :
		
		`--copy-tags-to-snapshot`
		
		`--no-copy-tags-to-snapshot`
		
		Paramètre de l'API RDS :
		
		`CopyTagsToSnapshot`
			Tous

Port de la base de données	Port par lequel vous souhaitez accéder à l'instance de base de données. La valeur par défaut du port est indiquée. Si vous utilisez un groupe de sécurité de base de données avec votre instance de base de données, cette valeur de port doit être identique à celle que vous avez fournie au moment de créer le groupe de sécurité de base de données.
	
	Note
	
	Dans certaines entreprises, les pare-feux bloquent les connexions aux ports MariaDB, MySQL et PostgreSQL par défaut. Si le pare-feu de votre entreprise bloque le port par défaut, entrez un autre port pour votre instance de base de données.
		Option de l'interface de ligne de commande :
		
		`--port`
		
		Paramètre de l'API RDS :
		
		`Port`
			Tous

Paramètre de la console	Description du paramètre	Option de l'interface de ligne de commande et paramètre de l'API RDS	Moteurs de base de données pris en charge

Authentification de base de données	L'option d'authentification de base de données que vous souhaitez utiliser.
	
	Choisissez Authentification par mot de passe pour authentifier les utilisateurs de base de données avec des mots de passe de base de données uniquement.
	
	Choisissez Mot de passe et authentification de base de données IAM pour authentifier les utilisateurs de base de données avec des mots de passe de base de données et des informations d'identification utilisateur via des utilisateurs et rôles IAM. Pour plus d'informations, consultez Authentification de base de données IAM pour MySQL et PostgreSQL (p. 1554). Cette option n'est prise en charge que pour MySQL et PostgreSQL.
	
	Choisissez Mot de passe et authentification Kerberos pour authentifier les utilisateurs de base de données avec des mots de passe de base de données et l'authentification Kerberos via un Microsoft AD géré par AWS créé avec AWS Directory Service. Ensuitez, choisissez le répertoire ou Créer un nouveau répertoire.
	
	Pour plus d'informations, consultez les étapes suivantes :
	
	• Utilisation de l'authentification Kerberos pour MySQL (p. 885)
	• Utilisation de l'authentification Kerberos avec Amazon RDS for Oracle (p. 1168)
	• Utilisation de l'authentification Kerberos avec Amazon RDS pour PostgreSQL (p. 1450)
		IAM :
		
		Option de l'interface de ligne de commande :
		
		`--enable-iam-database-authentication`
		
		`--no-enable-iam-database-authentication`
		
		Paramètre de l'API RDS :
		
		`EnableIAMDatabaseAuthentication`
		
		Kerberos :
		
		Option de l'interface de ligne de commande :
		
		`--domain`
		
		`--domain-iam-role-name`
		
		Paramètre de l'API RDS :
		
		`Domain`
		
		`DomainIAMRoleName`
			MySQL
			
			Oracle
			
			PostgreSQL

Paramètre de la console	Description du paramètre	Option de l'interface de ligne de commande et paramètre de l'API RDS	Moteurs de base de données pris en charge

Version du moteur de base de données	Version du moteur de base de données que vous souhaitez utiliser.	Option de l'interface de ligne de commande :
		
		`--engine-version`
		
		Paramètre de l'API RDS :
		
		`EngineVersion`
			Tous

Classe d'instance de base de données	Configuration pour votre instance de base de données. Par exemple, une classe d'instance db.t3.small a 2 Gio de mémoire, 2 vCPU, 1 cœur virtuel, un calculateur variable et une capacité d'E/S modérée.
	
	Dans la mesure du possible, choisissez une classe d'instance suffisamment grande pour qu'un ensemble de travail de requête classique puisse tenir dans la mémoire. Lorsque les ensembles de travail sont en mémoire, le système peut éviter d'écrire sur le disque, ce qui améliore les performances.
	
	Pour plus d'informations, consultez Classes d'instances de base de données (p. 6).
		Option de l'interface de ligne de commande :
		
		`--db-instance-class`
		
		Paramètre de l'API RDS :
		
		`DBInstanceClass`
			Tous

Identifiant d'instance de base de données	Nom de votre instance de base de données. Nommez vos instances de base de données de la même façon que vos serveurs sur site. Votre identifiant d'instance de base de données peut contenir jusqu'à 63 caractères alphanumériques et doit être unique pour votre compte dans la région AWS que vous avez choisie. Vous pouvez compliquer le nom, en incluant par exemple la région AWS et le moteur de base de données de votre choix, comme suit : **`sqlsrvr-instance1`**	Option de l'interface de ligne de commande :
		
		`--db-instance-identifier`
		
		Paramètre de l'API RDS :
		
		`DBInstanceIdentifier`
			Tous

Paramètre de la console	Description du paramètre	Option de l'interface de ligne de commande et paramètre de l'API RDS	Moteurs de base de données pris en charge

Groupe de paramètres de base de données	Groupe de paramètres pour l'instance de base de données. Vous pouvez choisir le groupe de paramètres par défaut, ou vous pouvez créer un groupe de paramètres personnalisé.
	
	Pour plus d'informations, consultez Utilisation de groupes de paramètres de base de données (p. 225).
		Option de l'interface de ligne de commande :
		
		`--db-parameter-group-name`
		
		Paramètre de l'API RDS :
		
		`DBParameterGroupName`
			Tous

Deletion protection (Protection contre la suppression)	Sélectionnez Enable deletion protection (Activer la protection contre la suppression) pour empêcher la suppression de votre instance de base de données. Si vous créez une instance de base de données de production avec AWS Management Console, la protection contre la suppression est activée par défaut.
	
	Pour plus d'informations, consultez Suppression d'une instance de base de données (p. 313).
		Option de l'interface de ligne de commande :
		
		`--deletion-protection`
		
		`--no-deletion-protection`
		
		Paramètre de l'API RDS :
		
		`DeletionProtection`
			Tous

Chiffrement	Activer le chiffrement si vous souhaitez activer le chiffrement au repos pour cette instance de base de données.
	
	Pour plus d'informations, consultez Chiffrement des ressources Amazon RDS (p. 1522).
		Option de l'interface de ligne de commande :
		
		`--storage-encrypted`
		
		`--no-storage-encrypted`
		
		Paramètre de l'API RDS :
		
		`StorageEncrypted`
			Tous

Surveillance améliorée	Activer la surveillance améliorée permet d'activer la collecte des métriques en temps réel pour le système d'exploitation sur lequel votre instance de base de données s'exécute.
	
	Pour plus d'informations, consultez Surveillance améliorée (p. 394).
		Options d'interface de ligne de commande :
		
		`--monitoring-interval`
		
		`--monitoring-role-arn`
		
		Paramètres de l'API RDS :
		
		`MonitoringInterval`
		
		`MonitoringRoleArn`
			Tous

Paramètre de la console	Description du paramètre	Option de l'interface de ligne de commande et paramètre de l'API RDS	Moteurs de base de données pris en charge

Nom de la base de données initiale	Nom de la base de données dans votre instance de base de données. Si vous ne fournissez pas de nom, Amazon RDS ne crée pas de base de données sur l'instance de base de données (à l'exception d'Oracle). Le nom ne peut pas être un mot réservé par le moteur de base de données et possède d'autres contraintes selon le moteur de base de données.
	
	MariaDB et MySQL :
	
	• Il doit contenir entre 1 et 64 caractères alphanumériques.
	
	Oracle :
	
	• Il doit contenir entre 1 et 8 caractères alphanumériques.
	• Il ne peut pas être `NULL`. La valeur par défaut est ORCL.
	• Il doit commencer par une lettre.
	
	PostgreSQL :
	
	• Il doit contenir entre 1 et 63 caractères alphanumériques.
	• Il doit commencer par une lettre ou un trait de soulignement. Les caractères suivants peuvent être des lettres, des traits de soulignement ou des chiffres (0-9).
		Option de l'interface de ligne de commande :
		
		`--db-name`
		
		Paramètre de l'API RDS :
		
		`DBName`
			Tous sauf SQL Server

Licence	Le modèle de licence :
	
	• Choisissez licence-incluse pour Microsoft SQL Server.
	• Choisissez licence-incluse ou Réutilisez vos licences pour Oracle.
		Option de l'interface de ligne de commande :
		
		`--license-model`
		
		Paramètre de l'API RDS :
		
		`LicenseModel`
			SQL Server
			
			Oracle

Paramètre de la console	Description du paramètre	Option de l'interface de ligne de commande et paramètre de l'API RDS	Moteurs de base de données pris en charge

Fenêtre de maintenance	Créneau de 30 minutes pendant lequel les modifications en attente pour votre instance de base de données sont appliquées. Si la période n'a pas d'importance, choisissez No Preference (Aucune préférence).
	
	Pour plus d'informations, consultez Le créneau de maintenance Amazon RDS (p. 264).
		Option de l'interface de ligne de commande :
		
		`--preferred-maintenance-window`
		
		Paramètre de l'API RDS :
		
		`PreferredMaintenanceWindow`
			Tous

Mot de passe principal	Mot de passe de votre compte utilisateur principal. Le mot de passe comporte le nombre suivant de caractères ASCII imprimables (à l'exclusion des caractères `/`, `"`, espace et `@`) selon le moteur de base de données :
	
	• Oracle : entre 8 et 30
	• MariaDB et MySQL : entre 8 et 41
	• SQL Server et PostgreSQL : entre 8 et 128
		Option de l'interface de ligne de commande :
		
		`--master-user-password`
		
		Paramètre de l'API RDS :
		
		`MasterUserPassword`
			Tous

Paramètre de la console	Description du paramètre	Option de l'interface de ligne de commande et paramètre de l'API RDS	Moteurs de base de données pris en charge

Identifiant principal	Nom que vous utilisez comme nom d'utilisateur principal pour vous connecter à votre instance de base de données avec tous les privilèges de base de données.
	• Il peut contenir entre 1 et 16 caractères alphanumériques et des traits de soulignement.
	• Son premier caractère doit être une lettre.
	• Il ne peut pas être un mot réservé par le moteur de base de données.
	
	Pour de plus amples informations sur les privilèges accordés à l'utilisateur principal, veuillez consulter les rubriques suivantes :
	• Sécurité MariaDB sur Amazon RDS (p. 550)
	• Sécurité de Microsoft SQL Server (p. 598)
	• MySQL Security sur Amazon RDS (p. 786)
	• Sécurité Oracle (p. 937)
	• Versions et extensions Amazon RDS pour PostgreSQL (p. 1468)
		Option de l'interface de ligne de commande :
		`--master-username`
		Paramètre de l'API RDS :
		`MasterUsername`
			Tous

Authentification Windows Microsoft SQL Server	Activez l'authentification Windows pour Microsoft SQL Server, puis parcourez le répertoire pour choisir le répertoire dans lequel vous souhaitez permettre aux utilisateurs de domaine autorisés de s'authentifier auprès de cette instance SQL Server à l'aide de l'authentification Windows.	Options d'interface de ligne de commande :
		`--domain`
		`--domain-iam-role-name`
		Paramètres de l'API RDS :
		`Domain`
		`DomainIAMRoleName`
			SQL Server

Paramètre de la console	Description du paramètre	Option de l'interface de ligne de commande et paramètre de l'API RDS	Moteurs de base de données pris en charge

Déploiement multi-AZ	Create a standby instance (Créer une instance de secours) permet de créer un réplica secondaire passif de votre instance de base de données dans une autre zone de disponibilité pour la prise en charge du basculement. Nous recommandons Multi-AZ pour les charges de travail de production afin de maintenir une haute disponibilité.
	
	Pour le développement et les tests, vous pouvez choisir Do not create a standby instance (Ne pas créer d'instance de secours).
	
	Pour plus d'informations, consultez Haute disponibilité (multi-AZ) pour Amazon RDS (p. 43).
		Option de l'interface de ligne de commande :
		
		`--multi-az`
		
		`--no-multi-az`
		
		Paramètre de l'API RDS :
		
		`MultiAZ`
			Tous

Jeu de caractères national (NCHAR)	Jeu de caractères national pour votre instance de base de données, communément appelé jeu de caractères NCHAR. Vous pouvez définir le jeu de caractères national sur AL16UTF16 (par défaut) ou UTF-8. Vous ne pouvez pas modifier le jeu de caractères national après avoir créé l'instance de base de données.
	
	Le jeu de caractères national est différent du jeu de caractères de base de données. Contrairement au jeu de caractères de base de données, le jeu de caractères national spécifie le codage uniquement pour les colonnes de types de données NCHAR (NCHAR, NVARCHAR2 et NCLOB) sans affecter les métadonnées de base de données.
	
	Pour plus d'informations, consultez Jeux de caractères Oracle pris en charge dans Amazon RDS (p. 1010).
		Option de l'interface de ligne de commande :
		
		`--nchar-character-set-name`
		
		Paramètre de l'API :
		
		`NcharCharacterSetName`
			Oracle

Paramètre de la console	Description du paramètre	Option de l'interface de ligne de commande et paramètre de l'API RDS	Moteurs de base de données pris en charge

Groupe d'options	Groupe d'options pour l'instance de base de données. Vous pouvez choisir le groupe d'options par défaut, ou vous pouvez créer un groupe d'options personnalisé.
	
	Pour plus d'informations, consultez Utilisation de groupes d'options (p. 209).
		Option de l'interface de ligne de commande :
		
		`--option-group-name`
		
		Paramètre de l'API RDS :
		
		`OptionGroupName`
			Tous

Performance Insights	Activer Performance Insights permet de surveiller la charge de votre instance de base de données et ainsi d'analyser les performances de votre base de données et de résoudre les problèmes associés.
	
	Choisissez une période de rétention pour déterminer le volume d'historique des données propagées que vous voulez conserver. La valeur par défaut est de sept jours pour l'offre gratuite. La rétention à long terme (deux ans) est facturée par vCPU et par mois.
	
	Choisissez la clé principale à utiliser pour protéger la clé servant à chiffrer ce volume de base de données. Choisissez une des clés principales de votre compte ou entrez la clé d'un autre compte.
	
	Pour plus d'informations, consultez Utilisation d'Amazon RDS Performance Insights (p. 410).
		Options d'interface de ligne de commande :
		
		`--enable-performance-insights`
		
		`--no-enable-performance-insights`
		
		`--performance-insights-retention-period`
		
		`--performance-insights-kms-key-id`
		
		Paramètres de l'API RDS :
		
		`EnablePerformanceInsights`
		
		`PerformanceInsightsRetentionPeriod`
		
		`PerformanceInsightsKMSKeyId`
			Tous

Paramètre de la console	Description du paramètre	Option de l'interface de ligne de commande et paramètre de l'API RDS	Moteurs de base de données pris en charge

Accès public	Publicly accessible (Accessible publiquement) dote l'instance de base de données d'une adresse IP publique, ce qui signifie qu'elle est accessible en dehors du VPC. Pour être accessible au public, l'instance de base de données doit aussi se trouver dans un sous-réseau public du VPC.
	
	Not publicly accessible (Non accessible publiquement) rend l'instance de base de données accessible uniquement à partir de l'intérieur du VPC.
	
	Pour plus d'informations, consultez Masquer une instance de base de données dans un VPC depuis Internet (p. 1622).
	
	Pour se connecter à une instance de base de données hors de son Amazon VPC, l'instance de base de données doit être accessible au public, l'accès doit être accordé en utilisant les règles entrantes du groupe de sécurité de l'instance de base de données et d'autres exigences doivent être respectées. Pour de plus amples informations, veuillez consulter Impossible de se connecter à l'instance de base de données Amazon RDS (p. 1639).
	
	Si votre instance de base de données n'est pas accessible publiquement, vous pouvez également utiliser une connexion VPN site à site AWS ou une connexion AWS Direct Connect pour y accéder à partir d'un réseau privé. Pour de plus amples informations, veuillez consulter Confidentialité du trafic inter-réseaux (p. 1535).
		Option de l'interface de ligne de commande :
		
		`--publicly-accessible`
		
		`--no-publicly-accessible`
		
		Paramètre de l'API RDS :
		
		`PubliclyAccessible`
			Tous

Paramètre de la console	Description du paramètre	Option de l'interface de ligne de commande et paramètre de l'API RDS	Moteurs de base de données pris en charge

Dimensionnement automatique du stockage	Enable storage autoscaling (Activer le dimensionnement automatique du stockage) permet à Amazon RDS d'augmenter automatiquement l'espace de stockage quand cela est nécessaire pour éviter que votre instance de base de données en manque.
	
	Utilisez Maximum storage threshold (Seuil de stockage maximum) pour définir la limite supérieure au-delà de laquelle Amazon RDS augmente automatiquement l'espace de stockage pour votre instance de base de données. La valeur par défaut est 1 000 GiO.
	
	Pour plus d'informations, consultez Gestion automatique de la capacité avec le dimensionnement automatique du stockage Amazon RDS (p. 306).
		Option de l'interface de ligne de commande :
		
		`--max-allocated-storage`
		
		Paramètre de l'API RDS :
		
		`MaxAllocatedStorage`
			Tous

Type de stockage	Type de stockage pour votre instance de base de données.
	
	Pour plus d'informations, consultez Types de stockage Amazon RDS (p. 30).
		Option de l'interface de ligne de commande :
		
		`--storage-type`
		
		Paramètre de l'API RDS :
		
		`StorageType`
			Tous

Groupe de sous-réseaux	Ce paramètre dépend de la plateforme que vous utilisez. Si vous êtes un nouveau client AWS, choisissez par défaut, ce qui correspond au groupe de sous-réseaux de bases de données par défaut qui a été créé pour votre compte.
	
	Si vous créez une instance de base de données sur la plateforme E2-Classic précédente, vous pouvez souhaiter placer votre instance de base de données dans un VPC spécifique. Dans ce cas, choisissez le groupe de sous-réseaux de base de données que vous avez créé pour ce VPC.
		Option de l'interface de ligne de commande :
		
		`--db-subnet-group-name`
		
		Paramètre de l'API RDS :
		
		`DBSubnetGroupName`
			Tous

Paramètre de la console	Description du paramètre	Option de l'interface de ligne de commande et paramètre de l'API RDS	Moteurs de base de données pris en charge

Fuseau horaire	Fuseau horaire de votre instance de base de données. Si vous ne choisissez pas de fuseau horaire, votre instance de base de données utilise le fuseau horaire par défaut. Vous ne pouvez pas modifier le fuseau horaire après la création de l'instance de base de données.
	
	Pour plus d'informations, consultez Fuseau horaire local pour les instances de bases de données Microsoft SQL Server (p. 609).
		Option de l'interface de ligne de commande :
		
		`--timezone`
		
		Paramètre de l'API RDS :
		
		`Timezone`
			SQL Server

Virtual Private Cloud (VPC)	Ce paramètre dépend de la plateforme que vous utilisez. Si vous êtes un nouveau client AWS, choisissez le VPC par défaut indiqué. Si vous créez une instance de base de données sur la plateforme E2-Classic précédente qui n'utilise pas de VPC, sélectionnez Pas dans le VPC. Pour plus d'informations, consultez VPC Amazon Virtual Private Cloud et Amazon RDS (p. 1610).	Pour l'interface de ligne de commande et l'API, vous spécifiez les ID de groupe de sécurité VPC.	Tout

Groupe de sécurité VPC	Si vous êtes un nouveau client AWS, choisissez Create new (Créer) pour créer un groupe de sécurité VPC. Sinon, sélectionnez Choose existing (Choisir existant), puis effectuez un choix parmi les groupes de sécurité que vous avez créés précédemment.
	
	Quand vous choisissez Create new (Créer) dans la console RDS, un groupe de sécurité est créé. Ce nouveau groupe de sécurité dispose d'une règle de trafic entrant qui l'autorise à accéder à l'instance de base de données à partir de l'adresse IP détectée dans votre navigateur.
	
	Pour plus d'informations, consultez Utilisation des groupes de sécurité DB (plateforme EC2-Classic) (p. 1596).
		Option de l'interface de ligne de commande :
		
		`--vpc-security-group-ids`
		
		Paramètre de l'API RDS :
		
		`VpcSecurityGroupIds`
			Tous

Exemple de console d'origine

Vous pouvez créer une instance de base de données avec la console AWS Management Console d'origine. Cet exemple utilise Microsoft SQL Server.

Pour lancer une instance de base de données SQL Server

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le coin supérieur droit de la console Amazon RDS, choisissez la région AWS dans laquelle vous voulez créer l'instance de base de données.
3. Dans la panneau de navigation, choisissez Databases (Bases de données).

   Si le panneau de navigation est fermé, choisissez l'icône de menu en haut à gauche pour l'ouvrir.
4. Choisissez Create database (Créer une base de données) pour ouvrir la page Sélectionner un moteur.
5. Choisissez l'icône Microsoft SQL Server.

6. Sélectionnez l'édition du moteur DB SQL Server que vous voulez utiliser. Les éditions de SQL Server disponibles varient en fonction de la région AWS.
7. Pour certaines éditions, l'étape Use Case (Cas d'utilisation) demande si vous envisagez d'utiliser l'instance de base de données que vous créez pour la production. Si c'est le cas, choisissez Production. Si vous choisissez Production, tous les éléments suivants sont présélectionnés dans une étape ultérieure :

- Option de basculement Multi-AZ
- Option de stockage IOPS provisionnés
- Option Enable deletion protection (Activer la protection contre la suppression)

Ces fonctions sont recommandées pour tous les environnements de production.

8. Choisissez Next pour continuer. La page Specify DB Details (Spécifier les détails de la base de données) s'affiche.

   Sur la page Specify DB Details (Spécifier les détails de base de données), spécifiez les informations de votre instance de base de données. Pour plus d'informations sur chaque paramètre, consultez Paramètres des instances de base de données (p. 151).

9. Choisissez Next pour continuer. La page Configure Advanced Settings (Configurer les paramètres avancés) s'affiche.

   Dans la page Configure Advanced Settings (Configurer les paramètres avancés), fournissez des informations supplémentaires dont Amazon RDS a besoin pour lancer l'instance de bases de données.

Pour plus d'informations sur chaque paramètre, consultez Paramètres des instances de base de données (p. 151).

10. Choisissez Launch DB Instance (Lancer l'instance de base de données).
11. Sur la dernière page de l'assistant, choisissez Fermer.

Sur la console RDS, la nouvelle instance de base de données s'affiche dans la liste des instances de bases de données. L'instance de base de données a le statut creating (création en cours) jusqu'à ce qu'elle soit créée et prête à l'emploi. Lorsque l'état devient available (disponible), vous pouvez vous connecter à l'instance de base de données. En fonction de la quantité de stockage et de la classe d'instance de base de données, la mise à disposition de la nouvelle instance peut prendre jusqu'à 20 minutes.

Connexion à une instance de base de données Amazon RDS

Après avoir créé une instance Amazon RDS, vous pouvez utiliser n'importe quelle application cliente SQL standard pour vous connecter à l'instance de base de données. Pour vous connecter à une instance de base de données Amazon RDS, suivez les instructions pour votre moteur de base de données spécifique.

- Connexion à une instance de base de données exécutant le moteur de base de données MariaDB (p. 556)
- Connexion à une instance de base de données exécutant le moteur de base de données Microsoft SQL Server (p. 618)
- Connexion à une instance de base de données exécutant le moteur de base de données MySQL (p. 793)
- Connexion à une instance de base de données Oracle (p. 961)
- Connexion à une instance de base de données exécutant le moteur de base de données PostgreSQL (p. 1364)

Vous pouvez également utiliser Amazon RDS Proxy pour gérer les connexions aux instances de base de données MySQL et PostgreSQL. RDS Proxy autorise les applications à grouper et partager les connexions de bases de données pour améliorer l'évolutivité.

- Gestion des connexions avec Amazon RDS Proxy (p. 169)

Gestion des connexions avec Amazon RDS Proxy

En utilisant Amazon RDS Proxy, vous pouvez autoriser vos applications à grouper et partager les connexions de bases de données pour améliorer leur capacité de mise à l'échelle. RDS Proxy rend les applications plus résistantes aux défaillances de bases de données en se connectant automatiquement à une instance de base de données de secours tout en préservant les connexions des applications.RDS Proxy vous permet également d'appliquer une authentification AWS Identity and Access Management

(IAM) pour les bases de données et de stocker en toute sécurité les informations d'identification dans AWS Secrets Manager.

> Note
>
> RDS Proxy est entièrement compatible avec MySQL et PostgreSQL. Vous pouvez activer RDS Proxy pour la plupart des applications sans modifier le code.

Avec RDS Proxy, vous pouvez gérer les pics imprévisibles du trafic des bases de données qui pourraient entraîner des problèmes liés au dépassement du nombre de connexions ou à la création de connexions à un rythme rapide. RDS Proxy établit un regroupement de connexions de bases de données et réutilise les connexions de ce groupe sans la mémoire ni la surcharge de l'UC liées à l'ouverture d'une nouvelle connexion de base de données. Pour protéger la base de données contre cette congestion, vous pouvez contrôler le nombre de connexions créées.

RDS Proxy met en file d'attente ou limite les connexions des applications qui ne peuvent pas être servies immédiatement à partir du groupe de connexions. Bien que les latences puissent augmenter, votre application peut continuer à évoluer sans échouer brusquement ou surcharger la base de données. Si les demandes de connexion dépassent les limites que vous définissez, RDS Proxy rejette les connexions des applications (en d'autres termes, il déleste la charge). Parallèlement, il conserve des performances prévisibles pour la charge pouvant être desservie avec la capacité disponible.

Vous pouvez réduire la surcharge pour traiter des informations d'identification et établir une connexion sécurisée pour chaque nouvelle connexion. RDS Proxy peut gérer une partie de ce travail pour le compte de la base de données.

Rubriques

- Concepts et terminologie RDS Proxy (p. 170)
- Planification et configuration de RDS Proxy (p. 175)
- Connexion à une base de données via RDS Proxy (p. 185)
- Gestion d'un RDS Proxy (p. 188)
- Surveillance de RDS Proxy à l'aide d'Amazon CloudWatch (p. 196)
- Exemples de ligne de commande pour RDS Proxy (p. 201)
- Résolution des problèmes liés au RDS Proxy (p. 203)
- Utilisation de RDS Proxy avec AWS CloudFormation (p. 209)

Concepts et terminologie RDS Proxy

Vous pouvez simplifier la gestion des connexions pour vos instances de base de donnéesAmazon RDS et vos clusters de base de données Amazon Aurora à l'aide de RDS Proxy.

RDS Proxy gère le trafic réseau entre l'application cliente et la base de données. Il le fait d'abord de manière active en comprenant le protocole de la base de données. Il ajuste ensuite son comportement en fonction des opérations SQL de votre application et des jeux de résultats de la base de données.

RDS Proxy réduit la charge de mémoire et d'UC pour la gestion des connexions sur votre base de données. La base de données a besoin de moins de mémoire et de ressources de l'UC lorsque les applications ouvrent de nombreuses connexions simultanées. La logique n'est pas non plus nécessaire dans vos applications pour fermer et rouvrir les connexions qui restent inactives pendant longtemps. De même, il faut logique d'application moindre pour rétablir les connexions en cas de problème de base de données.

L'infrastructure de RDS Proxy est hautement disponible et déployée sur plusieurs zones de disponibilité. Le calcul, la mémoire et le stockage pour RDS Proxy sont indépendants de vos instances de base de données

RDS et de vos clusters de base de données Aurora. Cette séparation permet de réduire la surcharge sur vos serveurs de base de données, afin qu'ils puissent dédier leurs ressources à la gestion des charges de travail de base de données. Les ressources de calcul de RDS Proxy sont sans serveur et automatiquement mises à l'échelle en fonction de la charge de travail de votre base de données.

Rubriques

- Présentation des concepts RDS Proxy (p. 171)
- Regroupement de connexions (p. 172)
- Sécurité RDS Proxy (p. 172)
- Basculement (p. 173)
- Transactions (p. 174)

Présentation des concepts RDS Proxy

RDS Proxy gère l'infrastructure pour effectuer le regroupement de connexions et les autres fonctionnalités décrites ci-après. Vous voyez les serveurs proxy qui figurent dans la console RDS sur la page Proxys.

Chaque proxy gère les connexions à une seule instance de base de données RDS ou cluster de base de données Aurora. Le proxy détermine automatiquement l'instance d'enregistreur actuelle pour les instances de base de données RDS multi-AZ et les clusters provisionnés Aurora. Pour les clusters à plusieurs maîtres Aurora, le proxy se connecte à l'une des instances d'enregistreur et utilise les autres instances d'enregistreur comme cibles de secours à chaud.

Les connexions qu'un proxy garde ouvertes et disponibles pour votre application de base de données forment le groupe de connexions.

Par défaut, RDS Proxy peut réutiliser une connexion après chaque transaction dans votre session. « multiplexage » est le terme utilisé pour cette réutilisation au niveau de la transaction. Lorsque RDS Proxy supprime temporairement une connexion du groupe de connexions pour la réutiliser, cette opération est appelée un emprunt de connexion. lorsque l'opération peut être effectué sans risque, RDS Proxy renvoie cette connexion au groupe de connexions.

Dans certains cas, RDS Proxy ne peut pas s'assurer que la réutilisation d'une connexion à une base de données en dehors de la session en cours peut être effectuée sans risque. Dans ce cas, il maintient la session sur la même connexion jusqu'à la fin. Ce comportement de secours est appelé épinglage.

Un proxy est doté d'un point de terminaison. Vous vous connectez à ce point de terminaison lorsque vous utilisez une instance de base de données RDS ou un cluster de bases de données Aurora, plutôt qu'au point de terminaison en lecture-écriture qui se connecte directement à l'instance ou au cluster. Les points de terminaison à usage spécial d'un cluster Aurora restent disponibles pour vous.

Par exemple, vous pouvez toujours vous connecter au point de terminaison du cluster pour les connexions en lecture-écriture sans regroupement de connexions. Vous pouvez toujours vous connecter au point de terminaison du lecteur pour des connexions en lecture seule à charge équilibrée. Vous pouvez toujours vous connecter aux points de terminaison de l'instance pour le diagnostic et le dépannage d'instances de base de données spécifiques au sein d'un cluster Aurora. Si vous utilisez d'autres services AWS tels que AWS Lambda pour vous connecter à des bases de données RDS, vous modifiez leurs paramètres de connexion pour utiliser le point de terminaison proxy. Par exemple, vous indiquez au point de terminaison proxy de permettre aux fonctions de Lambda d'accéder à votre base de données tout en profitant des fonctionnalités de RDS Proxy.

Chaque proxy contient un groupe cible. Ce groupe cible incarne l'instance de base de données RDS ou le cluster de base de données Aurora auquel le proxy peut se connecter. Pour un cluster Aurora, le groupe cible est associé par défaut à toutes les instances de base de données de ce cluster. Le proxy peut ainsi se connecter à l'instance de base de données Aurora promue comme instance de rédacteur dans le cluster.

L'instance de base de données RDS associée à un proxy ou le cluster de base de données Aurora et ses instances sont appelés les cibles de ce proxy. Pour des raisons pratiques, lorsque vous créez un proxy via la console, RDS Proxy crée également le groupe cible correspondant et enregistre automatiquement les cibles associées.

Une famille de moteurs est un ensemble associé de moteurs de base de données qui utilisent le même protocole de base de données. Vous choisissez la famille de moteurs pour chaque proxy que vous créez.

Regroupement de connexions

Chaque proxy effectue le regroupement de connexions pour l'instance de rédacteur de sa base de données Aurora ou RDS associée. Le regroupement de connexions est une optimisation qui réduit la surcharge associée à l'ouverture et à la fermeture des connexions, tout en maintenant plusieurs connexions ouvertes simultanément. Cette surcharge inclut la mémoire nécessaire pour gérer chaque nouvelle connexion. Cette opération implique également une surcharge de l'UC pour fermer chaque connexion et en ouvrir une nouvelle : liaison Transport Layer Security/Secure Sockets Layer (TLS/SSL), authentification, négociation, etc. Le regroupement de connexions simplifie la logique de votre application. Vous n'avez pas besoin d'écrire de code d'application pour minimiser le nombre de connexions ouvertes simultanées.

Chaque proxy effectue également le multiplexage de connexion, également connu sous le nom de réutilisation de connexion. Grâce au multiplexage, RDS Proxy exécute toutes les opérations d'une transaction à l'aide d'une connexion de base de données sous-jacente, avant d'utiliser une connexion différente pour la transaction suivante. Si vous ouvrez de nombreuses connexions simultanées au proxy, celui-ci conserve un plus petit nombre de connexions ouvertes à l'instance ou au cluster de base de données. Cela permet de réduire davantage la surcharge de mémoire pour les connexions sur le serveur de base de données. Cette technique réduit également le risque que des erreurs liées au « nombre de connexions trop élevé » se produisent.

Sécurité RDS Proxy

RDS Proxy utilise les mécanismes de sécurité RDS existants tels que TLS/SSL et AWS Identity and Access Management (IAM). Pour obtenir des informations générales sur ces fonctionnalités de sécurité, reportez-vous à la section Sécurité dans Amazon RDS (p. 1518). Si vous n'êtes pas familier avec la façon dont RDS et Aurora utilisent l'authentification, l'autorisation et d'autres domaines de sécurité, commencez par découvrir la façon dont RDS et Aurora utilisent ces domaines.

RDS Proxy peut agir comme une couche de sécurité supplémentaire entre les applications clientes et la base de données sous-jacente. Vous pouvez par exemple vous connecter au proxy à l'aide de la version 1.2 de TLS, même si l'instance de base de données sous-jacente prend uniquement en charge les versions 1.0 ou 1.1 de TLS. Vous pouvez vous connecter au proxy à l'aide d'un rôle IAM, même si le proxy se connecte à la base de données à l'aide de la méthode native d'authentification par nom d'utilisateur et mot de passe. Grâce à cette technique, vous pouvez appliquer de fortes exigences d'authentification pour les applications de base de données sans avoir à fournir un effort de migration coûteux pour les instances de base de données elles-mêmes.

Vous stockez les informations d'identification de base de données utilisées par RDS Proxy dans AWS Secrets Manager. Chaque utilisateur de base de données pour l'instance de base de données RDS ou le cluster de base de données Aurora auquel un proxy accède doit avoir un secret correspondant dans Secrets Manager. Vous pouvez également configurer l'authentification IAM pour les utilisateurs de RDS Proxy. Vous pouvez ainsi appliquer l'authentification IAM pour l'accès à la base de données, même si les bases de données utilisent l'authentification native par mot de passe. Nous vous recommandons d'utiliser ces fonctions de sécurité au lieu d'intégrer les informations d'identification de base de données dans votre code d'application.

Utilisation de TLS/SSL avec RDS Proxy

Vous pouvez vous connecter à RDS Proxy à l'aide du protocole TLS/SSL.

> **Note**
>
> RDS Proxy utilise des certificats provenant de l'AWS Certificate Manager (ACM). Si vous utilisez RDS Proxy, lorsque vous effectuez la rotation de votre certificat TLS/SSL, vous n'avez pas besoin de mettre à jour les applications qui utilisent des connexions RDS Proxy.

Afin d'appliquer TLS pour toutes les connexions entre le proxy et votre base de données, vous pouvez spécifier un paramètre Exiger la sécurité de la couche de transport lorsque vous créez ou modifiez un proxy.

RDS Proxy permet également de garantir que votre session utilise TLS/SSL entre votre client et le point de terminaison RDS Proxy. Pour que RDS Proxy procède ainsi, spécifiez l'exigence côté client. Les variables de session SSL ne sont pas définies pour les connexions SSL à une base de données utilisant RDS Proxy.

- Pour Amazon RDS MySQL et Aurora MySQL, spécifiez l'exigence côté client avec le paramètre `--ssl-mode` lorsque vous exécutez la commande `mysql`.
- Pour Amazon RDS PostgreSQL et Aurora PostgreSQL, spécifiez `sslmode=require` comme partie de la chaîne `conninfo` lorsque vous exécutez la commande `psql`.

RDS Proxy prend en charge le protocole TLS versions 1.0, 1.1 et 1.2. Vous pouvez vous connecter au proxy à l'aide d'une version de TLS supérieure à celle utilisée dans la base de données sous-jacente.

Par défaut, les programmes client établissent une connexion chiffrée avec RDS Proxy. L'option `--ssl-mode` fournit davantage de contrôle. Du côté client, RDS Proxy prend en charge tous les modes SSL.

Pour le client, les modes SSL sont les suivants :

PREFERRED

SSL est le premier choix, mais n'est pas obligatoire.

DISABLED

Aucun mode SSL n'est autorisé.

REQUIRED

SSL est obligatoire.

VERIFY_CA

SSL est obligatoire et une vérification de l'autorité de certification (CA) est effectuée.

VERIFY_IDENTITY

SSL est obligatoire et une vérification de l'autorité de certification (CA) et de son nom d'hôte est effectuée.

Lorsque vous utilisez un client avec `--ssl-mode VERIFY_CA` ou `VERIFY_IDENTITY`, spécifiez l'option `--ssl-ca` pointant vers une autorité de certification au format .pem. Pour un fichier .pem que vous pouvez utiliser, téléchargez le référentiel d'approbations Amazon Root CA 1 à partir d'Amazon Trust Services.

RDS Proxy utilise des certificats à caractères génériques, qui s'appliquent à un domaine et à ses sous-domaines. Si vous utilisez le client `mysql` pour vous connecter avec le mode SSL `VERIFY_IDENTITY`, vous devez actuellement exécuter la commande `mysql` compatible avec MySQL 8.0.

Basculement

Le basculement est une fonction de haute disponibilité qui remplace une instance de base de données par une autre lorsque l'instance d'origine est indisponible. Un problème lié à une instance de base de données

peut entraîner un basculement. Celui-ci peut également faire partie de procédures de maintenance normales, lors d'une mise à niveau de la base de données par exemple. Cette opération s'applique aux instances de base de données RDS dans une configuration multi-AZ et aux clusters de base de données Aurora dotés d'une ou plusieurs instances de lecteur en plus de l'instance de rédacteur.

La connexion via un proxy rend votre application plus résistante aux basculements de base de données. Lorsque l'instance de base de données d'origine est indisponible, RDS Proxy se connecte à la base de données de secours sans supprimer les connexions d'application inactives. Cela permet d'accélérer et de simplifier le processus de basculement. Par conséquent, le basculement est plus rapide et interrompt moins longtemps votre application par rapport à un problème de redémarrage ou de base de données classique.

Sans RDS Proxy, un basculement provoque une brève interruption de service. Pendant la panne, vous ne pouvez pas effectuer d'opérations d'écriture sur cette base de données. Toutes les connexions de base de données existantes sont interrompues et votre application doit les rouvrir. La base de données est ouverte à de nouvelles connexions et opérations d'écriture lorsqu'une instance de base de données en lecture seule est promue pour remplacer celle qui n'est pas disponible.

Pendant les basculements de base de données, RDS Proxy continue d'accepter les connexions à la même adresse IP et redirige automatiquement les connexions vers la nouvelle instance de base de données principale. Les clients qui se connectent via RDS Proxy ne sont pas sujets aux éléments suivants :

- Délais de propagation du système de noms de domaine (DNS) lors du basculement.
- Mise en cache DNS locale.
- Délai d'expiration de connexion.
- Incertitude concernant l'instance de base de données qui est le rédacteur en cours.
- Attente d'une réponse à la requête d'un ancien rédacteur devenu indisponible sans fermer les connexions.

Pour les applications qui conservent leur propre regroupement de connexions, passer parRDS Proxy implique que la plupart des connexions restent actives pendant des basculements ou d'autres interruptions. Seules les connexions qui se trouvent au milieu d'une transaction ou d'une instruction SQL sont annulées. RDS Proxy accepte immédiatement les nouvelles connexions. Lorsque le rédacteur de base de données n'est pas disponible, RDS Proxy place les demandes entrantes dans la file d'attente.

Pour les applications qui ne conservent pas leurs propres regroupements de connexions, RDS Proxy offre des taux de connexion plus rapides et davantage de connexions ouvertes. Il permet de réduire la surcharge coûteuse des reconnexions fréquentes à la base de données. Il effectue cette opération en réutilisant les connexions de base de données maintenues dans le regroupement de connexions de RDS Proxy. Cette approche est particulièrement importante pour les connexions TLS, où les coûts d'installation sont importants.

Transactions

Toutes les instructions d'une seule transaction utilisent toujours la même connexion à la base de données sous-jacente. La connexion devient disponible pour une session différente lorsque la transaction se termine. Voici les conséquences de l'utilisation de la transaction en tant qu'unité de granularité :

- La réutilisation de la connexion peut se produire après chaque instruction individuelle lorsque le paramètre RDS MySQL ou Aurora MySQL `autocommit` est activé.
- Inversement, lorsque le paramètre `autocommit` est désactivé, la première instruction que vous émettez dans une session lance une nouvelle transaction. Par conséquent, si vous saisissez une séquence `SELECT`, `INSERT`, `UPDATE` ainsi que d'autres instructions en langage de manipulation de données (DML), la réutilisation de la connexion ne se produit que lorsque vous émettez `COMMIT`, `ROLLBACK` ou que vous mettez fin à la transaction.
- La saisie d'une instruction en langage de définition de données (DDL) entraîne la fin de la transaction une fois l'instruction terminée.

RDS Proxy détecte lorsqu'une transaction se termine par le protocole réseau utilisé par l'application cliente de base de données. La détection des transactions ne repose pas sur des mots-clés tels que `COMMIT` ou `ROLLBACK` apparaissant dans le texte de l'instruction SQL.

Dans certains cas, RDS Proxy peut détecter une demande de base de données qui rend impossible le déplacement de votre session vers une autre connexion. Dans ce cas, il désactive le multiplexage pour cette connexion pendant le reste de votre session. La même règle s'applique si RDS Proxy ne peut pas s'assurer de la praticité du multiplexage pour la session. Cette opération est appelée épinglage. Pour savoir comment détecter et réduire l'épinglage, consultez Contournement de l'épinglage (p. 194).

Planification et configuration de RDS Proxy

Vous découvrirez ci-après comment configurer RDS Proxy. Vous pouvez également trouver comment définir les options de sécurité associées qui contrôlent les accès à chaque proxy et la connexion de ces derniers aux instances de base de données.

Rubriques

- Limites de RDS Proxy (p. 175)
- Identification des instances de base de données, des clusters et des applications à utiliser avec RDS Proxy (p. 177)
- Configuration des prérequis réseau (p. 177)
- Configuration des informations d'identification de base de données dans AWS Secrets Manager (p. 178)
- Configuration de stratégies IAM AWS Identity and Access Management (p. 179)
- Création d'un RDS Proxy (p. 181)
- Affichage d'un RDS Proxy (p. 184)

Limites de RDS Proxy

Les limites suivantes s'appliquent à RDS Proxy :

- RDS Proxy est disponible seulement dans ces régions AWS :
  - Région USA Est (Virginie du N.)
  - Région USA Est (Ohio)
  - Région USA Ouest (Californie du Nord)
  - Région USA Ouest (Oregon)
  - Région Asie-Pacifique (Mumbai)
  - Région Asie-Pacifique (Séoul)
  - Région Asie-Pacifique (Singapour)
  - Région Asie-Pacifique (Sydney)
  - Région Asie-Pacifique (Tokyo)
  - Région Canada (Centre)
  - Région Europe (Francfort)
  - Région Europe (Irlande)
  - Région Europe (Londres)
- Vous pouvez avoir jusqu'à 20 proxy pour chaque ID de compte AWS. Si votre application nécessite plus de proxys, vous pouvez demander des proxys supplémentaires en ouvrant un ticket auprès de l'organisation AWS Support.
- Chaque proxy peut avoir jusqu'à 200 secrets Secrets Manager associés. Ainsi, chaque proxy peut se connecter avec 200 comptes d'utilisateur différents maximum à tout moment.

- Dans un cluster Aurora, toutes les connexions du regroupement de connexions sont gérées par l'instance de rédacteur Aurora. Pour effectuer l'équilibrage de charge pour les charges de travail intensives en lecture, vous utilisez toujours le point de terminaison du lecteur directement pour le cluster Aurora.

  La même considération s'applique aux instances de base de données RDS dans les configurations de réplication. Vous pouvez associer un proxy uniquement à l'instance de base de données de l'enregistreur, et non à un réplica en lecture.
- Vous ne pouvez pas utiliser RDS Proxy avec des clusters Aurora sans serveur.
- Vous ne pouvez pas utiliser RDS Proxy avec des clusters Aurora qui font partie d'une base de données Aurora globale.
- Votre RDS Proxy doit se trouver dans le même VPC que la base de données. Le proxy peut ne pas être accessible au public, contrairement à la base de données.
- Vous ne pouvez pas utiliser RDS Proxy avec un VPC qui a une location dédiée.
- Si vous utilisez RDS Proxy avec une instance de base de données RDS ou un cluster de base de données Aurora dont l'authentification IAM est activée, assurez-vous que tous les utilisateurs qui se connectent via un proxy s'authentifient par des noms d'utilisateur et des mots de passe. Veuillez consulter Configuration de stratégies IAM AWS Identity and Access Management (p. 179) pour de plus amples informations sur la prise en charge d'IAM dans RDS Proxy.
- Vous ne pouvez pas utiliser RDS Proxy avec DNS personnalisé.
- RDS Proxy est disponible pour les familles de moteurs MySQL et PostgreSQL.
- Chaque proxy peut être associé à une instance de base de données ou à un cluster cible unique. Toutefois, vous pouvez associer plusieurs proxys à la même instance ou au même cluster de base de données.

Les conditions préalables et limitations RDS Proxy suivantes s'appliquent à MySQL :

- Pour RDS MySQL, RDS Proxy prend en charge MySQL 5.6 et 5.7. Pour Aurora MySQL, RDS Proxy prend en charge la version 1 (compatible avec MySQL 5.6) et la version 2 (compatible avec MySQL 5.7).
- Actuellement, tous les proxy écoutent sur le port 3306 pour MySQL. Les proxys se connectent toujours à votre base de données à l'aide du port spécifié dans les paramètres de la base de données.
- Vous ne pouvez pas utiliser RDS Proxy avec RDS MySQL 8.0.
- Vous ne pouvez pas utiliser RDS Proxy avec des bases de données MySQL autogérées dans des instances EC2.
- Les proxy ne prennent pas en charge le mode compressé de MySQL. Par exemple, ils ne prennent pas en charge la compression utilisée par les options `-C` ou `--compress` de la commande `mysql`.
- Certaines instructions et fonctions SQL peuvent modifier l'état de connexion sans provoquer d'épinglage. Pour connaître le comportement d'épinglage le plus récent, consultez la section Contournement de l'épinglage (p. 194).

Les conditions préalables et limitations RDS Proxy suivantes s'appliquent à PostgreSQL :

- Pour RDS PostgreSQL, RDS Proxy prend en charge la version 10.10 et les versions mineures supérieures, et la version 11.5 et les versions mineures supérieures. Pour Aurora PostgreSQL, RDS Proxy prend en charge la version 10.11 et les versions mineures supérieures, et 11.6 et les versions mineures supérieures.
- Actuellement, tous les proxys écoutent sur le port 5432 pour PostgreSQL.
- L'annulation de requêtes n'est pas prise en charge pour PostgreSQL.
- Les résultats de la fonction PostgreSQL lastval() ne sont pas toujours précis. Pour contourner ce problème, utilisez l'instruction INSERT avec la clause `RETURNING`.

Identification des instances de base de données, des clusters et des applications à utiliser avec RDS Proxy

Vous pouvez déterminer les instances de base de données, clusters et applications qui pourraient bénéficier le plus de l'utilisation de RDS Proxy. Pour ce faire, tenez compte des facteurs suivants :

- RDS Proxy est hautement disponible et déployé sur plusieurs zones de disponibilité. Pour garantir une haute disponibilité globale de votre base de données, déployez votre instance de base de données Amazon RDS ou votre cluster Aurora dans une configuration multi-AZ.
- Il est judicieux d'associer à un proxy les instances ou clusters de base de données qui rencontrent des erreurs liées au « nombre de connexions trop élevé ». Le proxy permet aux applications d'ouvrir de nombreuses connexions client, tandis que le proxy gère un plus petit nombre de connexions à long terme à l'instance ou au cluster de base de données.
- Pour les instances de base de données ou les clusters qui utilisent des classes d'instance AWS plus petites (instances T2 ou T3, par exemple), l'utilisation d'un proxy peut contribuer à éviter les conditions de mémoire insuffisante. Il peut également contribuer à réduire la surcharge de l'UC lors de l'établissement des connexions. Ces conditions peuvent se produire lorsque vous faites face à un grand nombre de connexions.
- Vous pouvez surveiller certaines métriques Amazon CloudWatch pour déterminer si une instance de base de données ou un cluster approche certains types de limites. Ces limites concernent le nombre de connexions et la mémoire associées à la gestion des connexions. Vous pouvez également surveiller certaines métriques CloudWatch pour déterminer si une instance ou un cluster de base de données gère de nombreuses connexions de courte durée. L'ouverture et la fermeture de telles connexions peuvent entraîner une surcharge de performances sur votre base de données. Pour en savoir plus sur les métriques à surveiller, consultez Surveillance de RDS Proxy à l'aide d'Amazon CloudWatch (p. 196).
- Il peut également être judicieux d'utiliser les fonctions AWS Lambda avec un proxy. Ces fonctions réalisent fréquemment des connexions de base de données courtes qui bénéficient du regroupement de connexions offert par RDS Proxy. Vous pouvez profiter de toute authentification IAM dont vous disposez déjà pour les fonctions Lambda, plutôt que de gérer les informations d'identification de base de données dans votre code d'application Lambda.
- Les applications qui utilisent des langages et des cadres tels que PHP et Ruby on Rails fonctionnent généralement bien avec un proxy. Ces applications ouvrent et ferment habituellement un grand nombre de connexions à la base de données et ne disposent pas de mécanismes de regroupement de connexions intégrés.
- Il est souvent judicieux d'utiliser les applications qui maintiennent un grand nombre de connexions ouvertes pendant de longues périodes avec un proxy. Les applications dans des secteurs tels que le logiciel en tant que service (SaaS) ou le e-commerce réduisent souvent la latence pour les demandes de base de données en laissant les connexions ouvertes. Avec RDS Proxy, une application peut garder davantage de connexions ouvertes que lorsqu'elle se connecte directement à l'instance ou au cluster de base de données.
- Vous n'avez peut-être pas adopté l'authentification IAM et Secrets Manager en raison de sa complexité de configuration pour toutes les instances et clusters de base de données. Le cas échéant, vous pouvez garder les méthodes d'authentification existantes et déléguer l'authentification à un proxy. Le proxy peut appliquer les politiques d'authentification relatives aux connexions client pour des applications spécifiques. Vous pouvez profiter de toute authentification IAM dont vous disposez déjà pour les fonctions Lambda, plutôt que de gérer les informations d'identification de base de données dans votre code d'application Lambda.

Configuration des prérequis réseau

L'utilisation du RDS Proxy nécessite un ensemble de ressources de mise en réseau. Celles-ci incluent un VPC (Virtual Private Cloud), deux sous-réseaux ou plus, une instance Amazon EC2 au sein du même VPC et une passerelle Internet. Si vous êtes bien connecté à des instances de base de données RDS ou à des clusters de base de données Aurora, vous disposez déjà des ressources réseau requises.

Configuration des informations d'identification de base de données dans AWS Secrets Manager

Pour chaque proxy que vous créez, vous utilisez d'abord le service Secrets Manager pour stocker des ensembles d'informations de nom d'utilisateur et de mot de passe. Vous créez un Secrets Manager secret distinct pour chaque compte d'utilisateur de base de données auquel le proxy se connecte sur l'instance de base de données RDS ou le cluster de base de données Aurora.

Dans Secrets Manager, vous créez ces secrets avec des valeurs pour les champs `username` et `password`. Cela permet au proxy de se connecter aux utilisateurs de base de données correspondants sur les instances de base de données RDS ou clusters de base de données Aurora que vous associez au proxy. Vous pouvez le faire à l'aide des paramètres Informations d'identification pour une autre base de données, Informations d'identification pour la base de données RDS ou Autre type de secrets. Remplissez les valeurs appropriées pour les champs Nom d'utilisateur et Mot de passe, ainsi que les valeurs d'espace réservé pour tous les autres champs obligatoires. Le proxy ignore d'autres champs tels que Hôte et Port s'ils sont présents dans le secret. Ces détails sont automatiquement fournis par le proxy.

Vous pouvez également choisir Autre type de secrets. Dans ce cas, vous créez le secret avec des clés nommées `username` et `password`.

Les secrets utilisés par votre proxy n'étant pas liés à un serveur de base de données spécifique, vous pouvez réutiliser un secret sur différents serveurs proxy si vous utilisez les mêmes informations d'identification sur plusieurs serveurs de base de données. Par exemple, vous pouvez utiliser les mêmes informations d'identification sur un groupe de serveurs de développement et de test.

Pour vous connecter via le proxy en tant qu'utilisateur spécifique, assurez-vous que le mot de passe associé à un secret correspond au mot de passe de base de données de cet utilisateur. En cas d'incompatibilité, vous pouvez mettre à jour le secret associé dans Secrets Manager. Dans ce cas, vous pouvez toujours vous connecter à d'autres comptes où les informations d'identification secrètes et les mots de passe de base de données correspondent.

Lorsque vous créez un proxy via l'API AWS CLI ou RDS, vous indiquez les ARN (Amazon Resource Names) des secrets correspondants pour tous les comptes d'utilisateur de base de données auxquels le proxy peut accéder. Dans la AWS Management Console, vous choisissez les secrets selon leurs noms descriptifs.

Pour obtenir des instructions sur la création de secrets dans Secrets Manager, reportez-vous à la page Création d'un secret dans la documentation Secrets Manager. Utilisez l'une des techniques suivantes :
Pour obtenir des instructions sur la création de secrets dans Secrets Manager, veuillez consulter la section Création d'un secret dans Guide de l'utilisateur AWS Secrets Manager. Utilisez l'une des techniques suivantes :

- Utilisez Secrets Manager dans la console.
- Pour utiliser l'interface de ligne de commande lors de la création d'un secret Secrets Manager à utiliser avec RDS Proxy, utilisez une commande indiquée ci-après.

```
aws secretsmanager create-secret
--name "secret_name"
--description "secret_description"
--region region_name
--secret-string '{"username":"db_user","password":"db_user_password"}'
```

Par exemple, les commandes suivantes créent des secrets Secrets Manager pour deux utilisateurs de base de données, l'un nommé `admin` et l'autre `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"}'
```

Configuration de stratégies IAM AWS Identity and Access Management

Après avoir créé les secrets dans Secrets Manager, vous créez une stratégie IAM qui peut accéder à ces secrets. Pour obtenir des informations générales sur l'utilisation d'IAM avec RDS et Aurora, veuillez consulter Identity and Access Management dans Amazon RDS (p. 1536).

> **Tip**
>
> La procédure suivante s'applique si vous utilisez la console IAM. Si vous utilisez AWS Management Console pour RDS, RDS peut créer automatiquement la stratégie IAM pour vous. Dans ce cas, vous pouvez ignorer la procédure suivante.

Pour créer une stratégie IAM qui accède à vos secrets Secrets Manager pour une utilisation avec votre proxy

1. Connectez-vous à la console IAM. Suivez le processus Créer un rôle comme décrit dans la section Création de rôles IAM. Incluez l'étape Ajout d'un rôle à la base de données.
2. Pour le nouveau rôle, effectuez l'étape Ajout d'une stratégie en ligne. Utilisez les mêmes procédures générales que dans Modification des stratégies IAM. Collez le texte JSON suivant dans la zone de texte JSON. Indiquez votre propre ID de compte. Indiquez votre région AWS à la place de `us-east-2`. Remplacez les ARN (Amazon Resource Names) par les secrets que vous avez créés. Pour l'action `kms:Decrypt`, remplacez l'ARN de la clé principale client (CMK) AWS KMS par défaut ou de votre propre CMK AWS KMS, selon celui que vous avez utilisé pour chiffrer les secrets Secrets Manager.

```
{
    "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. Modifiez la stratégie d'approbation pour cette stratégie IAM. Collez le texte JSON suivant dans la zone de texte JSON.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "rds.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Les commandes suivantes exécutent la même opération via le 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":"*"
      }
    ]
}
"""
```

Création d'un RDS Proxy

Vous pouvez créer un proxy afin de gérer les connexions pour un ensemble d'instances de base de données précis. Vous pouvez associer un proxy à une instance de base de données MySQL RDS, une instance de base de données PostgreSQL ou un cluster de bases de données Aurora.

AWS Management Console

Pour créer un proxy

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, sélectionnez Proxies.
3. Choisissez Création d'un proxy.
4. Définissez tous les paramètres de votre proxy.

   Pour Configuration du proxy, fournissez des informations pour les éléments suivants :

   - Identifiant du proxy. Indiquez un nom unique de votre choix au sein de votre ID de compte AWS et de votre région AWS actuelle.
   - Compatibilité moteur. Choisissez MySQL ou POSTGRESQL.
   - Imposer le protocole Transport Layer Security. Choisissez ce paramètre si vous souhaitez que le proxy applique le protocole TLS/SSL pour toutes les connexions client. Lorsque vous vous connectez à un proxy à l'aide d'une connexion chiffrée ou non chiffrée, celui-ci utilise le même paramètre de chiffrement lorsqu'il établit une connexion à la base de données sous-jacente.
   - Délai d'inactivité de la connexion client. Choisissez une période pendant laquelle une connexion client peut être inactive avant que le proxy puisse la fermer. La valeur par défaut est de 1 800 secondes (30 minutes). Une connexion client est considérée comme inactive lorsque l'application ne soumet aucune nouvelle demande dans le délai défini après l'achèvement de la demande précédente. La connexion à la base de données sous-jacente reste ouverte et est renvoyée au regroupement de connexions. Ainsi, elle peut être réutilisée pour de nouvelles connexions client.

     Pensez à réduire le délai d'expiration de la connexion client inactive si vous souhaitez que le proxy supprime proactivement les connexions obsolètes. Si votre charge de travail augmente, pensez à augmenter le délai d'expiration de la connexion client inactive pour économiser le coût d'établissement de connexions.

   Pour la Configuration du groupe cible, fournissez des informations pour les éléments suivants :

   - Base de données. Choisissez une instance de base de données RDS ou un cluster de base de données Aurora pour accéder via ce proxy. La liste inclut uniquement les instances et les clusters

de base de données dotés de moteurs de base de données, de versions de moteur et d'autres paramètres compatibles. Si la liste est vide, créez une instance ou un cluster de base de données compatible avec RDS Proxy. Pour ce faire, suivez la procédure décrite dans Création d'une instance de base de données Amazon RDS (p. 146) . Puis, réessayez de créer le proxy.

- Connexions maximales au regroupement de connexions. Spécifiez une valeur comprise entre 1 et 100. Ce paramètre représente le pourcentage de la valeur `max_connections` que le RDS Proxy peut utiliser pour ses connexions. Si vous ne prévoyez d'utiliser qu'un seul proxy avec cette instance ou ce cluster de base de données, vous pouvez définir cette valeur sur 100. Pour plus d'informations sur la manière dont RDS Proxy utilise ce paramètre, consultez la section Contrôle des limites et des délais d'expiration des connexions (p. 192).
- Filtres d'épinglage de session. (Facultatif) Il s'agit d'un paramètre avancé permettant de résoudre les problèmes de performances liés à des applications spécifiques. Actuellement, `EXCLUDE_VARIABLE_SETS` est le seul choix possible. Choisissez un filtre uniquement si les deux conditions suivantes sont remplies : votre application ne réutilise pas les connexions en raison de certains types d'instructions SQL et vous pouvez vérifier que la réutilisation des connexions avec ces instructions SQL n'affecte pas le bon fonctionnement de l'application. Pour de plus amples informations, consultez Contournement de l'épinglage (p. 194).
- Délai d'expiration de l'emprunt de connexion. Dans certains cas, le proxy est susceptible d'utiliser occasionnellement toutes les connexions de base de données disponibles. Vous pouvez alors définir combien de temps le proxy doit attendre la disponibilité d'une connexion de base de données avant de renvoyer une erreur de dépassement de délai d'attente. Vous pouvez spécifier une période maximale de cinq minutes. Ce paramètre s'applique uniquement lorsque le proxy a atteint le nombre maximal de connexions ouvertes et que toutes les connexions sont déjà utilisées.

Pour Connectivité, fournissez des informations sur les éléments suivants :

- ARN Secrets Manager. Choisissez au moins un secret Secrets Manager qui contient les informations d'identification de l'utilisateur de la base de données pour l'instance de base de données RDS ou le cluster de base de données Aurora auquel vous avez l'intention d'accéder avec ce proxy.
- Rôle IAM. Choisissez un rôle IAM qui a l'autorisation d'accéder aux secrets Secrets Manager que vous avez choisis précédemment. Vous pouvez également laisser la AWS Management Console créer un nouveau rôle IAM pour vous et l'utiliser.
- Authentification IAM. Choisissez si vous souhaitez exiger ou interdire l'authentification IAM pour les connexions à votre proxy. Le choix de l'authentification IAM ou de l'authentification de base de données native s'applique à tous les utilisateurs de base de données qui accèdent à ce proxy.
- Sous-réseaux. Ce champ est pré-rempli avec tous les sous-réseaux associés à votre VPC. Vous pouvez supprimer tous les sous-réseaux dont vous n'avez pas besoin pour ce proxy. Vous devez garder au moins deux sous-réseaux.

Fournissez la configuration de connectivité supplémentaire :

- Groupe de sécurité VPC. Choisissez un groupe de sécurité VPC existant. Vous pouvez également laisser la AWS Management Console créer un nouveau groupe de sécurité pour vous et l'utiliser.

  Note

  Ce groupe de sécurité doit autoriser l'accès à la base de données à laquelle le proxy se connecte. Le même groupe de sécurité est utilisé pour l'entrée de vos applications vers le proxy, et pour la sortie du proxy vers la base de données. Par exemple, supposons que vous utilisiez le même groupe de sécurité pour votre base de données et votre proxy. Dans ce cas, assurez-vous de spécifier que les ressources de ce groupe de sécurité peuvent communiquer avec d'autres ressources du même groupe de sécurité.

(Facultatif) Fournissez une configuration avancée :

- Activation de la journalisation améliorée. Vous pouvez activer ce paramètre pour résoudre les problèmes liés à la compatibilité des proxy ou aux performances.

  Lorsque ce paramètre est activé, RDS Proxy inclut des informations détaillées sur les instructions SQL dans ses journaux. Ces informations vous aident à déboguer les problèmes relatifs au comportement SQL ou aux performances et l'évolutivité des connexions proxy. Les informations de débogage incluent le texte des instructions SQL que vous soumettez via le proxy. Par conséquent, n'activez ce paramètre que s'il est nécessaire au débogage, et seulement lorsque vous disposez de mesures de sécurité pour protéger les informations sensibles qui apparaissent dans les journaux.

  Pour réduire les frais généraux associés à votre proxy, RDS Proxy désactive automatiquement ce paramètre 24 heures après l'avoir activé. Activez-le temporairement pour résoudre un problème spécifique.

5. Choisissez Création d'un proxy.

AWS CLI

Pour créer un proxy, utilisez la commande AWS CLI create-db-proxy. La valeur `--engine-family` est sensible à la casse.

Example

Pour Linux, macOS ou Unix :

```
aws rds create-db-proxy \
    --db-proxy-name proxy_name \
    --role-arn iam_role \
    --engine-family { MYSQL | POSTGRESQL } \
    --vpc-subnet-ids space_separated_list \
    [--vpc-security-group-ids space_separated_list] \
    [--auth ProxyAuthenticationConfig_JSON_string] \
    [--require-tls | --no-require-tls] \
    [--idle-client-timeout value] \
    [--debug-logging | --no-debug-logging] \
    [--tags comma_separated_list]
```

Pour Windows :

```
aws rds create-db-proxy ^
    --db-proxy-name proxy_name ^
    --role-arn iam_role ^
    --engine-family { MYSQL | POSTGRESQL } ^
    --vpc-subnet-ids space_separated_list ^
    [--vpc-security-group-ids space_separated_list] ^
    [--auth ProxyAuthenticationConfig_JSON_string] ^
    [--require-tls | --no-require-tls] ^
    [--idle-client-timeout value] ^
    [--debug-logging | --no-debug-logging] ^
    [--tags comma_separated_list]
```

Pour créer les informations et les associations requises pour le proxy, vous utilisez également la commande register-db-proxy-targets. Spécifiez le nom du groupe cible `default`. RDS Proxy crée automatiquement un groupe cible portant ce nom lorsque vous créez chaque 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)
```

API RDS

Pour créer un proxy RDS, appelez l'opération d'API Amazon RDS CreateDBProxy. Vous transmettez un paramètre avec la structure de données AuthConfig.

RDS Proxy crée automatiquement un groupe cible nommé `default` lorsque vous créez chaque proxy. Vous associez une instance de base de données RDS ou un cluster de base de données Aurora au groupe cible en appelant la fonction RegisterDBProxyTargets.

Affichage d'un RDS Proxy

Après avoir créé un ou plusieurs proxy RDS, vous pouvez les afficher pour examiner les détails de leur configuration et choisir ceux que vous souhaitez modifier, supprimer, etc.

Toutes les applications de base de données qui utilisent le proxy nécessitent que le point de terminaison du proxy soit utilisé dans la chaîne de connexion.

AWS Management Console

Pour afficher votre proxy

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le coin supérieur droit de la AWS Management Console, sélectionnez la région AWS dans laquelle vous avez créé le RDS Proxy.
3. Dans le panneau de navigation, sélectionnez Proxies.
4. Indiquez le nom d'un proxy RDS pour afficher ses détails.
5. Sur la page de détails, la section Groupes cibles montre comment le proxy est associé à une instance de base de données RDS ou un cluster de base de données Aurora spécifique. Vous pouvez suivre le lien vers la page du groupe cible par défaut pour voir plus de détails sur l'association entre le proxy et la base de données. Cette page affiche les paramètres que vous avez spécifiés lors de la création du proxy, tels que le pourcentage maximal de connexion, le délai d'attente d'emprunt de connexion, la compatibilité du moteur et les filtres d'épinglage de session.

Interface de ligne de commande

Pour afficher votre proxy à l'aide de l'interface de ligne de commande, utilisez la commande describe-db-proxies. Par défaut, il affiche tous les proxy appartenant à votre compte AWS. Pour afficher les détails d'un proxy, spécifiez son nom avec le paramètre `--db-proxy-name`.

```
aws rds describe-db-proxies [--db-proxy-name proxy_name]
```

Pour afficher les autres informations associées au proxy, utilisez les commandes suivantes.

```
aws rds describe-db-proxy-target-groups  --db-proxy-name proxy_name

aws rds describe-db-proxy-targets --db-proxy-name proxy_name
```

Utilisez la séquence de commandes suivante pour afficher plus de détails sur les éléments associés au proxy :

1. Pour obtenir une liste des proxys, exécutez describe-db-proxies.
2. Pour afficher les paramètres de connexion tels que le pourcentage maximal de connexions que le proxy peut utiliser, exécutez describe-db-proxy-target-groups `--db-proxy-name` et utilisez le nom du proxy comme valeur de paramètre.
3. Pour afficher les détails de l'instance de base de données RDS ou du cluster de bases de données Aurora associé au groupe cible renvoyé, exécutez describe-db-proxy-targets.

API RDS

Pour afficher vos proxy à l'aide de l'API RDS, utilisez l'opération DescribeDBProxies. Elle renvoie les valeurs du type de données DBProxy.

Pour afficher les détails des paramètres de connexion du proxy, utilisez les identifiants de proxy à partir de la valeur renvoyée à l'aide de l'opération DescribeDBProxyTargetGroups. Elle renvoie les valeurs du type de données DBProxyTargetGroup.

Pour voir l'instance RDS ou le cluster de base de données Aurora associé au proxy, utilisez l'opération DescribeDBProxyTargets. Elle renvoie les valeurs du type de données DBProxyTarget.

Connexion à une base de données via RDS Proxy

La connexion à une instance de base de données RDS ou à un cluster de base de données Aurora via un proxy est identique à une connexion directe à la base de données. La principale différence est que vous indiquez le point de terminaison du proxy et non celui de l'instance ou du cluster. Pour un cluster de base de données Aurora, toutes les connexions de proxy ont une capacité de lecture-écriture et utilisent l'instance de rédacteur. Si vous utilisez le point de terminaison du lecteur pour les connexions en lecture seule, vous faites la même utilisation du point de terminaison du lecteur.

Rubriques

- Connexion à un proxy à l'aide de l'authentification native (p. 185)
- Connexion à un proxy à l'aide de l'authentification IAM (p. 186)
- Considérations relatives à la connexion à un proxy avec PostgreSQL (p. 187)

Connexion à un proxy à l'aide de l'authentification native

Utilisez les étapes de base suivantes pour vous connecter à un proxy à l'aide de l'authentification native :

1. Recherchez le point de terminaison du proxy. Dans la AWS Management Console, vous pouvez trouver le point de terminaison sur la page de détails du proxy correspondant. Avec l'AWS CLI, vous pouvez utiliser la commande describe-db-proxies. L'exemple suivant indique comment procéder.

```
# 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. Spécifier ce point de terminaison comme paramètre hôte dans la chaîne de connexion de votre application cliente. Par exemple, spécifiez le point de terminaison du proxy comme valeur pour l'option `mysql -h` ou `psql -h`.
3. Fournissez le nom d'utilisateur et le mot de passe de base de données que vous utilisez habituellement.

Connexion à un proxy à l'aide de l'authentification IAM

Lorsque vous utilisez l'authentification IAM avec RDS Proxy, configurez les utilisateurs de votre base de données de sorte qu'ils s'authentifient avec des noms d'utilisateur et des mots de passe normaux. L'authentification IAM s'applique à la récupération RDS Proxy des informations d'identification (nom d'utilisateur et mot de passe) depuis Secrets Manager. La connexion depuis RDS Proxy à la base de données sous-jacente ne passe pas par IAM.

Pour vous connecter à RDS Proxy l'aide de l'authentification IAM, suivez la même procédure générale que pour vous connecter à une instance de base de données RDS ou à un cluster Aurora à l'aide de l'authentification IAM. Pour obtenir des informations générales sur l'utilisation d'IAM avec RDS et Aurora, veuillez consulter Sécurité dans Amazon RDS (p. 1518).

Les principales différences dans l'utilisation d'IAM pour RDS Proxy sont les suivantes :

- Vous ne configurez pas chaque utilisateur de base de données avec un plug-in d'autorisation. Les utilisateurs de base de données ont toujours des noms d'utilisateur et des mots de passe réguliers dans la base de données. Vous configurez des secrets Secrets Manager contenant ces noms et mots de passe d'utilisateur, et autorisez RDS Proxy à récupérer les informations d'identification à partir d'Secrets Manager.

  > **Important**
  >
  > L'authentification IAM s'applique à la connexion entre votre programme client et le proxy. Le proxy s'authentifie ensuite à la base de données à l'aide des informations d'identification (nom d'utilisateur et mot de passe) extraites via Secrets Manager. Lorsque vous utilisez IAM pour la connexion à un proxy, assurez-vous que l'instance de base de données RDS ou le cluster de base de données Aurora sous-jacent n'est pas activé.
- Spécifiez le point de terminaison du proxy plutôt que celui de l'instance, du cluster ou du lecteur. Pour de plus amples informations sur le point de terminaison du proxy, veuillez consulter Connexion à votre instance de base de données à l'aide de l'authentification IAM. (p. 1562).
- Dans le cas d'une authentification IAM de base de données directe, vous choisissez de manière sélective les utilisateurs de base de données et vous les configurez de sorte qu'ils soient identifiés avec un plug-in d'authentification spécial. Vous pouvez ensuite vous connecter à ces utilisateurs à l'aide de l'authentification IAM.

  Dans le cas d'utilisation du proxy, vous devez fournir au proxy des secrets qui contiennent le nom d'utilisateur et le mot de passe de certains utilisateurs (authentification native). Vous vous connectez ensuite au proxy en utilisant l'authentification IAM (en générant un jeton d'authentification avec le point de terminaison du proxy, et non le point de terminaison de la base de données) et en utilisant un nom d'utilisateur correspondant à l'un des noms d'utilisateur pour les secrets que vous avez précédemment fournis.
- Veuillez vous assurer d'utiliser TLS (Transport Layer Security) / SSL (Secure Sockets Layer) lors de la connexion à un proxy avec l'authentification IAM.

Vous pouvez accorder l'accès au proxy à un utilisateur spécifique en modifiant la stratégie IAM. Un exemple suit.

```
"Resource": "arn:aws:rds-db:us-east-2:1234567890:dbuser:prx-ABCDEFGHIJKL01234/db_user"
```

Considérations relatives à la connexion à un proxy avec PostgreSQL

Pour PostgreSQL, lorsqu'un client démarre une connexion à une base de données PostgreSQL, il envoie un message de démarrage qui inclut des paires de chaînes de nom de paramètre et de valeur. Pour plus de détails, veuillez consulter `StartupMessage` dans la section relative aux formats de message PostgreSQL de la documentation PostgreSQL.

Lors de la connexion via un proxy RDS, le message de démarrage peut inclure les paramètres actuellement reconnus suivants :

- `user`
- `database`
- `replication`

Le message de démarrage peut également inclure les paramètres d'exécution supplémentaires suivants :

- `application_name`
- `client_encoding`
- `DateStyle`
- `TimeZone`
- `extra_float_digits`

Pour de plus amples informations sur la messagerie PostgreSQL, consultez la section relative au protocole frontend/backend de la documentation PostgreSQL.

Pour PostgreSQL, si vous utilisez JDBC, nous vous recommandons ce qui suit pour éviter l'épinglage :

- Définissez le paramètre de connexion JDBC `assumeMinServerVersion` sur `9.0` au minimum afin d'éviter l'épinglage. Cela empêche le pilote JDBC d'effectuer un aller-retour supplémentaire au démarrage de la connexion lorsqu'il exécute `SET extra_float_digits = 3`.
- Définissez le paramètre de connexion JDBC `ApplicationName` sur *`any/your-application-name`* afin d'éviter l'épinglage. Cela empêche le pilote JDBC d'effectuer un aller-retour supplémentaire au démarrage de la connexion lorsqu'il exécute `SET application_name = "PostgreSQL JDBC Driver"`. Notez que le paramètre JDBC est `ApplicationName`, mais que le paramètre PostgreSQL `StartupMessage` est `application_name`.
- Définissez le paramètre de connexion JDBC `preferQueryMode` sur `extendedForPrepared` afin d'éviter l'épinglage. `extendedForPrepared` garantit que le mode étendu est utilisé uniquement pour les instructions préparées.

  La valeur par défaut pour le paramètre `preferQueryMode` est `extended`, qui utilise le mode étendu pour toutes les requêtes. Le mode étendu utilise une série de demandes `Prepare`, `Bind`, `Execute` et `Sync`, ainsi que les réponses correspondantes. Ce type de série provoque l'épinglage de connexion dans un proxy RDS.

Pour plus d'informations, consultez Contournement de l'épinglage (p. 194). Pour de plus amples informations sur la connexion à l'aide de JDBC, veuillez consulter la section relative à la connexion à la base de données dans la documentation PostgreSQL.

Gestion d'un RDS Proxy

Vous trouverez ci-dessous une explication sur la façon de gérer le fonctionnement et la configuration d'un proxy RDS. Ces procédures aident votre application à utiliser de manière optimale les connexions de base de données et à obtenir une réutilisation maximale des connexions. Plus vous tirez profit de la réutilisation des connexions, plus vous évitez une surcharge de l'UC et de la mémoire. Cela réduit la latence de votre application et permet à la base de données de dédier une plus grande partie de ses ressources au traitement des requêtes d'application.

Rubriques

- Modification d'un RDS Proxy (p. 188)
- Ajout d'un nouvel utilisateur de base de données (p. 192)
- Modification du mot de passe d'un utilisateur de base de données (p. 192)
- Contrôle des limites et des délais d'expiration des connexions (p. 192)
- Gestion et surveillance du regroupement de connexions (p. 193)
- Contournement de l'épinglage (p. 194)
- Suppression d'un RDS Proxy (p. 196)

Modification d'un RDS Proxy

Vous pouvez modifier certains paramètres associés à un proxy après avoir sa création. Pour ce faire, modifiez le proxy lui-même, son groupe cible associé, ou les deux. Chaque proxy dispose d'un groupe cible associé.

AWS Management Console

Modifications des paramètres d'un proxy

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, sélectionnez Proxies.
3. Dans la liste de proxy, choisissez celui dont vous souhaitez modifier les paramètres ou accédez à sa page de détails.
4. Pour Actions, choisissez Modify (Modifier).
5. Saisissez ou sélectionnez les propriétés à modifier. Vous pouvez effectuer les actions suivantes :
   - Renommer le proxy en saisissant un nouvel identifiant.
   - Imposer ou non le protocole Transport Layer Security (TLS).
   - Définir un délai d'inactivité de la connexion.
   - Ajouter ou supprimer des secrets Secrets Manager. Ces secrets correspondent aux noms d'utilisateur et mots de passe de la base de données.
   - Modifier le rôle IAM utilisé pour récupérer les secrets de Secrets Manager.
   - Exiger ou interdire l'authentification IAM pour les connexions au proxy.
   - Ajouter ou supprimer des sous-réseaux VPC que le proxy doit utiliser.
   - Ajouter ou supprimer des groupes de sécurité VPC que le proxy doit utiliser.
   - Activer ou désactiver la journalisation améliorée.
6. Sélectionnez Modify.

Si vous n'avez pas trouvé les paramètres répertoriés que vous souhaitez modifier, procédez comme suit pour mettre à jour le groupe cible du proxy. Le groupe cible associé à un proxy contrôle les paramètres liés

aux connexions à la base de données physique. Chaque proxy dispose d'un groupe cible associé, nommé `default`, qui est créé automatiquement avec le proxy.

Vous pouvez uniquement modifier le groupe cible à partir de la page de détails du proxy, et non depuis la liste de la page Proxies.

Modification des paramètres d'un groupe cible proxy

1. Sur la page Proxys, accédez à la page des détails d'un proxy.
2. Pour les Groupes cibles, choisissez le lien `default`. Actuellement, tous les proxy ont un groupe cible unique nommé `default`.
3. Sur la page de détails du groupe cible par défaut, sélectionnez Modifier.
4. Définissez de nouveaux paramètres pour les propriétés que vous pouvez modifier :

   - Choisissez une instance de base de données RDS ou un cluster Aurora différent.
   - Ajustez le pourcentage du nombre de connexions maximum disponibles que le proxy peut utiliser.
   - Choisissez un filtre d'épinglage de session. Cela peut contribuer à réduire les problèmes de performances liés à une réutilisation insuffisante au niveau de la transaction pour les connexions. L'utilisation de ce paramètre exige une compréhension du comportement de l'application et des circonstances dans lesquelles RDS Proxy épingle une session à une connexion à une base de données.
   - Ajustez l'intervalle du délai d'attente d'emprunt de connexion. Ce paramètre s'applique lorsque le nombre maximal de connexions est déjà utilisé pour le proxy. Ce paramètre permet de définir combien de temps le proxy doit attendre la disponibilité d'une connexion avant de renvoyer une erreur de dépassement de délai d'attente.

   Certaines propriétés, telles que l'identifiant du groupe cible et le moteur de base de données, sont corrigées.
5. Sélectionnez Modification du groupe cible.

AWS CLI

Pour modifier un proxy à l'aide de l'AWS CLI, utilisez les commandes modify-db-proxy, modify-db-proxy-target-group, deregister-db-proxy-targets et register-db-proxy-targets.

Avec la commande `modify-db-proxy`, vous pouvez modifier des propriétés, par exemple :

- Ensemble des secrets Secrets Manager utilisés par le proxy.
- TLS requis ou non.
- Délai d'expiration de la connexion client inactive.
- Nécessité ou non de consigner des informations supplémentaires des instructions SQL pour le débogage.
- Rôle IAM utilisé pour récupérer les secrets Secrets Manager.
- Groupes de sécurité utilisés par le proxy.

L'exemple suivant montre comment renommer un proxy existant.

```
aws rds modify-db-proxy --db-proxy-name the-proxy --new-db-proxy-name the_new_name
```

Pour modifier les paramètres liés à la connexion ou renommer le groupe cible, utilisez la commande `modify-db-proxy-target-group`. Actuellement, tous les proxy ont un groupe cible unique nommé `default`. Lorsque vous travaillez avec ce groupe cible, vous indiquez le nom du proxy et `default` pour le nom du groupe cible.

L'exemple suivant montre comment vérifier le paramètre `MaxConnectionsPercent` d'un proxy avant de le modifier à l'aide du groupe cible.

```
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
    }
}
```

Grâce aux commandes `register-db-proxy-targets` et `deregister-db-proxy-targets`, vous modifiez l'instance de base de données RDS ou le cluster de base de donnéesAurora auquel le proxy est associé via son groupe cible. Actuellement, chaque proxy peut se connecter à une instance de base de données RDS ou à un cluster de base de données Aurora. Le groupe cible suit les détails de connexion de toutes les instances de base de données RDS dans une configuration multi-AZ ou de toutes les instances de base de données dans un cluster Aurora.

L'exemple suivant commence par un proxy associé à un cluster Aurora MySQL nommé `cluster-56-2020-02-25-1399`. L'exemple vous explique comment modifier le proxy afin qu'il puisse se connecter à un autre cluster nommé `provisioned-cluster`.

Lorsque vous travaillez avec une instance de base de données RDS, sélectionnez l'option `--db-instance-identifier`. Lorsque vous travaillez avec un cluster de base de données Aurora DB, préférez l'option `--db-cluster-identifier`.

L'exemple suivant modifie un proxy Aurora MySQL. Un proxy PostgreSQL Aurora dispose du 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"
        }
```

```
    ]
}
```

API RDS

Pour modifier un proxy à l'aide de l'API RDS, utilisez les opérations ModifyDBProxy, ModifyDBProxyTargetGroup, DeregisterDBProxyTargets, et RegisterDBProxyTargets.

Avec `ModifyDBProxy`, vous pouvez modifier des propriétés, par exemple :

- Ensemble des secrets Secrets Manager utilisés par le proxy.
- TLS requis ou non.
- Délai d'expiration de la connexion client inactive.
- Nécessité ou non de consigner des informations supplémentaires des instructions SQL pour le débogage.
- Rôle IAM utilisé pour récupérer les secrets Secrets Manager.
- Groupes de sécurité utilisés par le proxy.

Avec `ModifyDBProxyTargetGroup`, vous pouvez modifier les paramètres liés à la connexion ou renommer le groupe cible. Actuellement, tous les proxy ont un groupe cible unique nommé `default`. Lorsque vous travaillez avec ce groupe cible, vous indiquez le nom du proxy et `default` pour le nom du groupe cible.

Avec `DeregisterDBProxyTargets` et `RegisterDBProxyTargets`, vous pouvez modifier l'instance de base de données RDS ou le cluster de base de données Aurora auquel le proxy est associé via son groupe cible. Actuellement, chaque proxy peut se connecter à une instance de base de données RDS ou à un cluster de base de données Aurora. Le groupe cible suit les détails de connexion de toutes les instances de base de données RDS dans une configuration multi-AZ ou de toutes les instances de base de données dans un cluster Aurora.

Ajout d'un nouvel utilisateur de base de données

Dans certains cas, vous pouvez ajouter un nouvel utilisateur de base de données à une instance de base de données RDS ou un cluster Aurora associé à un proxy. Le cas échéant, ajoutez ou réaffectez un secret Secrets Manager pour stocker les informations d'identification de cet utilisateur. Pour ce faire, choisissez l'une des options suivantes :

- Créez un nouveau secret Secrets Manager en suivant les instructions décrites dans la section Configuration des informations d'identification de base de données dans AWS Secrets Manager (p. 178).
- Mettez à jour le rôle IAMpour permettre à RDS Proxy d'accéder au nouveau secret Secrets Manager. Pour ce faire, mettez à jour la section des ressources de la stratégie de rôle IAM.
- Si le nouvel utilisateur remplace un utilisateur existant, mettez à jour les informations d'identification stockées dans le secret Secrets Manager du proxy pour l'utilisateur existant.

Modification du mot de passe d'un utilisateur de base de données

Dans certains cas, vous pouvez modifier le mot de passe d'un utilisateur de base de données dans une instance de base de données RDS ou un cluster Aurora associé à un proxy. Le cas échéant, mettez à jour le secret Secrets Manager correspondant avec le nouveau mot de passe.

Contrôle des limites et des délais d'expiration des connexions

RDS Proxy utilise le paramètre `max_connections` pour votre instance de base de données RDS ou votre cluster de base de données Aurora. Ce paramètre représente la limite supérieure globale des connexions

que le proxy peut ouvrir à tout moment. Dans les clusters Aurora et les configurations multi-AZ RDS, la valeur `max_connections` utilisée par le proxy est celle de l'instance principale Aurora ou de l'instance d'enregistreur RDS.

Pour définir cette valeur pour votre instance de base de données RDS ou votre cluster de base de données Aurora, suivez les procédures de Utilisation de groupes de paramètres de base de données (p. 225). Ces procédures expliquent comment associer un groupe de paramètres à votre base de données et modifier la valeur `max_connections` du groupe de paramètres.

Le paramètre de proxy pour les connexions maximales représente un pourcentage de la valeur `max_connections` pour la base de données associée au proxy. Si plusieurs applications utilisent la même base de données, vous pouvez diviser leurs quotas de connexion de manière efficace à l'aide d'un proxy pour chaque application avec un pourcentage spécifique de `max_connections`. Si vous effectuez cette opération, vérifiez que les pourcentages totalisent une valeur inférieure ou égale à 100 pour tous les proxys associés à la même base de données.

RDS Proxy déconnecte régulièrement les connexions inactives et les renvoie au regroupement de connexions. Vous pouvez ajuster cet intervalle d'expiration. Cela permet à vos applications de gérer les ressources obsolètes, en particulier si l'application laisse par erreur une connexion ouverte tout en conservant des ressources de base de données importantes.

Gestion et surveillance du regroupement de connexions

Comme décrit dans la section Regroupement de connexions (p. 172), le regroupement de connexions est une caractéristique clé de RDS Proxy. Vous pouvez ensuite apprendre à optimiser l'utilisation du regroupement de connexions et la réutilisation des connexions au niveau de la transaction (multiplexage).

Le regroupement de connexions étant géré par RDS Proxy, vous pouvez le surveiller et ajuster les limites et intervalles d'expiration de connexions sans modifier votre code d'application.

Pour chaque proxy, vous pouvez définir une limite supérieure sur le nombre de connexions utilisées par le regroupement de connexions. Vous indiquez la limite sous forme de pourcentage. Ce pourcentage s'applique au nombre maximal de configurées dans la base de données. Le nombre exact varie en fonction de la taille de l'instance de base de données et des paramètres de configuration.

Supposons, par exemple, que vous ayez configuré RDS Proxy pour qu'il utilise 75 % du nombre maximal de connexions de la base de données. Pour MySQL, la valeur maximale est définie par le paramètre de configuration `max_connections`. Dans ce cas, les 25 % restants du nombre maximal de connexions resteraient disponibles pour d'autres proxy ou pour les connexions qui ne passent pas par un proxy. Dans certains cas, le proxy peut conserver moins de 75 % du nombre maximal de connexions ouvertes à un moment donné. C'est notamment le cas lorsque la base de données ne dispose pas d'un grand nombre de connexions simultanées ou que certaines connexions restent inactives pendant de longues périodes.

Le nombre total de connexions disponibles pour le regroupement de connexions change lorsque vous mettez à jour le paramètre de configuration `max_connections` qui s'applique à une instance de base de données RDS ou à un cluster Aurora.

Le proxy ne réserve pas toutes ces connexions à l'avance. Ainsi, vous pouvez définir un pourcentage relativement élevé. Ces connexions ne sont ouvertes que lorsque le proxy en a besoin en raison de son taux d'occupation.

Vous pouvez établir la durée d'attente d'une connexion pour qu'elle soit disponible en vue d'une utilisation dans votre application. Ce paramètre est représenté par l'option Délai d'expiration d'emprunt de connexion lorsque vous créez un proxy. Il indique le temps d'attente pour qu'une connexion devienne disponible dans le regroupement de connexions avant de renvoyer une erreur de délai d'expiration. Il s'applique lorsque le nombre maximal de connexions est atteint et qu'aucune connexion n'est disponible dans le regroupement de connexions. Il s'applique également si aucune instance de rédacteur n'est disponible en raison d'une opération de basculement en cours. À l'aide de ce paramètre, vous pouvez définir la meilleure période d'attente pour votre application sans avoir à modifier le délai d'attente de requête dans votre code d'application.

Contournement de l'épinglage

Le multiplexage est plus efficace lorsque les demandes de base de données ne dépendent pas des informations d'état issues de demandes précédentes. Dans ce cas, RDS Proxy peut réutiliser une connexion à la fin de chaque transaction. Ces informations d'état incluent la plupart des variables et des paramètres de configuration que vous pouvez modifier à l'aide des instructions `SET` ou `SELECT`. Les transactions SQL sur une connexion client peuvent se multiplexer entre les connexions de base de données sous-jacentes par défaut.

Vos connexions au proxy peuvent entrer dans un état appelé épinglage. Lorsqu'une connexion est épinglée, chaque transaction ultérieure utilise la même connexion de base de données sous-jacente jusqu'à la fin de la session. De même, les autres connexions client ne peuvent pas réutiliser cette connexion à la base de données tant que la session n'est pas terminée. La session se termine lorsque la connexion client est supprimée.

RDS Proxy épingle automatiquement une connexion client à une connexion de base de données spécifique lorsqu'il détecte un changement d'état de session qui n'est pas approprié pour d'autres sessions. L'épinglage réduit l'efficacité de la réutilisation des connexions. Si la totalité, ou presque, de vos connexions font l'objet d'un épinglage, pensez à modifier le code de votre application ou votre charge de travail afin de réduire les conditions à l'origine de l'épinglage.

Par exemple, si votre application modifie une variable de session ou un paramètre de configuration, les instructions ultérieures peuvent reposer sur la nouvelle variable ou le nouveau paramètre pour entrer en vigueur. Ainsi, lorsque le RDS Proxy traite des demandes de modification des variables ou des paramètres de configuration de session, il épingle cette session à la connexion de base de données. De cette manière, l'état de session reste en vigueur pour toutes les transactions ultérieures de la même session.

Cette règle ne s'applique pas à tous les paramètres que vous pouvez définir. RDS Proxy suit les modifications apportées au jeu de caractères, au classement, au fuseau horaire, à la validation automatique, à la base de données actuelle, au mode SQL et aux paramètres `session_track_schema`. Ainsi, RDS Proxy n'épingle pas la session lorsque vous modifiez ces éléments. Dans ce cas, RDS Proxy réutilise la connexion uniquement pour les autres sessions dont les valeurs de ces paramètres sont identiques.

Le réglage des performances RDS Proxy entraîne une tentative d'optimisation de la réutilisation des connexions au niveau de la transaction (multiplexage) en réduisant l'épinglage. Vous pouvez effectuer cette opération en procédant comme suit :

- Évitez les requêtes de base de données inutiles qui pourraient provoquer l'épinglage.
- Définissez les variables et les paramètres de configuration de manière cohérente sur toutes les connexions. De cette façon, les sessions ultérieures sont plus susceptibles de réutiliser les connexions qui ont ces paramètres particuliers.

  En revanche, pour PostgreSQL, la définition d'une variable entraîne l'épinglage de la session.
- Appliquez un filtre d'épinglage de session au proxy. Vous pouvez configurer certains types d'opérations pour qu'elles n'épinglent pas la session si vous savez que cela n'affecte pas le bon fonctionnement de votre application.
- Observez la fréquence de l'épinglage en surveillant la métrique CloudWatch `DatabaseConnectionsCurrentlySessionPinned`. Pour en savoir plus sur ce sujet et sur d'autres métriques CloudWatch, consultez la section Surveillance de RDS Proxy à l'aide d'Amazon CloudWatch (p. 196).
- Si vous utilisez des instructions `SET` pour exécuter une initialisation identique pour chaque connexion client, vous pouvez conserver le multiplexage au niveau de la transaction. Dans ce cas, vous déplacez les instructions qui définissent l'état initial de la session vers la requête d'initialisation utilisée par un proxy. Cette propriété est une chaîne contenant une ou plusieurs instructions SQL, séparées par des points-virgules.

Par exemple, vous pouvez définir une requête d'initialisation pour un proxy qui établit certains paramètres de configuration. RDS Proxy applique ensuite ces paramètres dès qu'il configure une nouvelle connexion pour ce proxy. Vous pouvez supprimer les instructions `SET` correspondantes de votre code d'application, afin qu'elles n'interfèrent pas avec le multiplexage au niveau de la transaction.

> **Important**
>
> Pour les proxy associés aux bases de données MySQL, ne définissez pas le paramètre de configuration `sql_auto_is_null` sur `true` ou sur une valeur différente de zéro dans la requête d'initialisation. Cela pourrait entraîner un comportement incorrect de l'application.

Le proxy épingle la session à la connexion en cours dans les situations suivantes où le multiplexage peut entraîner un comportement inattendu :

- Le proxy épingle la session si la taille de texte de l'instruction est supérieure à 16 Ko.
- Le proxy épingle la session en cas d'instructions préparées. Cette règle s'applique si l'instruction préparée utilise du texte SQL ou le protocole binaire.
- Le proxy épingle la session en cas d'instructions MySQL `LOCK TABLE`, `LOCK TABLES` ou `FLUSH TABLES WITH READ LOCK` explicites.
- Le proxy épingle la session lors de la définition d'une variable utilisateur ou d'une variable système (à quelques exceptions près). Si cette situation réduit trop la réutilisation de votre connexion, vous pouvez configurer les opérations `SET` pour qu'elles ne provoquent pas d'épinglage. Pour de plus amples informations sur la façon d'effectuer cette opération en définissant la propriété `SessionPinningFilters`, veuillez consulter Création d'un RDS Proxy (p. 181).
- Le proxy épingle la sessions lors de la création d'une table temporaire. De cette façon, le contenu de la table temporaire est conservé tout au long de la session, sans tenir compte des limites de transaction.
- L'appel aux fonctions MySQL `ROW_COUNT`, `FOUND_ROWS` et `LAST_INSERT_ID` provoque parfois l'épinglage.

  Les circonstances exactes dans lesquelles ces fonctions provoquent l'épinglage peuvent différer selon les versions Aurora MySQL compatibles avec MySQL 5.6 et MySQL 5.7.

L'appel de procédures et de fonctions stockées de MySQL ne provoque pas d'épinglage. RDS Proxy ne détecte aucun changement d'état de session résultant de ces appels. Par conséquent, assurez-vous que votre application ne modifie pas l'état de session dans les routines stockées et qu'elle repose sur cet état de session pour persister entre les transactions. Par exemple, si une procédure stockée crée une table temporaire destinée à persister entre les transactions, cette application n'est actuellement pas compatible avec RDS Proxy.

Pour PostgreSQL, les interactions suivantes provoquent l'épinglage :

- Utilisation des commandes SET
- Utilisation du protocole de requête étendu, par exemple en utilisant les paramètres par défaut JDBC
- Création de séquences, de tables ou de vues temporaires
- Déclaration de curseurs
- Suppression de l'état de la session
- Écoute d'un canal de notification
- Chargement d'un module de bibliothèque comme `auto_explain`
- Manipulation de séquences à l'aide de fonctions comme `nextval()` et `setval()`
- Interaction avec des verrous utilisant des fonctions comme `pg_advisory_lock()` et `pg_try_advisory_lock()`
- Utilisation d'instructions préparées, définition de paramètres ou rétablissement d'un paramètre à sa valeur par défaut

Si vous avez des connaissances avancées sur le comportement de votre application, vous pouvez ignorer le comportement d'épinglage de certaines instructions d'application. Pour ce faire, sélectionnez l'option Filtres d'épinglage de session lors de la création du proxy. Actuellement, vous pouvez désactiver l'épinglage de session pour définir des variables de session et des paramètres de configuration.

Pour les métriques relatives à la fréquence d'épinglage d'un proxy, veuillez consulter Surveillance de RDS Proxy à l'aide d'Amazon CloudWatch (p. 196).

Suppression d'un RDS Proxy

Vous pouvez supprimer un proxy si vous n'en avez plus besoin. Vous pouvez supprimer un proxy si l'application qui l'utilisait n'est plus pertinente. Vous pouvez également supprimer un proxy si vous mettez hors service l'instance ou le cluster de base de données qui lui est associé.

AWS Management Console

Suppression d'un proxy

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, sélectionnez Proxies.
3. Choisissez le proxy à supprimer de la liste.
4. Sélectionnez Suppression du proxy.

AWS CLI

Pour supprimer un proxy de base de données, utilisez la commande de l'AWS CLI delete-db-proxy. Pour supprimer les associations connexes, utilisez également la commande deregister-db-proxy-targets.

```
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]
```

API RDS

Pour supprimer un proxy de base de données, appelez la fonction d'API Amazon RDS DeleteDBProxy. Pour supprimer les éléments et associations connexes, vous appelez également les fonctions DeleteDBProxyTargetGroup et DeregisterDBProxyTargets.

Surveillance de RDS Proxy à l'aide d'Amazon CloudWatch

Vous pouvez surveiller RDS Proxy à l'aide de Amazon CloudWatch. CloudWatch recueille et transforme les données brutes des proxys en métriques lisibles et disponibles presque en temps réel. Pour trouver ces mesures dans la console CloudWatch, sélectionnez Métriques, puis RDS et enfin Métriques par proxy. Pour de plus amples informations, veuillez consulter Utilisation des métriques Amazon CloudWatch dans le Guide de l'utilisateur Amazon CloudWatch.

> **Note**
>
> RDS publie ces métriques pour chaque instance Amazon EC2 sous-jacente associée au proxy. Un proxy unique peut être servi par plusieurs instances EC2. Utilisez les statistiques CloudWatch pour agréger les valeurs d'un proxy sur l'ensemble des instances associées.

Certaines de ces métriques peuvent ne pas être visibles avant la première connexion réussie par un proxy.

Toutes les métriques RDS Proxy sont dans le groupe `proxy`.

Métrique	Description	Période de validité	Dimensions CloudWatch
`AvailabilityPercentage`	Pourcentage de temps pendant lequel le groupe cible était disponible dans le rôle indiqué par la dimension. Cette métrique est donnée toutes les minutes. `Average` est la statistique la plus utile pour cette métrique.	1 minute	`ProxyName`, `TargetGroup`, `TargetRole`
`ClientConnections`	Le nombre actuel de connexions client. Cette métrique est donnée toutes les minutes. `Sum` est la statistique la plus utile pour cette métrique.	1 minute	`ProxyName`
`ClientConnectionsClosed`	Le nombre de connexions client fermées. `Sum` est la statistique la plus utile pour cette métrique.	1 minute et plus	`ProxyName`
`ClientConnectionsNoTLS`	Le nombre actuel de connexions client sans TLS (Transport Layer Security). Cette métrique est donnée toutes les minutes. `Sum` est la statistique la plus utile pour cette métrique.	1 minute et plus	`ProxyName`
`ClientConnectionsReceived`	Le nombre de demandes de connexion client reçues. `Sum` est la statistique la plus utile pour cette métrique.	1 minute et plus	`ProxyName`
`ClientConnectionsSetupFailedAuth`	Nombre de tentatives de connexion client ayant échoué en raison d'une mauvaise configuration de l'authentification ou du protocole TLS. `Sum` est la statistique la plus utile pour cette métrique.	1 minute et plus	`ProxyName`

Métrique	Description	Période de validité	Dimensions CloudWatch
`ClientConnectionsSetup`	Le nombre de connexions client établies avec succès via n'importe quel mécanisme d'authentification avec ou sans protocole TLS. `Sum` est la statistique la plus utile pour cette métrique.	1 minute et plus	`ProxyName`
`ClientConnectionsTLS`	Nombre actuel de connexions client avec TLS. Cette métrique est donnée toutes les minutes. `Sum` est la statistique la plus utile pour cette métrique.	1 minute et plus	`ProxyName`
`DatabaseConnectionRequests`	Le nombre de demandes de création d'une connexion à une base de données. `Sum` est la statistique la plus utile pour cette métrique.	1 minute et plus	`ProxyName`, `TargetGroup`, `Target`
`DatabaseConnectionRequestsWithTLS`	Nombre de demandes de création d'une connexion à une base de données avec TLS. `Sum` est la statistique la plus utile pour cette métrique.	1 minute et plus	`ProxyName`, `TargetGroup`, `Target`
`DatabaseConnections`	Le nombre actuel de connexions à une base de données. Cette métrique est donnée toutes les minutes. `Sum` est la statistique la plus utile pour cette métrique.	1 minute	`ProxyName`, `TargetGroup`, `Target`
`DatabaseConnectionsBorrowLatency`	Temps, en microsecondes, nécessaire au proxy surveillé pour obtenir une connexion à la base de données. `Average` est la statistique la plus utile pour cette métrique.	1 minute et plus	`ProxyName`

Métrique	Description	Période de validité	Dimensions CloudWatch
`DatabaseConnectionsCurrentlyBorrowed`	Le nombre actuel de connexions à une base de données en état d'emprunt. Cette métrique est donnée toutes les minutes. `Sum` est la statistique la plus utile pour cette métrique.	1 minute	`ProxyName`, `TargetGroup`, `Target`
`DatabaseConnectionsCurrentlyInTransaction`	Nombre actuel de connexions à la base de données dans une transaction. Cette métrique est donnée toutes les minutes. `Sum` est la statistique la plus utile pour cette métrique.	1 minute	`ProxyName`, `TargetGroup`, `Target`
`DatabaseConnectionsCurrentlySessionPinned`	Nombre de connexions à la base de données actuellement épinglées en raison d'opérations dans les demandes client qui modifient l'état de session. Cette métrique est donnée toutes les minutes. `Sum` est la statistique la plus utile pour cette métrique.	1 minute	`ProxyName`, `TargetGroup`, `Target`
`DatabaseConnectionsSetupFailed`	Le nombre de demandes de connexion à une base de données qui ont échoué. `Sum` est la statistique la plus utile pour cette métrique.	1 minute et plus	`ProxyName`, `TargetGroup`, `Target`
`DatabaseConnectionsSetupSucceeded`	Le nombre de connexions à une base de données correctement établies avec ou sans protocole TLS. `Sum` est la statistique la plus utile pour cette métrique.	1 minute et plus	`ProxyName`, `TargetGroup`, `Target`

Métrique	Description	Période de validité	Dimensions CloudWatch
`DatabaseConnectionsWithTLS`	Nombre actuel de connexions à une base de données avec TLS. Cette métrique est donnée toutes les minutes. `Sum` est la statistique la plus utile pour cette métrique.	1 minute	`ProxyName`, `TargetGroup`, `Target`
`MaxDatabaseConnectionsAllowed`	Le nombre maximal de connexions à une base de données autorisées. Cette métrique est donnée toutes les minutes. `Sum` est la statistique la plus utile pour cette métrique.	1 minute	`ProxyName`, `TargetGroup`, `Target`
`QueryDatabaseResponseLatency`	Temps en microsecondes, pris par la base de données pour répondre à la requête. `Average` est la statistique la plus utile pour cette métrique.	1 minute et plus	`ProxyName`, `TargetGroup`, `Target`
`QueryRequests`	Le nombre de requêtes reçues. Une requête comprenant plusieurs instructions est comptée comme étant une seule et même requête. `Sum` est la statistique la plus utile pour cette métrique.	1 minute et plus	`ProxyName`
`QueryRequestsNoTLS`	Nombre de requêtes reçues de connexions non TLS. Une requête comprenant plusieurs instructions est comptée comme étant une seule et même requête. `Sum` est la statistique la plus utile pour cette métrique.	1 minute et plus	`ProxyName`

Métrique	Description	Période de validité	Dimensions CloudWatch
`QueryRequestsTLS`	Nombre de requêtes reçues des connexions TLS. Une requête comprenant plusieurs instructions est comptée comme étant une seule et même requête. `Sum` est la statistique la plus utile pour cette métrique.	1 minute et plus	`ProxyName`
`QueryResponseLatency`	Temps, en microsecondes, entre l'obtention d'une demande de requête et le proxy qui y répond. `Average` est la statistique la plus utile pour cette métrique.	1 minute et plus	`ProxyName`

Exemples de ligne de commande pour RDS Proxy

Pour voir comment les combinaisons de commandes de connexion et d'instructions SQL interagissent avec RDS Proxy, observez les exemples suivants.

Exemples

- Préservation des connexions à une base de données MySQL lors d'un basculement
- Réglage du paramètre max_connections pour un cluster de bases de données Aurora

Example Préservation des connexions à une base de données MySQL lors d'un basculement

Cet exemple MySQL montre comment les connexions ouvertes continuent de fonctionner pendant un basculement, par exemple lorsque vous redémarrez une base de données ou qu'un problème la rend indisponible. Cet exemple utilise un proxy nommé `the-proxy` et un cluster de base de données Aurora avec des instances de base de données `instance-8898` et `instance-9814`. Lorsque vous exécutez la commande `failover-db-cluster` à partir de la ligne de commande Linux, l'instance de rédacteur à laquelle le proxy est connecté change d'instance de base de données. Vous pouvez voir que l'instance de base de données associée au proxy change pendant que la connexion est ouverte.

```
$ 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-id 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-id 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 Réglage du paramètre max_connections pour un cluster de bases de données Aurora

Cet exemple montre comment ajuster le paramètre `max_connections` pour un cluster de base de données Aurora MySQL. Pour ce faire, vous créez votre propre groupe de paramètres de cluster de base de données en fonction des paramètres par défaut des clusters compatibles avec MySQL 5.6 ou 5.7. Vous indiquez une valeur pour le paramètre `max_connections`, en remplaçant la formule qui définit la valeur par défaut. Vous associez le groupe de paramètres de cluster de base de données à votre cluster de base de données.

```
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"
```

Résolution des problèmes liés au RDS Proxy

Vous trouverez ci-dessous des idées de dépannage pour certains problèmes RDS Proxy courants, ainsi que des informations sur les journaux CloudWatch pour RDS Proxy.

Rubriques

- Problèmes courants et solutions correspondantes (p. 203)
- Utilisation des journaux CloudWatch pour RDS Proxy (p. 207)
- Vérification de la connectivité pour un proxy (p. 208)

Problèmes courants et solutions correspondantes

Pour connaître les causes possibles et les solutions à certains problèmes courants que vous pourriez rencontrer en utilisant RDS Proxy, reportez-vous à la section suivante.

Vous pouvez rencontrer les problèmes suivants lors de la création d'un proxy ou de la connexion à un proxy.

Erreur	Causes ou solutions de contournement
`403: The security token included in the request is invalid`	Sélectionnez un rôle IAM existant au lieu d'en créer un nouveau.

Vous pouvez rencontrer les problèmes suivants lors de la connexion à un proxy MySQL.

Erreur	Causes ou solutions de contournement
`ERROR 1040 (HY000): Connections rate`	Le taux de demandes de connexion du client au proxy a dépassé la limite.

Erreur	Causes ou solutions de contournement
`limit exceeded (limit_value)`	
`ERROR 1040 (HY000): IAM authentication rate limit exceeded`	Le nombre de demandes de connexion simultanée avec authentification IAM du client au proxy a dépassé la limite.
`ERROR 1040 (HY000): Number simultaneous connections exceeded (limit_value)`	Le nombre de demandes de connexion simultanée du client au proxy a dépassé la limite.
`ERROR 1045 (28000): Access denied for user 'DB_USER'@'%' (using password: YES)`	Les causes possibles sont notamment les suivantes : • Le secret Secrets Manager utilisé par le proxy ne correspond pas au nom d'utilisateur et au mot de passe d'un utilisateur de base de données existant. Mettez à jour les informations d'identification dans le secret Secrets Manager ou assurez-vous que l'utilisateur de base de données existe et possède le même mot de passe que celui du secret.
`ERROR 1105 (HY000): Unknown error`	Une erreur inconnue s'est produite.
`ERROR 1231 (42000): Variable ''character_set_client'' can't be set to the value of value`	La valeur définie pour le paramètre `character_set_client` n'est pas valide. Par exemple, la valeur `ucs2` n'est pas valide, car elle peut bloquer le serveur MySQL.
`ERROR 3159 (HY000): This RDS Proxy requires TLS connections.`	Vous avez activé le paramètre Exiger la sécurité de la couche de transport dans le proxy, mais votre connexion a inclus le paramètre `ssl-mode=DISABLED` dans le client MySQL. Effectuez l'une des actions suivantes : • Désactivez le paramètre Exiger la sécurité de la couche de transport pour le proxy. • Connectez-vous à la base de données en utilisant le paramètre minimal de `ssl-mode=REQUIRED` dans le client MySQL.
`ERROR 2026 (HY000): SSL connection error: Internal Server Error`	La négociation TLS avec le proxy a échoué. Les causes possibles sont notamment les suivantes : • SSL est requis, mais le serveur ne le prend pas en charge. • Une erreur interne du serveur s'est produite. • Une mauvaise négociation s'est produite.

Erreur	Causes ou solutions de contournement
`ERROR 9501 (HY000): Timed-out waiting to acquire database connection`	Le proxy a expiré en attendant l'obtention d'une connexion à la base de données. Les causes possibles sont notamment les suivantes : • Le proxy n'est pas en mesure d'établir une connexion à la base de données, car le nombre maximal de connexions a été atteint. • Le proxy n'est pas en mesure d'établir une connexion à la base de données, car la base de données n'est pas disponible.

Vous pouvez rencontrer les problèmes suivants lors de la connexion à un proxy PostgreSQL.

Erreur	Cause	Solution
`IAM authentication is allowed only with SSL connections.`	L'utilisateur a essayé de se connecter à la base de données à l'aide de l'authentification IAM en utilisant le paramètre `sslmode=disable` du client PostgreSQL.	L'utilisateur doit se connecter à la base de données en utilisant le paramètre minimal `sslmode=require` du client PostgreSQL. Pour de plus amples informations, veuillez consulter la documentation PostgreSQL SSL Support .
`This RDS Proxy requires TLS connections.`	L'utilisateur a activé l'option Exiger la sécurité de la couche de transportmais a essayé de se connecter en utilisant `sslmode=disable` dans le client PostgreSQL.	Pour corriger cette erreur, effectuez l'une des opérations suivantes : • Désactivez l'option Exiger la sécurité de la couche de transport du proxy. • Connectez-vous à la base de données en utilisant le paramètre minimal `sslmode=allow` du client PostgreSQL.
`IAM authentication failed for user` *`user_name`*`. Check the IAM token for this user and try again.`	Cette erreur peut être due aux raisons suivantes : • Le client a indiqué un nom d'utilisateur IAM incorrect. • Le client a fourni un jeton d'autorisation IAM incorrect pour l'utilisateur • Le client utilise une stratégie IAM qui ne dispose pas des autorisations nécessaires. • Le client a fourni un jeton d'autorisation IAM expiré pour l'utilisateur.	Pour corriger cette erreur, procédez comme suit : 1. Vérifiez que l'utilisateur IAM indiqué existe. 2. Vérifiez que le jeton d'autorisation IAM appartient à l'utilisateur IAM indiqué. 3. Vérifiez que la stratégie IAM dispose des autorisations adéquates pour RDS. 4. Vérifiez la validité du jeton d'autorisation IAM utilisé.
`This RDS proxy has no credentials for the role` *`role_name`*`. Check the`	Il n'y a pas de secret Secrets Manager pour ce rôle.	Ajoutez un secret Secrets Manager pour ce rôle.

Erreur	Cause	Solution
`credentials for this role and try again.`		
`RDS supports only IAM or MD5 authentication.`	Le client de base de données utilisé pour se connecter au proxy utilise un mécanisme d'authentification qui n'est pas actuellement pris en charge par le proxy, tel que SCRAM-SHA-256.	Si vous n'utilisez pas l'authentification IAM, utilisez uniquement l'authentification par mot de passe MD5.
`A user name is missing from the connection startup packet. Provide a user name for this connection.`	Le client de base de données utilisé pour la connexion au proxy n'envoie pas de nom d'utilisateur lorsqu'il tente d'établir une connexion.	Veillez à définir un nom d'utilisateur lors de la configuration d'une connexion au proxy à l'aide du client PostgreSQL de votre choix.
`Feature not supported: RDS Proxy supports only version 3.0 of the PostgreSQL messaging protocol.`	Le client PostgreSQL utilisé pour la connexion au proxy utilise un protocole antérieur à la version 3.0.	Utilisez un client PostgreSQL plus récent qui prend en charge le protocole de messagerie 3.0. Si vous utilisez l'interface de ligne de commande `psql` de PostgreSQL, utilisez une version supérieure ou égale à 7.4.
`Feature not supported: RDS Proxy currently doesn't support streaming replication mode.`	Le client PostgreSQL utilisé pour la connexion au proxy essaie d'utiliser le mode de réplication de streaming, lequel n'est actuellement pas pris en charge par RDS Proxy.	Désactivez le mode de réplication de streaming sur le client PostgreSQL utilisé pour la connexion.
`Feature not supported: RDS Proxy currently doesn't support the option` *`option_name`*`.`	Par le biais du message de démarrage, le client PostgreSQL utilisé pour la connexion au proxy demande une option qui n'est pas actuellement prise en charge par RDS Proxy.	Désactivez l'option indiquée comme non prise en charge dans le message ci-dessus sur le client PostgreSQL utilisé pour la connexion.
`The IAM authentication failed because of too many competing requests.`	Le nombre de demandes de connexion simultanée avec authentification IAM du client au proxy a dépassé la limite.	Réduisez le taux d'établissement de connexions à l'aide de l'authentification IAM à partir d'un client PostgreSQL.
`The maximum number of client connections to the proxy exceeded` *`number_value`*`.`	Le nombre de demandes de connexion simultanée du client au proxy a dépassé la limite.	Réduisez le nombre de connexions actives des clients PostgreSQL à ce proxy RDS.
`Rate of connection to proxy exceeded` *`number_value`*`.`	Le taux de demandes de connexion du client au proxy a dépassé la limite.	Réduisez le taux d'établissement de connexions à partir d'un client PostgreSQL.

Erreur	Cause	Solution
`The password that was provided for the role` *`role_name`* `is wrong.`	Le mot de passe de ce rôle ne correspond pas au secret Secrets Manager.	Vérifiez le secret de ce rôle dans Secrets Manager pour voir si le mot de passe est le même que celui utilisé sur votre client PostgreSQL.
`The IAM authentication failed for the role` *`role_name`*`. Check the IAM token for this role and try again.`	Il y a un problème avec le jeton IAM utilisé pour l'authentification IAM.	Générez un nouveau jeton d'authentification et utilisez-le dans une nouvelle connexion.
`IAM is allowed only with SSL connections.`	Un client a essayé de se connecter à l'aide de l'authentification IAM, mais le protocole SSL n'était pas activé.	Activez SSL sur le client PostgreSQL.
`Unknown error.`	Une erreur inconnue s'est produite.	Contactez AWS Support pour que nous analysions le problème.
`Timed-out waiting to acquire database connection.`	Le proxy a expiré en attendant l'obtention d'une connexion à la base de données. Les causes possibles sont notamment les suivantes : • Le proxy ne peut pas établir une connexion à la base de données, car le nombre maximal de connexions a été atteint. • Le proxy ne peut pas établir une connexion à la base de données, car la base de données n'est pas disponible.	Solutions possibles : • Vérifiez la cible de l'instance de base de données RDS ou l'état du cluster de bases de données Aurora pour vérifier sa disponibilité. • Vérifiez s'il y a des transactions et/ou des requêtes de longue durée en cours d'exécution. Elles peuvent utiliser les connexions de base de données à partir du groupe de connexions pendant une longue période.
`Request returned an error:` *`database_error`*`.`	La connexion à la base de données établie à partir du proxy a renvoyé une erreur.	La solution dépend de l'erreur de base de données spécifique. Par exemple : `Request returned an error: database "your-database-name" does not exist`. Cela signifie que le nom de base de données spécifié ou le nom d'utilisateur utilisé comme nom de base de données (au cas où un nom de base de données n'a pas été spécifié) n'existe pas sur le serveur de base de données.

Utilisation des journaux CloudWatch pour RDS Proxy

Vous pouvez trouver les journaux d'activité de RDS Proxy sous CloudWatch dans la AWS Management Console. Chaque proxy dispose d'une entrée dans la page Groupes de journaux.

> **Important**
>
> Ces journaux sont destinés à la consommation humaine à des fins de dépannage et non à un accès par programmation. Le format et le contenu des journaux sont susceptibles d'être modifiés.

Vérification de la connectivité pour un proxy

Vous pouvez utiliser les commandes suivantes pour vérifier que tous les composants du mécanisme de connexion peuvent communiquer avec les autres composants.

Examinez le proxy lui-même à l'aide de la commande describe-db-proxies. Examinez également le groupe cible associé à l'aide de describe-db-proxy-target-groups. Vérifiez que les détails des cibles correspondent à l'instance de base de données RDS ou au cluster de base de données Aurora que vous avez l'intention d'associer au proxy. Utilisez des commandes telles que les suivantes.

```
aws rds describe-db-proxies --db-proxy-name $DB_PROXY_NAME
aws rds describe-db-proxy-target-groups --db-proxy-name $DB_PROXY_NAME
```

Pour confirmer que le proxy peut se connecter à la base de données sous-jacente, examinez les cibles spécifiées dans les groupes cibles à l'aide de la commande describe-db-proxy-targets. Utilisez une commande telle que la suivante.

```
aws rds describe-db-proxy-targets --db-proxy-name $DB_PROXY_NAME
```

La sortie de la commande describe-db-proxy-targets contient un champ `TargetHealth`. Vous pouvez examiner les champs `State`, `Reason` et `Description` dans `TargetHealth` pour vérifier si le proxy peut communiquer avec l'instance de base de données sous-jacente.

- Si la valeur `State` est `AVAILABLE`, cela indique que le proxy peut se connecter à l'instance de base de données.
- Si la valeur `State` est `UNAVAILABLE`, cela signale un problème de connexion temporaire ou permanent. Dans ce cas, examinez les champs `Description` et `Reason`. Par exemple, si `Reason` a une valeur `PENDING_PROXY_CAPACITY`, essayez de vous connecter à nouveau une fois que le proxy a terminé son opération de mise à l'échelle. Si `Reason` a une valeur `UNREACHABLE`, `CONNECTION_FAILED` ou `AUTH_FAILURE`, utilisez l'explication du champ `Description` pour vous aider à diagnostiquer le problème.
- Le champ `State` peut avoir une valeur `REGISTERING` pendant une courte période avant de passer à `AVAILABLE` ou `UNAVAILABLE`.

Si la commande Netcat (`nc`) suivante aboutit, vous pouvez accéder au point de terminaison du proxy à partir de l'instance EC2 ou d'un autre système auquel vous êtes connecté. Cette commande signale un échec si vous n'êtes pas dans le même VPC que le proxy et la base de données associée. Vous pouvez peut-être vous connecter directement à la base de données sans vous trouver dans le même VPC. Cependant, vous ne pouvez pas vous connecter au proxy sauf si vous êtes dans le même VPC.

```
nc -zx MySQL_proxy_endpoint 3306

nc -zx PostgreSQL_proxy_endpoint 5432
```

Vous pouvez utiliser les commandes suivantes pour vous assurer que votre instance EC2 possède les propriétés requises. Le VPC de l'instance EC2 doit notamment être le même que le VPC de l'instance de base de données RDS ou du cluster de base de données Aurora auquel le proxy se connecte.

```
aws ec2 describe-instances --instance-ids your_ec2_instance_id
```

Examinez les secrets Secrets Manager utilisés pour le proxy.

```
aws secretsmanager list-secrets
aws secretsmanager get-secret-value --secret-id your_secret_id
```

Assurez-vous que le champ `SecretString` affiché par `get-secret-value` est codé au format d'une chaîne JSON qui inclut les champs `username`et `password`. L'exemple suivant illustre le format du champ `SecretString`.

```
{
  "ARN": "some_arn",
  "Name": "some_name",
  "VersionId": "some_version_id",
  "SecretString": '{"username":"some_username","password":"some_password"}',
  "VersionStages": [ "some_stage" ],
  "CreatedDate": some_timestamp
}
```

Utilisation de RDS Proxy avec AWS CloudFormation

Vous pouvez utiliser RDS Proxy avec AWS CloudFormation. Cela vous aide à créer des groupes de ressources connexes, y compris un proxy qui peut se connecter à une instance de base de données Amazon RDS ou à un cluster de base de données Aurora nouvellement créé. La prise en charge de RDS Proxy dans AWS CloudFormation implique deux nouveaux types de registre : `DBProxy` et `DBProxyTargetGroup`.

La liste suivante présente un exemple de modèle AWS CloudFormation pour 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
     InstanceIdentifiers:
       - Fn::ImportValue: DBInstanceName
   DependsOn: DBProxy
```

Pour de plus amples informations sur les ressources Amazon RDS et Aurora que vous pouvez créer avec AWS CloudFormation, veuillez consulter RDS Référence de type de ressource.

Utilisation de groupes d'options

Certains moteurs DB offrent des fonctions supplémentaires qui facilitent la gestion des données et des bases de données ainsi que la fourniture d'une sécurité supplémentaire pour votre base de données.

Amazon RDS utilise les groupes d'options pour activer et configurer ces fonctions. Un groupe d'options peut spécifier des fonctions, appelées options, qui sont disponibles pour une instance de base de données Amazon RDS spécifique. Les options peuvent avoir des paramètres spécifiant le mode de fonctionnement de l'option. Lorsque vous associez une instance de base de données a un groupe d'options, les paramètres d'options et les options spécifiés sont activés pour cette instance de base de données.

Amazon RDS prend en charge les options pour les moteurs de base de données suivants :

Moteur de base de données	Documentation
`MariaDB`	Options pour le moteur de base de données MariaDB (p. 581)
`Microsoft SQL Server`	Options pour le moteur de base de données Microsoft SQL Server (p. 699)
`MySQL`	Options pour les instances de base de données MySQL (p. 873)
`Oracle`	Options propres aux instances de bases de données Oracle (p. 1013)
`PostgreSQL`	PostgreSQL n'utilise pas d'options et de groupes d'options. PostgreSQL utilise des extensions et des modules pour fournir des fonctionnalités supplémentaires. Pour plus d'informations, consultez Fonctions et extensions PostgreSQL prises en charge (p. 1488).

Présentation des groupes d'options

Amazon RDS fournit un groupe d'options vide par défaut pour chaque nouvelle instance DB. Vous ne pouvez pas modifier ce groupe d'options par défaut, mais tout nouveau groupe d'options que vous créez tire ses paramètres du groupe d'options par défaut. Pour appliquer une option à une instance de base de données, vous devez effectuer les opérations suivantes :

1. Créer un groupe d'options ou copier ou modifier un groupe existant.
2. Ajouter une ou plusieurs options au groupe.
3. Associer un groupe d'options à une instance de base de données.

   Pour associer un groupe d'options à une instance de base de données, modifiez l'instance de base de données. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Les instances de base de données et les snapshots DB peuvent tous deux être associés à un groupe d'options. Dans certains cas, vous pouvez effectuer une restauration à partir d'un instantané de base de données ou une restauration à un moment dans le temps pour une instance de base de données. Dans ces cas, le groupe d'options associé à l'instantané de base de données ou à l'instance de base de données est associé, par défaut, à l'instance de base de données restaurée. Vous pouvez associer un groupe d'options différent à une instance de base de données restaurée. Toutefois, le nouveau groupe d'options doit contenir toutes les options persistantes ou permanentes qui étaient incluses dans le groupe d'origine. Les options persistantes et permanentes sont décrites ci-dessous.

Les options nécessitent d'avantage de mémoire pour s'exécuter sur une instance de base de données. Ainsi, selon votre utilisation actuelle de l'instance de base de données, il vous faudra peut-être lancer une instance de plus grande taille pour les utiliser. Par exemple, Oracle Enterprise Manager Database Control utilise environ 300 Mo de RAM. Si vous activez cette option pour une petite instance de base de données, vous pouvez rencontrer des problèmes de performances ou de mémoire insuffisante.

Options persistantes et permanentes

Deux types d'options, persistantes et permanentes, nécessitent une considération spéciale lorsque vous les ajoutez à un groupe d'options.

Les options persistantes ne peuvent pas être supprimées d'un groupe d'options tant que des instances de base de données sont associées au groupe d'options. L'option TDE pour Microsoft SQL Server TDE (transparent data encryption) est un exemple d'option persistante. Pour qu'une option persistante puisse être supprimée, vous devez dissocier toutes les instances de base de données du groupe d'options. Dans certains cas, vous pouvez effectuer une restauration simple ou une restauration à un moment dans le temps à partir d'un instantané de base de données. Dans ces cas, si le groupe d'options associé à cet instantané de base de données contient une option persistante, vous ne pouvez associer l'instance de base de données restaurée qu'à ce groupe d'options.

Les options permanentes, telles que l'option TDE pour Oracle Advanced Security TDE, ne peuvent jamais être supprimées d'un groupe d'options. Vous pouvez cependant modifier le groupe d'options d'une instance de base de données qui utilise l'option permanente. Notez cependant que le groupe d'options associé à l'instance de base de données doit inclure la même option permanente. Dans certains cas, vous pouvez effectuer une restauration simple ou une restauration à un moment dans le temps à partir d'un instantané de base de données. Dans ces cas, si le groupe d'options associé à cet instantané de base de données contient une option permanente, vous ne pouvez associer l'instance de base de données restaurée qu'à un groupe d'options avec cette option permanente.

Pour les instances de base de données Oracle, vous pouvez copier les instantanés de bases de données partagés ayant les options `Timezone` ou `OLS` (ou les deux). Pour ce faire, spécifiez un groupe d'options cibles qui inclut ces options lorsque vous copiez l'instantané de bases de données. L'option OLS est permanente et persistante uniquement pour les instances de bases de données Oracle exécutant Oracle version 12.2 ou ultérieure. Pour de plus amples informations sur ces options, veuillez consulter Fuseau horaire Oracle (p. 1088) et Oracle Label Security (p. 1054).

Considérations sur le VPC et la plateforme

Lorsqu'un groupe d'options est affecté à une instance de base de données, il est lié à la plateforme sur laquelle se trouve l'instance de base de données. Cette plateforme peut être un VPC pris en charge par le service Amazon VPC ou une instance EC2-Classic (non VPC) prise en charge par le service Amazon EC2. Pour plus d'informations sur ces deux plateformes, consultez la page Amazon EC2 et Amazon Virtual Private Cloud.

Si une instance de base de données est dans un VPC, le groupe d'options associé à l'instance est lié à ce VPC. Cela signifie que vous ne pouvez pas utiliser le groupe d'options assigné à une instance de base de données si vous tentez de restaurer l'instance dans un VPC différent ou sur une autre plateforme. Si vous restaurez une instance de base de données dans un VPC différent ou sur une autre plateforme, vous pouvez effectuer l'une des opérations suivantes :

- Affectez le groupe d'options par défaut à l'instance de base de données.
- Affectez un groupe d'options qui est lié à ce VPC ou à cette plateforme.
- Créez un nouveau groupe d'options et affectez-le à l'instance de base de données.

Avec les options permanentes ou persistantes, telles qu'Oracle TDE, vous devez créer un nouveau groupe d'options incluant l'option persistante ou permanente lorsque vous restaurez une instance de base de données dans un VPC différent.

Les paramètres d'options contrôlent le comportement d'une option. Par exemple, l'option Oracle Advanced Security `NATIVE_NETWORK_ENCRYPTION` a un paramètre que vous pouvez utiliser pour spécifier l'algorithme de chiffrement pour le trafic réseau vers et depuis l'instance de base de données. Certains paramètres d'options sont optimisés pour une utilisation avec Amazon RDS et ne peuvent pas être modifiés.

Options mutuellement exclusives

Certaines options sont mutuellement exclusives. Vous pouvez utiliser l'une ou l'autre, mais pas les deux en même temps. Les options suivantes sont mutuellement exclusives :

- Oracle Enterprise Manager Database Express (p. 1037) et Oracle Management Agent pour Enterprise Manager Cloud Control (p. 1042).
- Oracle NNE (Native Network Encryption) (p. 1062) et Oracle Secure Sockets Layer (SSL) (p. 1068).

Création d'un groupe d'options

Vous pouvez créer un groupe d'options qui tire ses paramètres du groupe par défaut, puis ajouter une ou plusieurs options au nouveau groupe d'options. Si vous avez déjà un groupe d'options existant, vous pouvez également copier ce groupe avec toutes ses options dans un nouveau groupe d'options. Pour plus d'informations, consultez Copie d'un groupe d'options (p. 213).

Une fois que vous avez créé un groupe d'options, il ne contient pas d'options. Pour savoir comment ajouter des options au groupe d'options, consultez la page Ajout d'une option à un groupe d'options (p. 214). Une fois que vous avez ajouté les options que vous voulez, vous pouvez associer une instance de base de données au groupe d'options afin que ces dernières deviennent disponibles sur l'instance de base de données. Pour plus d'informations sur l'association d'un groupe d'options à une instance de base de données, consultez la documentation pour votre moteur spécifique répertoriée à l'adresse Utilisation de groupes d'options (p. 209).

Console

Une manière de créer un groupe d'options consiste à utiliser la AWS Management Console.

Pour créer un nouveau groupe d'options à l'aide de la console

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes d'options.
3. Choisissez Create group.
4. Dans la fenêtre Créer un groupe d'options, procédez comme suit :
   a. Dans la zone Nom, saisissez un nom pour le groupe d'options qui soit unique dans votre compte AWS. Le nom ne peut contenir que des lettres, des chiffres et des tirets.
   b. Pour Description, saisissez une brève description du groupe d'options. La description est utilisée à des fins d'affichage.
   c. Dans la zone Moteur, choisissez le moteur de base de données que vous souhaitez.
   d. Dans la zone Version majeure du moteur, choisissez la version majeure du moteur de base de données que vous souhaitez.
5. Pour continuer, choisissez Créer. Pour annuler l'opération à la place, choisissez Cancel (Annuler).

AWS CLI

Pour créer un groupe d'options, utilisez la commande `create-option-group` de l'AWS CLI avec les paramètres obligatoires suivants.

- `--option-group-name`
- `--engine-name`
- `--major-engine-version`

- `--option-group-description`

Example

L'exemple suivant crée un groupe d'options nommé `testoptiongroup` qui est associé au moteur de base de données Oracle Enterprise Edition. La description est entre guillemets.

Pour Linux, macOS ou 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"
```

Pour Windows :

```
aws rds create-option-group ^
    --option-group-name testoptiongroup ^
    --engine-name oracle-ee ^
    --major-engine-version 12.1 ^
    --option-group-description "Test option group"
```

API RDS

Pour créer un groupe d'options, appelez l'opération d'API Amazon RDS `CreateOptionGroup`. Incluez les paramètres suivants :

- `OptionGroupName`
- `EngineName`
- `MajorEngineVersion`
- `OptionGroupDescription`

Copie d'un groupe d'options

Vous pouvez utiliser le AWS CLI ou l'API Amazon RDS pour copier un groupe d'options. La copie d'un groupe d'options est une solution pratique lorsque vous avez un groupe d'options existant et que vous souhaitez inclure la plupart de ses valeurs et paramètres personnalisés dans un nouveau groupe d'options. Vous pouvez aussi faire une copie d'un groupe d'options que vous utilisez en production, puis modifier la copie pour tester d'autres paramètres d'options.

> **Note**
>
> Actuellement, vous ne pouvez pas copier un groupe d'options vers une autre région AWS.

AWS CLI

Pour copier un groupe d'options, utilisez la commande copy-option-group de l'AWS CLI. Inclure les options requises suivantes :

- `--source-option-group-identifier`
- `--target-option-group-identifier`

- `--target-option-group-description`

Example

L'exemple suivant crée un groupe d'options nommé `new-option-group` qui est une copie locale du groupe d'options `my-option-group`.

Pour Linux, macOS ou 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"
```

Pour 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"
```

API RDS

Pour copier un groupe d'options, appelez l'opération d'API Amazon RDS CopyOptionGroup. Incluez les paramètres requis suivants.

- `SourceOptionGroupIdentifier`
- `TargetOptionGroupIdentifier`
- `TargetOptionGroupDescription`

Ajout d'une option à un groupe d'options

Vous pouvez ajouter une option à un groupe d'options existant. Une fois que vous avez ajouté les options que vous voulez, vous pouvez associer une instance de base de données au groupe d'options afin que ces dernières deviennent disponibles sur l'instance de base de données. Pour plus d'informations sur l'association d'un groupe d'options à une instance de base de données, consultez la documentation pour votre moteur de base de données spécifique répertorié à l'adresse Utilisation de groupes d'options (p. 209).

Les modifications apportées au groupe d'options doivent être appliquées immédiatement dans deux cas :

- Lorsque vous ajoutez une option qui ajoute ou met à jour une valeur de port, telle que l'option `OEM`.
- Lorsque vous ajoutez ou supprimez un groupe d'options avec une option qui inclut une valeur de port.

Dans ces cas, choisissez l'option Appliquer immédiatement dans la console. Vous pouvez aussi inclure l'option `--apply-immediately` si vous utilisez l'AWS CLI ou définir le paramètre `ApplyImmediately` sur `true` si vous utilisez l'API Amazon RDS. Les options qui n'incluent pas de valeur de port peuvent être appliquées immédiatement ou pendant la fenêtre de maintenance suivant pour l'instance de base de données.

> **Note**
>
> Si vous spécifiez un groupe de sécurité comme valeur d'une option dans un groupe d'options, vous gérez le groupe de sécurité en modifiant le groupe d'options. Vous ne pouvez pas modifier

ou supprimer ce groupe de sécurité en modifiant une instance de base de données. En outre, le groupe de sécurité n'apparaît pas dans les détails de l'instance de base de données dans l'AWS Management Console ou dans la sortie de la commande de l'AWS CLI `describe-db-instances`.

Console

Vous pouvez utiliser la AWS Management Console pour ajouter une option à un groupe d'options.

Pour ajouter une option à un groupe d'options à l'aide de la console

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes d'options.
3. Cochez la case pour le groupe d'options que vous souhaitez modifier, puis choisissez Ajouter une option.

4. Dans la fenêtre Ajouter une option, procédez comme suit :
   a. Choisissez l'option que vous souhaitez ajouter. Selon l'option que vous sélectionnez, vous devrez peut-être fournir des valeurs supplémentaires. Par exemple, lorsque vous sélectionnez l'option `OEM`, vous devez également saisir une valeur de port et spécifier un groupe de sécurité.
   b. Pour activer l'option sur toutes les instances de base de données associées dès que vous l'ajoutez, pour Apply Immediately (Appliquer immédiatement), choisissez Oui. Si vous choisissez Non (valeur par défaut), l'option est activée pour chaque instance de base de données associée pendant sa fenêtre de maintenance suivante.

5. Lorsque les paramètres vous conviennent, choisissez Ajouter une option.

AWS CLI

Pour ajouter une option à un groupe d'options, exécutez la commande add-option-to-option-group d'AWS CLI avec l'option que vous souhaitez ajouter. Pour activer immédiatement la nouvelle option sur toutes les instances de base de données associées, incluez le paramètre `--apply-immediately`. Par défaut, l'option est activée pour chaque instance de base de données associée pendant sa fenêtre de maintenance suivante. Incluez le paramètre requis suivant :

- `--option-group-name`

Example

L'exemple suivant ajoute l'option Oracle Enterprise Manager Database Control (OEM) à un groupe d'options nommé `testoptiongroup` et l'active immédiatement. Même si vous utilisez le groupe de sécurité par défaut, vous devez le spécifier.

Pour Linux, macOS ou Unix :

```
aws rds add-option-to-option-group \
 --option-group-name testoptiongroup \
 --options OptionName=OEM,Port=5500,DBSecurityGroupMemberships=default \
 --apply-immediately
```

Pour Windows :

```
aws rds add-option-to-option-group ^
 --option-group-name testoptiongroup ^
 --options OptionName=OEM,Port=5500,DBSecurityGroupMemberships=default ^
 --apply-immediately
```

Le résultat de la commande est similaire à ce qui suit :

```
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
DBSECURITYGROUPMEMBERSHIPS   default authorized
```

Example

L'exemple suivant permet d'ajouter l'option Oracle OEM à un groupe d'options. Il spécifie également un port personnalisé et une paire de groupes de sécurité VPC Amazon EC2 à utiliser pour ce port.

Pour Linux, macOS ou Unix :

```
aws rds add-option-to-option-group \
 --option-group-name testoptiongroup \
 --options OptionName=OEM,Port=5500,VpcSecurityGroupMemberships="sg-test1,sg-test2" \
 --apply-immediately
```

Pour Windows :

```
aws rds add-option-to-option-group ^
 --option-group-name testoptiongroup ^
 --options OptionName=OEM,Port=5500,VpcSecurityGroupMemberships="sg-test1,sg-test2" ^
 --apply-immediately
```

Le résultat de la commande est similaire à ce qui suit :

```
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
VPCSECURITYGROUPMEMBERSHIPS     active  sg-test1
VPCSECURITYGROUPMEMBERSHIPS     active  sg-test2
```

Example

L'exemple suivant ajoute l'option Oracle NATIVE_NETWORK_ENCRYPTION à un groupe d'options et spécifie les paramètres d'options. Si aucun paramètre d'options n'est spécifié, les valeurs par défaut sont utilisées.

Pour Linux, macOS ou 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_ENC
 \
  --apply-immediately
```

Pour 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_E
 ^
--apply-immediately
```

Le résultat de la commande est similaire à ce qui suit :

```
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
```

API RDS

Pour ajouter une option à un groupe d'options à l'aide de l'API Amazon RDS, appelez l'opération ModifyOptionGroup avec l'option que vous souhaitez ajouter. Pour activer immédiatement la nouvelle option sur toutes les instances de base de données associées, incluez le paramètre `ApplyImmediately` et affectez-lui la valeur `true`. Par défaut, l'option est activée pour chaque instance de base de données associée pendant sa fenêtre de maintenance suivante. Incluez le paramètre requis suivant :

- `OptionGroupName`

Liste des options et des paramètres d'options pour un groupe d'options

Vous pouvez répertorier toutes les options et tous les paramètres d'options pour un groupe d'options.

Console

Vous pouvez utiliser la AWS Management Console pour répertorier toutes les options et tous les paramètres d'options pour un groupe d'options.

Pour répertorier les options et les paramètres d'options pour un groupe d'options

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Groupes d'options.
3. Sélectionnez le nom du groupe d'options pour afficher ses informations détaillées. Les options et les paramètres d'options du groupe d'options sont affichés.

AWS CLI

Pour répertorier les options et les paramètres d'options pour un groupe d'options, utilisez la commande `describe-option-groups` de l'AWS CLI. Spécifiez le nom du groupe d'options dont vous souhaitez afficher les options et les paramètres. Si vous ne spécifiez pas un nom de groupe d'options, tous les groupes d'options sont décrits.

Example

L'exemple suivant répertorie les options et les paramètres d'options pour tous les groupes d'options.

```
aws rds describe-option-groups
```

Example

L'exemple suivant répertorie les options et les paramètres d'options pour un groupe d'options nommé `testoptiongroup`.

```
aws rds describe-option-groups --option-group-name testoptiongroup
```

API RDS

Pour répertorier les options et les paramètres d'options pour un groupe d'options, utilisez l'opération d'API Amazon RDS `DescribeOptionGroups`. Spécifiez le nom du groupe d'options dont vous souhaitez afficher les options et les paramètres. Si vous ne spécifiez pas un nom de groupe d'options, tous les groupes d'options sont décrits.

Modification d'un paramètre d'option

Après que vous avez ajouté une option dont les paramètres d'options sont modifiables, vous pouvez modifier les paramètres à tout moment. Si vous modifiez des options ou des paramètres d'options dans un groupe d'options, ces modifications sont appliquées à toutes les instances DB qui sont associées à ce groupe d'options. Pour plus d'informations sur les paramètres disponibles pour les différentes options, consultez la documentation de votre moteur spécifique répertoriée à l'adresse Utilisation de groupes d'options (p. 209).

Les modifications apportées au groupe d'options doivent être appliquées immédiatement dans deux cas :

- Lorsque vous ajoutez une option qui ajoute ou met à jour une valeur de port, telle que l'option `OEM`.
- Lorsque vous ajoutez ou supprimez un groupe d'options avec une option qui inclut une valeur de port.

Dans ces cas, choisissez l'option Appliquer immédiatement dans la console. Vous pouvez aussi inclure l'option `--apply-immediately` si vous utilisez l'AWS CLI ou définir le paramètre `ApplyImmediately` sur `true` si vous utilisez l'API RDS. Les options qui n'incluent pas de valeur de port peuvent être appliquées immédiatement ou pendant la fenêtre de maintenance suivant pour l'instance de base de données.

> **Note**
>
> Si vous spécifiez un groupe de sécurité comme valeur d'une option dans un groupe d'options, vous gérez le groupe de sécurité en modifiant le groupe d'options. Vous ne pouvez pas modifier ou supprimer ce groupe de sécurité en modifiant une instance de base de données. En outre, le groupe de sécurité n'apparaît pas dans les détails de l'instance de base de données dans l'AWS Management Console ou dans la sortie de la commande de l'AWS CLI `describe-db-instances`.

Console

Vous pouvez utiliser la AWS Management Console pour modifier un paramètre d'option.

Pour modifier un paramètre d'option à l'aide de la console

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes d'options.
3. Sélectionnez le groupe d'options que vous souhaitez modifier, et choisissez Modify option (Modifier une option).
4. Dans la fenêtre Modify option (Modifier une option), dans la zone Options installées, choisissez l'option dont vous souhaitez modifier le paramètre. Apportez les modifications que vous souhaitez.
5. Pour activer l'option dès que vous l'ajoutez, pour Apply Immediately (Appliquer immédiatement), choisissez Oui. Si vous choisissez Non (valeur par défaut), l'option est activée pour chaque instance de base de données associée pendant sa fenêtre de maintenance suivante.
6. Lorsque les paramètres vous conviennent, choisissez Modify Option (Modifier l'option).

AWS CLI

Pour modifier un paramètre d'options, utilisez la commande `add-option-to-option-group` de l'AWS CLI. Par défaut, l'option est activée pour chaque instance de base de données associée pendant sa fenêtre de maintenance suivante. Pour appliquer la modification immédiatement à toutes les instances de base de données associées, incluez le paramètre `--apply-immediately`. Pour modifier un paramètre d'option, utilisez l'argument `--settings`.

Example

L'exemple suivant modifie le port que l'Oracle Enterprise Manager Database Control (OEM) utilise dans un groupe d'options nommé `testoptiongroup` et applique immédiatement la modification.

Pour Linux, macOS ou Unix :

```
aws rds add-option-to-option-group \
```

```
 --option-group-name testoptiongroup \
 --options OptionName=OEM,Port=5432,DBSecurityGroupMemberships=default \
 --apply-immediately
```

Pour Windows :

```
aws rds add-option-to-option-group ^
 --option-group-name testoptiongroup ^
 --options OptionName=OEM,Port=5432,DBSecurityGroupMemberships=default ^
 --apply-immediately
```

Le résultat de la commande est similaire à ce qui suit :

```
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

L'exemple suivant modifie l'option Oracle NATIVE_NETWORK_ENCRYPTION à un groupe d'options et change les paramètres d'options.

Pour Linux, macOS ou 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_NET
 \
--apply-immediately
```

Pour 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
```

Le résultat de la commande est similaire à ce qui suit :

```
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
```

API RDS

Pour modifier un paramètre d'options, utilisez la commande `ModifyOptionGroup` de l'API Amazon RDS. Par défaut, l'option est activée pour chaque instance de base de données associée pendant sa fenêtre de maintenance suivante. Pour appliquer la modification immédiatement à toutes les instances de base de données associées, incluez le paramètre `ApplyImmediately` et affectez-lui la valeur `true`.

Suppression d'une option d'un groupe d'options

Certaines options peuvent être supprimées d'un groupe d'options, et certaines ne le peuvent pas. Il n'est pas possible de supprimer une option persistante d'un groupe d'options tant que l'ensemble des instances de base de données associées à ce groupe d'options est dissocié. Une option permanente ne peut jamais être supprimée d'un groupe d'options. Pour plus d'informations sur les options pouvant être supprimées, consultez la documentation pour votre moteur spécifique répertoriée à l'adresse Utilisation de groupes d'options (p. 209).

Si vous supprimez tous les éléments d'un groupe d'options, Amazon RDS ne supprime pas ce groupe. Les instances de base de données qui sont associées au groupe d'options vide continuent de l'être. Elles ne comportent simplement plus aucune option active. Pour supprimer toutes les options d'une instance de base de données simultanément, vous pouvez aussi associer l'instance de base de données au groupe d'options par défaut (vide).

Console

Vous pouvez utiliser la AWS Management Console pour supprimer une option d'un groupe d'options.

Pour supprimer une option à partir d'un groupe d'options à l'aide de la console

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes d'options.
3. Sélectionnez le groupe d'options que vous souhaitez supprimer, et choisissez Delete option (Supprimer l'option).
4. Dans la fenêtre Delete option (Supprimer l'option), procédez comme suit :
   - Cochez la case correspondant à l'option à supprimer.
   - Pour que la suppression entre en vigueur dès que vous l'effectuez, pour Apply immediately (Appliquer immédiatement), choisissez Oui. Si vous choisissez Non (valeur par défaut), l'option est supprimée pour chaque instance de base de données associée pendant sa fenêtre de maintenance suivante.

5. Lorsque les paramètres vous conviennent, choisissez Yes, Delete (Oui, supprimer).

AWS CLI

Pour supprimer une option d'un groupe d'options, utilisez la commande `remove-option-from-option-group` de l'AWS CLI. Par défaut, l'option est supprimée de chaque instance de base de données associée pendant sa fenêtre de maintenance suivante. Pour appliquer immédiatement la modification, incluez le paramètre `--apply-immediately`.

Example

L'exemple suivant supprime l'option Oracle Enterprise Manager Database Control (OEM) d'un groupe d'options nommé `testoptiongroup` et applique immédiatement la modification.

Pour Linux, macOS ou Unix :

```
aws rds remove-option-from-option-group \
    --option-group-name testoptiongroup \
    --options OEM \
    --apply-immediately
```

Pour Windows :

```
aws rds remove-option-from-option-group ^
    --option-group-name testoptiongroup ^
    --options OEM ^
    --apply-immediately
```

Le résultat de la commande est similaire à ce qui suit :

```
OPTIONGROUP    testoptiongroup oracle-ee   12.1    Test option group
```

API RDS

Pour supprimer une option d'un groupe d'options, utilisez l'action `ModifyOptionGroup` d'API Amazon RDS. Par défaut, l'option est supprimée de chaque instance de base de données associée pendant sa fenêtre de maintenance suivante. Pour appliquer la modification immédiatement, incluez le paramètre `ApplyImmediately` et affectez-lui la valeur `true`.

Incluez les paramètres suivants :

- `OptionGroupName`
- `OptionsToRemove.OptionName`

Suppression d'un groupe d'options

Vous pouvez supprimer un groupe d'options qui n'est pas associé à une ressource Amazon RDS. Un groupe d'options peut être associé à une instance de base de données, un instantané de base de données manuel ou un instantané de base de données automatique.

Si vous tentez de supprimer un groupe d'options associé à une ressource Amazon RDS, une erreur similaire à la suivante est renvoyée.

```
An error occurred (InvalidOptionGroupStateFault) when calling the DeleteOptionGroup
 operation: The option group 'optionGroupName' cannot be deleted because it is in use.
```

Pour rechercher les ressources Amazon RDS associées à un groupe d'options

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Groupes d'options.
3. Sélectionnez le nom du groupe d'options pour afficher ses informations détaillées.
4. Cochez la section Instances et instantanés associés pour les ressources Amazon RDS associées.

Si une instance de base de données est associée au groupe d'options, modifiez-la afin qu'elle utilise un autre groupe d'options. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Si un instantané de base de données manuel est associé au groupe d'options, modifiez-le afin qu'il utilise un autre groupe d'options à l'aide de la commande `modify-db-snapshot` de l'AWS CLI.

> Note
>
> Vous ne pouvez pas modifier le groupe d'options d'un instantané de base de données automatique.

Console

Une manière de créer un groupe d'options consiste à utiliser l'AWS Management Console.

Pour supprimer un groupe d'options à l'aide de la console

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.

2. Dans le panneau de navigation, choisissez Groupes d'options.
3. Choisissez le groupe d'options.
4. Choisissez Supprimer un groupe.
5. Dans la page de confirmation, choisissez Supprimer pour terminer la suppression du groupe d'options ou Annuler pour annuler la suppression.

AWS CLI

Pour supprimer un groupe d'options, utilisez la commande `delete-option-group` de l'AWS CLI avec le paramètre obligatoire suivant.

- `--option-group-name`

Example

L'exemple suivant supprime un groupe d'options nommé `testoptiongroup`.

Pour Linux, macOS ou Unix :

```
aws rds delete-option-group \
    --option-group-name testoptiongroup
```

Pour Windows :

```
aws rds delete-option-group ^
    --option-group-name testoptiongroup
```

API RDS

Pour supprimer un groupe d'options, appelez l'opération d'API Amazon RDS `DeleteOptionGroup`. Incluez le paramètre suivant :

- `OptionGroupName`

Utilisation de groupes de paramètres de base de données

Vous pouvez gérer la configuration de votre moteur de base de données en associant vos instances de base de données à l'aide de groupes de paramètres. Amazon RDS définit les groupes de paramètres à l'aide de paramètres par défaut qui s'appliquent aux instances de bases de données nouvellement créés.

> **Important**
>
> Vous pouvez définir vos propres groupes de paramètres à l'aide de paramètres personnalisés. Vous pouvez ensuite modifier vos instances de bases de données afin d'utiliser vos propres groupes de paramètres.

Pour plus d'informations sur la modification d'une instance de base de données , consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Un groupe de paramètres de base de données sert de conteneur pour les valeurs de configuration du moteur qui sont appliquées à une ou plusieurs instances de base de données. Les

Si vous créez une instance de base de données sans spécifier de groupe de paramètres de base de données, l'instance de base de données utilise un groupe de paramètres de base de données par défaut. Chaque groupe de paramètres de base de données par défaut contient des valeurs par défaut du moteur de base de données, ainsi que celles du système Amazon RDS en fonction du moteur, de la classe de calcul et de l'espace de stockage alloué de l'instance. Vous ne pouvez pas modifier les valeurs de paramètre d'un groupe de paramètres de base de données par défaut. Vous pouvez par contre créer votre propre groupe de paramètres et choisir les valeurs de chaque paramètre. Il n'est pas possible de modifier tous les paramètres de moteur de base de données dans un groupe de paramètres créé.

Si vous souhaitez utiliser votre propre groupe de paramètres, vous devez créer un nouveau groupe de paramètres et modifier les paramètres en fonction de vos souhaits. Vous modifiez ensuite votre instance de base de données afin d'utiliser le nouveau groupe de paramètres. Si vous mettez à jour les paramètres d'un groupe de paramètres de base de données, les modifications effectuées s'appliquent à toutes les instances de base de données qui sont associées à ce groupe de paramètres.

Vous pouvez également copier un groupe de paramètres de base de données existant avec la commande copy-db-parameter-group de l'AWS CLI. La copie d'un groupe de paramètres peut être utile lorsque vous souhaitez inclure la plupart des paramètres et valeurs personnalisés d'un groupe de paramètres de base de données existant dans un nouveau groupe de paramètres de base de données.

Voici quelques éléments importants concernant l'utilisation de paramètres dans un groupe de paramètres de base de données :

- Lorsque vous modifiez un paramètre dynamique et que vous enregistrez le groupe de paramètres de base de données, la modification est appliquée immédiatement, quel que soit le paramètre Appliquer immédiatement. Lorsque vous modifiez un paramètre statique et que vous enregistrez le groupe de paramètres de base de données, la modification du paramètre est appliquée une fois que vous avez redémarré manuellement l'instance de base de données. Vous pouvez réinitialiser une instance de base de données en utilisant la console RDS ou en appelant explicitement l'opération d'API `RebootDbInstance` (sans basculement, si l'instance de base de données se trouve dans un déploiement Multi-AZ). Les critères pour redémarrer l'instance de base de données associée après un changement de paramètre statique contribuent à atténuer le risque d'erreur de configuration d'un paramètre affectant un appel d'API, comme appeler `ModifyDBInstance` pour modifier la classe d'instance de base de données ou le stockage évolutif.

  Si une instance de base de données n'utilise pas les dernières modifications apportées à son groupe de paramètres de base de données associé, AWS Management Console affiche le groupe de paramètres de base de données avec le statut suivant : pending-reboot. Le statut de groupe de paramètres pending-reboot n’entraîne pas de redémarrage automatique lors de la fenêtre de maintenance suivante. Pour appliquer les modifications de paramètre les plus récentes apportées à cette instance de base de données, vous devez la redémarrer manuellement.
- Lorsque vous modifiez le groupe de paramètres de base de données associé à une instance de base de données, vous devez redémarrer manuellement l'instance avant que le nouveau groupe de paramètres de base de données puisse être utilisé par l'instance de base de données. Pour de plus amples informations sur la modification du groupe de paramètres de base de données, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).
- Vous pouvez spécifier la valeur d'un paramètre de base de données sous la forme d'un entier ou d'une expression d'entiers créée à partir de formules, de variables, de fonctions et d'opérateurs. Les fonctions peuvent inclure une expression de journal mathématique. Pour plus d'informations, consultez Valeurs de paramètres de bases de données (p. 235).
- Définissez les paramètres qui concernent le jeu de caractères ou le classement de votre base de données dans votre groupe de paramètres avant de créer l'instance de base de données et avant de

créer une base de données dans votre instance de base de données. Cela garantit que la base de données par défaut et les nouvelles bases de données dans votre instance de base de données utilisent les valeurs de jeu de caractères et de classement que vous spécifiez. Si vous modifiez les paramètres de jeu de caractères ou de classement pour votre instance de base de données, les modifications de paramètre ne sont pas appliquées aux bases de données existantes.

Vous pouvez modifier les valeurs de jeu de caractères ou de classement pour une base de données existante à l'aide de la commande `ALTER DATABASE`, par exemple :

```
ALTER DATABASE database_name CHARACTER SET character_set_name COLLATE collation;
```

- La configuration incorrecte de paramètres dans un groupe de paramètres DB peut avoir des effets contraires involontaires, dont une dégradation de la performance et une instabilité du système. Montrez-vous toujours prudent lorsque vous modifiez des paramètres de base de données et sauvegardez vos données avant de modifier un groupe de paramètres de base de données. Testez les modifications des valeurs d'un groupe de paramètres sur une instance de base de données de test avant d'appliquer ces modifications à une instance de base de données de production.
- Pour déterminer les paramètres pris en charge par votre moteur de base de données, vous pouvez afficher les paramètres dans le groupe de paramètres de base de données utilisé par l'instance de base de données. Pour plus d'informations, consultez Affichage des valeurs de paramètres pour un groupe de paramètres de bases de données (p. 234).

Rubriques

- Création d'un groupe de paramètres de bases de données (p. 227)
- Modification de paramètres dans un groupe de paramètres de bases de données (p. 229)
- Copie d'un groupe de paramètres de bases de données (p. 231)
- Liste des groupes de paramètres de bases de données (p. 233)
- Affichage des valeurs de paramètres pour un groupe de paramètres de bases de données (p. 234)
- Comparaison des groupes de paramètres de bases de données (p. 235)
- Valeurs de paramètres de bases de données (p. 235)

Création d'un groupe de paramètres de bases de données

Vous pouvez créer un groupe de paramètres de base de données à l'aide de la AWS Management Console, de l'AWS CLI ou de l'API RDS.

Console

Pour créer un groupe de paramètres de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes de paramètres.
3. Choisissez Créer un groupe de paramètres.

   La fenêtre Créer un groupe de paramètres s'affiche.
4. Dans la liste Famille de groupe de paramètres, sélectionnez une famille de groupe de paramètres de base de données.
5. Dans la liste Type, sélectionnez Groupe de paramètres de base de données.

6. Dans la zone Nom du groupe, entrez le nom du nouveau groupe de paramètres de base de données.
7. Dans la zone Description, entrez une description pour le nouveau groupe de paramètres de base de données.
8. Sélectionnez Create.

AWS CLI

Pour créer un groupe de paramètres de base de données, utilisez la commande `create-db-parameter-group` de l'AWS CLI. L'exemple suivant crée un groupe de paramètres de base de données nommé mydbparametergroup pour MySQL version 5.6 avec une description de « My new parameter group (Mon nouveau groupe de paramètres) ».

Incluez les paramètres requis suivants :

- `--db-parameter-group-name`
- `--db-parameter-group-family`
- `--description`

Pour répertorier toutes les familles de groupes de paramètres, utilisez la commande suivante :

```
aws rds describe-db-engine-versions --query "DBEngineVersions[].DBParameterGroupFamily"
```

> **Note**
>
> La sortie contient des doublons.

Example

Pour Linux, macOS ou Unix :

```
aws rds create-db-parameter-group \
    --db-parameter-group-name mydbparametergroup \
    --db-parameter-group-family MySQL5.6 \
    --description "My new parameter group"
```

Pour Windows :

```
aws rds create-db-parameter-group ^
    --db-parameter-group-name mydbparametergroup ^
    --db-parameter-group-family MySQL5.6 ^
    --description "My new parameter group"
```

Le résultat produit lors de l'exécution de cette commande est semblable à ce qui suit :

```
DBPARAMETERGROUP  mydbparametergroup  mysql5.6  My new parameter group
```

API RDS

Pour créer un groupe de paramètres de base de données, utilisez l'opération d'API RDS `CreateDBParameterGroup`.

Incluez les paramètres requis suivants :

- `DBParameterGroupName`
- `DBParameterGroupFamily`
- `Description`

Modification de paramètres dans un groupe de paramètres de bases de données

Vous pouvez modifier des valeurs de paramètres dans un groupe de paramètres de base de données créé par le client. Par contre, vous ne pouvez pas modifier les valeurs de paramètres dans un groupe de paramètres de base de données par défaut. Les modifications apportées à des paramètres dans un groupe de paramètres DB créé par le client sont appliquées à toutes les instances de base de données qui sont associées au groupe de paramètres DB.

Les modifications apportées à certains paramètres sont appliquées immédiatement à l'instance de base de données sans redémarrage. Les modifications apportées à d'autres paramètres s'appliquent uniquement après le redémarrage de l'instance de base de données. La console RDS affiche le statut du groupe de paramètres de base de données associé à une instance de base de données dans l'onglet Configuration. Par exemple, si l'instance de base de données n'utilise pas les dernières modifications apportées à son groupe de paramètres de base de données associé, la console RDS affiche le groupe de paramètres de base de données avec le statut suivant : pending-reboot. Pour appliquer les modifications de paramètre les plus récentes apportées à cette instance de base de données, vous devez la redémarrer manuellement.

Console

Pour modifier un groupe de paramètres DB

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes de paramètres.
3. Dans la liste, sélectionnez le groupe de paramètres que vous souhaitez modifier.
4. Sous Parameter group actions (Actions de groupe de paramètres), choisissez Edit (Modifier).
5. Modifiez les valeurs des paramètres que vous souhaitez remplacer. Vous pouvez parcourir les paramètres en utilisant les touches fléchées en haut à droite de la boîte de dialogue.

   Vous ne pouvez pas modifier les valeurs dans un groupe de paramètres par défaut.
6. Sélectionnez Save Changes.

AWS CLI

Pour modifier un groupe de paramètres de base de données, utilisez la commande `modify-db-parameter-group` de l'AWS CLI avec les paramètres requis suivants :

- `--db-parameter-group-name`
- `--parameters`

L'exemple suivant modifie les valeurs `max_connections` et `max_allowed_packet` dans le groupe de paramètres de base de données nommé mydbparametergroup.

Example

Pour Linux, macOS ou 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"
```

Pour 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"
```

La commande produit un résultat similaire à ce qui suit :

```
DBPARAMETERGROUP  mydbparametergroup
```

API RDS

Pour modifier un groupe de paramètres de base de données, utilisez la commande d'API RDS `ModifyDBParameterGroup` avec les paramètres requis suivants :

- `DBParameterGroupName`
- `Parameters`

Copie d'un groupe de paramètres de bases de données

Vous pouvez copier des groupes de paramètres DB personnalisés que vous créez. La copie d'un groupe de paramètres est une solution pratique lorsque vous avez déjà créé un groupe de paramètres DB et que vous souhaitez inclure la plupart des valeurs et des paramètres personnalisés de ce groupe dans un nouveau groupe de paramètres DB. Vous pouvez copier un groupe de paramètres de base de données en utilisant la AWS Management Console, la commande AWS CLI copy-db-parameter-group ou l'opération d'API RDS CopyDBParameterGroup.

Après avoir copié un groupe de paramètres de base de données, patientez au moins 5 minutes avant de créer votre première instance de base de données utilisant ce groupe comme groupe de paramètres

par défaut. Cela permet à Amazon RDS de terminer complètement l'action de copie avant l'utilisation du groupe de paramètres. Cela est particulièrement important pour les paramètres qui sont essentiels lors de la création de la base de données par défaut d'une instance de base de données. Parmi ces paramètres, citons par exemple le jeu de caractères de la base de données par défaut défini par le paramètre `character_set_database`. Utilisez l'option Groupe de paramètres de la console Amazon RDS ou la commande describe-db-parameters pour vérifier que votre groupe de paramètres de base de données a été créé.

> **Note**
>
> Vous ne pouvez pas copier un groupe de paramètres par défaut. Toutefois, vous pouvez créer un nouveau groupe de paramètres basé sur un groupe de paramètres par défaut.
> Actuellement, vous ne pouvez pas copier de groupe de paramètres dans une autre région AWS.

Console

Pour copier un groupe de paramètres DB

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes de paramètres.
3. Dans la liste, choisissez le groupe de paramètres personnalisé que vous souhaitez copier.
4. Sous Parameter group actions (Actions de groupe de paramètres), choisissez Copy (Copier).
5. Dans New DB parameter group identifier (Nouvel identifiant de groupe de paramètres de base de données), saisissez un nom pour le nouveau groupe de paramètres.
6. Dans Description, saisissez une description pour le nouveau groupe de paramètres.
7. Choisissez Copy.

AWS CLI

Pour copier un groupe de paramètres de base de données, utilisez la commande `copy-db-parameter-group` de l'AWS CLI avec les options requises suivantes :

- `--source-db-parameter-group-identifier`
- `--target-db-parameter-group-identifier`
- `--target-db-parameter-group-description`

L'exemple suivant crée un groupe de paramètres DB nommé `mygroup2` qui est une copie du groupe de paramètres DB `mygroup1`.

Example

Pour Linux, macOS ou 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"
```

Pour 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"
```

API RDS

Pour copier un groupe de paramètres de base de données, utilisez l'opération d'API RDS `CopyDBParameterGroup` avec les paramètres requis suivants :

- `SourceDBParameterGroupIdentifier`
- `TargetDBParameterGroupIdentifier`
- `TargetDBParameterGroupDescription`

Liste des groupes de paramètres de bases de données

Vous pouvez répertorier les groupes de paramètres DB que vous avez créées pour votre compte AWS.

> **Note**
>
> Les groupes de paramètres par défaut sont automatiquement créés à partir d'un modèle de paramètre par défaut lorsque vous créez une instance de base de données pour une version et un moteur de base de données spécifiques. Ces groupes de paramètres par défaut contiennent des valeurs de paramètres préférentielles et ne peuvent pas être modifiés. Lorsque vous créez un groupe de paramètres personnalisé, vous pouvez modifier les réglages des paramètres.

Console

Pour répertorier tous les groupes de paramètres DB pour un compte AWS

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes de paramètres.

   Les groupes de paramètres DB s'affichent dans une liste.

AWS CLI

Pour répertorier tous les groupes de paramètres de base de données pour un compte AWS, utilisez la commande `describe-db-parameter-groups` de l'AWS CLI.

Example

L'exemple suivant répertorie tous les groupes de paramètres DB disponibles pour un compte AWS.

```
aws rds describe-db-parameter-groups
```

La commande renvoie une réponse telle que la suivante :

```
DBPARAMETERGROUP  default.mysql5.5     mysql5.5  Default parameter group for MySQL5.5
DBPARAMETERGROUP  default.mysql5.6     mysql5.6  Default parameter group for MySQL5.6
DBPARAMETERGROUP  mydbparametergroup   mysql5.6  My new parameter group
```

L'exemple suivant décrit le groupe de paramètres mydbparamgroup1.

Pour Linux, macOS ou Unix :

```
aws rds describe-db-parameter-groups \
    --db-parameter-group-name mydbparamgroup1
```

Pour Windows :

```
aws rds describe-db-parameter-groups ^
    --db-parameter-group-name mydbparamgroup1
```

La commande renvoie une réponse telle que la suivante :

```
DBPARAMETERGROUP  mydbparametergroup1  mysql5.5  My new parameter group
```

API RDS

Pour répertorier tous les groupes de paramètres de base de données pour un compte AWS, utilisez l'opération d'API RDS `DescribeDBParameterGroups`.

Affichage des valeurs de paramètres pour un groupe de paramètres de bases de données

Vous pouvez obtenir une liste de tous les paramètres dans un groupe de paramètres DB et de leurs valeurs.

Console

Pour afficher les valeurs de paramètres pour un groupe de paramètres DB

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes de paramètres.

   Les groupes de paramètres DB s'affichent dans une liste.
3. Choisissez le nom du groupe de paramètres pour consulter la liste des paramètres associée.

AWS CLI

Pour afficher les valeurs de paramètre d'un groupe de paramètres de base de données, utilisez la commande `describe-db-parameters` de l'AWS CLI avec le paramètre requis suivant.

- `--db-parameter-group-name`

Example

L'exemple suivant répertorie les paramètres et les valeurs de paramètres pour un groupe de paramètres de base de données nommé mydbparametergroup.

```
aws rds describe-db-parameters --db-parameter-group-name mydbparametergroup
```

La commande renvoie une réponse telle que la suivante :

```
DBPARAMETER  Parameter Name            Parameter Value  Source           Data Type  Apply
 Type  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
     true
DBPARAMETER  socket                    /tmp/mysql.sock  system           string     static
     false
```

API RDS

Pour afficher les valeurs de paramètre d'un groupe de paramètres de base de données, utilisez la commande d'API RDS `DescribeDBParameters` avec le paramètre requis suivant :

- `DBParameterGroupName`

Comparaison des groupes de paramètres de bases de données

Vous pouvez utiliser l'AWS Management Console afin d'examiner les différences entre les groupes de paramètres pour le même moteur et la même version de base de données.

Pour comparer deux groupes de paramètres de bases de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes de paramètres.
3. Dans la liste, choisissez les deux groupes de paramètres que vous souhaitez comparer.
4. Sous Parameter group actions (Actions de groupe de paramètres), choisissez Compare (Comparer).

   Note

   Si les éléments que vous avez sélectionnés ne sont pas équivalents, vous ne pouvez pas choisir Compare (Comparer). Par exemple, vous ne pouvez pas comparer un groupe de paramètres MySQL 5.6 et MySQL 5.7. Vous ne pouvez pas comparer un groupe de paramètres de base de données et un groupe de paramètres de cluster de bases de données Aurora.

Valeurs de paramètres de bases de données

Vous pouvez spécifier la valeur d'un paramètre de base de données sous l'une des formes suivantes :

- Une constante entière
- Une formule de paramètre DB
- Une fonction de paramètre DB
- Une constante de chaîne de caractères
- Une expression de journal (la fonction log correspond à la fonction logarithmique de base 2), telle que `value={log(DBInstanceClassMemory/8187281418)*1000}`

Des formules de paramètre de bases de données

Une formule de paramètre DB est une expression qui se réduit en une valeur entière ou booléenne et qui se trouve entre crochets : {}. Vous pouvez spécifier des formules soit pour une valeur de paramètre de base de données, soit en tant qu'argument pour une fonction de paramètre de base de données.

Syntaxe

```
{FormulaVariable}
{FormulaVariable*Integer}
{FormulaVariable*Integer/Integer}
{FormulaVariable/Integer}
```

Variables de formule de paramètre de bases de données

Chaque variable de formule renvoie une valeur entière ou booléenne. Les noms des variables sont sensibles à la casse.

AllocatedStorage

Renvoie la taille, en octets, du volume de données.

DBInstanceClassMemory

Renvoie le nombre d'octets de mémoire allouée à la classe d'instance de base de données associée à l'instance de base de données actuelle, moins la mémoire utilisée par les processus Amazon RDS qui gèrent l'instance.

EndPointPort

Renvoie le nombre de ports utilisés lors de la connexion à l'instance de base de données.

DBInstanceClassHugePagesDefault

Renvoie une valeur booléenne. Actuellement, cette variable est uniquement prise en charge pour les moteurs Oracle.

Pour plus d'informations, consultez Utilisation de HugePages avec une instance de base de données Oracle (p. 954).

Opérateurs de formule de paramètre de bases de données

Les formules de paramètre DB prennent en charge deux opérateurs : division et multiplication.

Opérateur de division : /

Divise le dividende par le diviseur, en renvoyant un quotient entier. Les décimales dans le quotient sont tronquées, pas arrondies.

Syntaxe

```
dividend / divisor
```

Les arguments de dividende et de diviseur doivent être des expressions entières.

Opérateur de multiplication : *

Multiplie les expressions, affichant ainsi le résultat des expressions. Les décimales dans les expressions sont tronquées, pas arrondies.

Syntaxe

```
expression * expression
```

Les deux expressions doivent être des entiers.

Fonctions de paramètre de bases de données

Les arguments de paramètre peuvent être spécifiés soit comme entiers, soit comme formules. Chaque fonction doit avoir au moins un argument. Plusieurs arguments peuvent être spécifiés comme une liste séparée par des virgules. Cette liste ne peut pas contenir de membres vides, tels que argument1,,argument3. Les noms de fonctions ne sont pas sensibles à la casse.

Note

Actuellement, les fonctions de paramètre de base de données ne sont pas prises en charge dans l'AWS CLI.

IF()

Renvoie un argument.

Actuellement, cette variable est uniquement prise en charge pour les moteurs Oracle et le seul premier argument pris en charge est `{DBInstanceClassHugePagesDefault}`. Pour plus d'informations, consultez Utilisation de HugePages avec une instance de base de données Oracle (p. 954).

Syntaxe

```
IF(argument1, argument2, argument3)
```

Renvoie le deuxième argument si le premier a la valeur true. Sinon, renvoie le troisième argument.

GREATEST()

Renvoie la plus grande valeur depuis une liste d'entiers ou de formules de paramètres.

Syntaxe

```
GREATEST(argument1, argument2,...argumentn)
```

Renvoie un entier.

LEAST()

Renvoie la plus petite valeur depuis une liste d'entiers ou de formules de paramètres.

Syntaxe

```
LEAST(argument1, argument2,...argumentn)
```

Renvoie un entier.

SUM()

Ajoute les valeurs des formules de paramètres ou d'entiers spécifiés.

Syntaxe

```
SUM(argument1, argument2,...argumentn)
```

Renvoie un entier.

Exemples de valeurs de paramètre de bases de données

Ces exemples s'affichent en utilisant des formules et des fonctions dans les valeurs pour des paramètres DB.

> **Warning**
>
> La configuration incorrecte de paramètres dans un groupe de paramètres DB peut avoir des effets contraires involontaires, dont une dégradation de la performance et une instabilité du système. Montrez-vous toujours prudent lorsque vous modifiez des paramètres de base de données et sauvegardez vos données avant de modifier votre groupe de paramètres DB. Testez les modifications d'un groupe de paramètres sur des instances de base de données de test, créées en utilisant des restaurations à un moment donné, avant d'appliquer ces modifications à vos instances de base de données de production.

Vous pouvez spécifier la fonction `GREATEST` dans un paramètre de processus Oracle pour définir le nombre de processus utilisateur pour la valeur la plus grande, entre 80 ou `DBInstanceClassMemory`, divisée par 9 868 951.

```
GREATEST({DBInstanceClassMemory/9868951},80)
```

Vous pouvez spécifier la fonction `LEAST()` dans une valeur de paramètre `max_binlog_cache_size` MySQL pour définir la taille de cache maximum qu'une transaction peut utiliser dans une instance MySQL, correspondant au plus petit de 1 Mo ou `DBInstanceClass`/256.

```
LEAST({DBInstanceClassMemory/256},10485760)
```

Gestion d'une instance de base de données Amazon RDS

Vous trouverez ci-dessous des instructions pour la gestion et la maintenance de votre instance de base de données Amazon RDS.

Rubriques

- Arrêt temporaire d'une instance de bases de données Amazon RDS (p. 239)
- Démarrage d'une instance de bases de données Amazon RDS précédemment arrêtée (p. 242)
- Modification d'une instance de base de données Amazon RDS (p. 243)
- Entretien d'une instance de base de données (p. 260)
- Mise à niveau d'une version du moteur d'une instance de base de données (p. 267)
- Affectation d'un nouveau nom à une instance DB (p. 270)
- Redémarrage d'une instance de base de données (p. 272)
- Utilisation des réplicas en lecture (p. 275)
- Balisage de ressources Amazon RDS (p. 293)
- Utilisation des Amazon Resource Names (ARN) dans Amazon RDS (p. 298)
- Utilisation du stockage pour les instances de base de données Amazon RDS (p. 304)
- Suppression d'une instance de base de données (p. 313)

Arrêt temporaire d'une instance de bases de données Amazon RDS

Si vous utilisez une instance de bases de données de façon intermittente pour des tests temporaires ou pour une activité de développement quotidienne, vous pouvez arrêter votre instance de bases de données Amazon RDS temporairement pour faire des économies. Lorsque votre instance de bases de données est arrêtée, vous payez le stockage provisionné (y compris les IOPS provisionnées) et le stockage de sauvegarde (y compris les instantanés et les sauvegardes automatiques dans votre fenêtre de conservation spécifiée), mais pas pour les heures d'instance de bases de données. Pour de plus amples informations, veuillez consulter FAQ sur la facturation.

> Note
>
> Dans certains cas, l'arrêt d'une instance de base de données peut prendre du temps. Si vous souhaitez arrêter votre instance de base de données et la redémarrer immédiatement, vous pouvez réamorcer l'instance de base de données. Pour de plus amples informations sur le redémarrage d'une instance de base de données, veuillez consulter Redémarrage d'une instance de base de données (p. 272).

Vous pouvez arrêter et démarrer des instances de base de données exécutant les moteurs suivants :

- MariaDB
- Microsoft SQL Server
- MySQL
- Oracle

- PostgreSQL

L'arrêt et le démarrage d'une instance de bases de données sont pris en charge pour tous les classes d'instance de bases de données et dans toutes les régions AWS.

Vous pouvez arrêter et démarrer une instance de base de données qu'elle soit configurée pour une zone de disponibilité unique ou pour plusieurs, pour des moteurs de base de données qui prennent en charge les déploiements multi-AZ. Vous ne pouvez pas arrêter une instance de bases de données Amazon RDS pour SQL Server dans une configuration multi-AZ.

> **Note**
>
> Pour un déploiement multi-AZ, l'arrêt d'une instance de base de données peut prendre du temps. Si vous disposez d'au moins une sauvegarde après un basculement précédent, vous pouvez accélérer l'arrêt de l'instance de base de données en effectuant un redémarrage avec basculement avant d'arrêter l'instance de base de données.

Lorsque vous arrêtez une instance de bases de données, celle-ci effectue un arrêt normal et cesse de s'exécuter. L'état de l'instance de bases de données devient `stopping`, puis `stopped`. Tous les volumes de stockage restent attachés à l'instance de bases de données et leurs données sont conservées. Toutes les données stockées dans la RAM de l'instance de base de données sont supprimées.

L'arrêt d'une instance de base de données supprime les actions en attente, à l'exception de celles pour le groupe d'options de l'instance de base de données ou le groupe de paramètres de base de données.

> **Important**
>
> Vous pouvez arrêter une instance de bases de données pour une période pouvant s'étendre à sept jours. Si vous ne démarrez pas manuellement votre instance de base de données après sept jours, votre instance de base de données est automatiquement lancée afin qu'elle ne prenne pas de retard sur les mises à jour de maintenance requises.

Avantages

L'arrêt et le démarrage d'une instance de bases de données est plus rapide que la création d'un instantané de base de données, et que la restauration d'un instantané.

Lorsque vous arrêtez une instance de bases de données, elle conserve ses ID, point de terminaison DNS (Domain Name Server), groupe de paramètres, groupe de sécurité et groupe d'options. Lorsque vous démarrez une instance de bases de données, sa configuration est la même que lorsque vous l'avez arrêtée. En outre, si vous arrêtez une instance de bases de données, Amazon RDS conserve les journaux de transactions Amazon Simple Storage Service (Amazon S3) pour vous permettre d'effectuer une restauration à un moment donné, si nécessaire.

Limites

Voici quelques limitations pour l'arrêt et le démarrage de votre instance de bases de données :

- Vous ne pouvez pas arrêter une instance de base de données qui possède un réplica en lecture ou qui est un réplica en lecture.
- Vous ne pouvez pas arrêter une instance de bases de données Amazon RDS pour SQL Server dans une configuration multi-AZ.
- Vous ne pouvez pas modifier une instance de bases de données arrêtée.
- Vous ne pouvez pas supprimer un groupe d'options associé à une instance de bases de données arrêtée.
- Vous ne pouvez pas supprimer un groupe de paramètres de base de données associé à une instance de bases de données arrêtée.

Considérations relatives au groupe d'options et de paramètres

Vous ne pouvez pas supprimer les options persistantes (y compris les options permanentes) d'un groupe d'options si des instances de bases de données sont associées à ce groupe d'options. Cette fonctionnalité vaut également pour les instances de bases de données ayant l'état `stopping`, `stopped`, ou `starting`.

Vous pouvez modifier un groupe d'options ou un groupe de paramètres de base de données associé à une instance de bases de données arrêtée, mais la modification ne sera appliquée qu'au prochain démarrage de l'instance de bases de données. Si vous avez choisi d'appliquer les modifications immédiatement, elles sont appliquées au démarrage de l'instance de bases de données. Dans le cas contraire, les modifications sont appliquées au cours de la fenêtre de maintenance suivante, après le démarrage de l'instance de bases de données.

Considérations VPC

Lorsque vous arrêtez une instance de bases de données, elle conserve son point de terminaison DNS. Si vous arrêtez une instance de bases de données qui ne figure pas dans un Amazon Virtual Private Cloud (Amazon VPC), Amazon RDS libère les adresses IP de l'instance de bases de données. Si vous arrêtez une instance de bases de données qui figure dans un VPC, l'instance de bases de données conserve les adresses IP.

> Note
>
> Vous devez toujours vous connecter à une instance de bases de données à l'aide du point de terminaison DNS, et non pas de l'adresse IP.

Arrêt temporaire d'une instance de bases de données

Vous pouvez arrêter une base de données à l'aide de AWS Management Console, l'API RDS AWS CLI, ou de l'API RDS.

Console

Pour arrêter une instance de bases de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Bases de données, puis l'instance de base de données que vous voulez arrêter.
3. Pour Actions, choisissez Arrêter.
4. (Facultatif) Dans la fenêtre Arrêter l'instance de base de données, choisissez Oui pour Créer un instantané ? et saisissez le nom de l'instantané sous Nom de l'instantané. Choisissez Oui si vous souhaitez créer un instantané de l'instance de base de données avant de l'arrêter.
5. Choisissez Oui, Arrêter maintenant pour arrêter votre instance de base de données, ou choisissez Annuler pour annuler l'opération.

AWS CLI

Pour arrêter une instance de bases de données Oracle à l'aide de l'AWS CLI, appelez la commande stop-db-instance avec l'option suivante :

- `--db-instance-identifier` – le nom de l'instance de base de données.

Example

```
aws rds stop-db-instance --db-instance-identifier mydbinstance
```

API RDS

Pour arrêter une instance de bases de données à l'aide de l'API Amazon RDS, appelez l'opération StopDBInstance avec le paramètre suivant :

- `DBInstanceIdentifier` – le nom de l'instance de base de données.

Démarrage d'une instance de bases de données Amazon RDS précédemment arrêtée

Vous pouvez arrêter votre instance de bases de données Amazon RDS temporairement pour faire des économies. Une fois votre instance de bases de données arrêtée, vous pouvez la redémarrer et recommencer à l'utiliser. Pour plus d'informations sur l'arrêt et le redémarrage des instances de bases de données, consultez Arrêt temporaire d'une instance de bases de données Amazon RDS (p. 239).

Lorsque vous démarrez une instance de bases de données que vous avez précédemment arrêtée, l'instance de bases de données conserve ses ID, point de terminaison DNS (Domain Name Server), groupe de paramètres, groupe de sécurité et groupe d'options. Lorsque vous démarrez une instance arrêtée, une heure d'instance complète vous est facturée.

Console

Pour démarrer une instance de bases de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Bases de données, puis l'instance de base de données que vous voulez démarrer.
3. Pour Actions, choisissez Start (Démarrer).

AWS CLI

Pour démarrer une instance de bases de données à l'aide de l'AWS CLI, appelez la commande start-db-instance avec l'option suivante :

- `--db-instance-identifier` – le nom de l'instance de base de données.

Example

```
aws rds start-db-instance --db-instance-identifier mydbinstance
```

API RDS

Pour démarrer une instance de bases de données à l'aide de l'API Amazon RDS, appelez l'opération StartDBInstance avec les paramètres suivants :

- `DBInstanceIdentifier` – le nom de l'instance de base de données.

Example

```
https://rds.amazonaws.com/
    ?Action=StartDBInstance
    &DBInstanceIdentifier=mydbinstance
    &SignatureMethod=HmacSHA256
    &SignatureVersion=4
    &Version=2014-10-31
    &X-Amz-Algorithm=AWS4-HMAC-SHA256
    &X-Amz-Credential=AKIADQKE4SARGYLE/20131016/us-west-1/rds/aws4_request
    &X-Amz-Date=20131016T233051Z
    &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
    &X-Amz-Signature=087a8eb41cb1ab5f99e81575f23e73757ffc6a1e42d7d2b30b9cc0be988cff97
```

Modification d'une instance de base de données Amazon RDS

Vous pouvez modifier les paramètres d'une instance de base de données pour accomplir des tâches telles que l'ajout de stockage supplémentaire ou la modification de la classe d'instance. Cette rubrique explique comment modifier une instance de base de données Amazon RDS et décrit les paramètres des instances de base de données.

Nous vous recommandons de tester toutes les modifications apportées à une instance test avant de modifier une instance de production, et ce afin de bien comprendre l'impact de chaque modification. Les tests sont particulièrement importants lors de la mise à niveau des versions de base de données.

La plupart des modifications apportées à une instance de base de données peuvent être appliquées immédiatement ou différées jusqu'à la fenêtre de maintenance suivante. Certaines modifications, telles que les modifications d'un groupe de paramètres, nécessitent que vous redémarriez manuellement votre instance de base de données pour que la modification entre en vigueur.

> Important
>
> Certaines modifications peuvent entraîner une indisponibilité, car Amazon RDS doit redémarrer votre instance de base de données pour que la modification entre en vigueur. Analysez l'impact sur votre base de données et les applications avant de modifier vos paramètres d'instance de base de données.

Console

Pour modifier une instance de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Bases de données, puis l'instance de base de données que vous souhaitez modifier.
3. Sélectionnez Modify. La page Modifier l'instance de base de données s'affiche.
4. Modifiez les paramètres de votre choix. Pour plus d'informations sur chaque paramètre, consultez Paramètres des instances de base de données (p. 245).
5. Lorsque tous les changements vous conviennent, choisissez Continuer et vérifiez le résumé des modifications.
6. (Facultatif) Choisissez Appliquer immédiatement pour appliquer les modifications immédiatement. La sélection de cette option peut entraîner une interruption de service dans certains cas. Pour plus d'informations, consultez Utilisation du paramètre Appliquer immédiatement (p. 244).

7. Sur la page de confirmation, examinez vos modifications. Si elles sont correctes, choisissez Modification d'une instance de base de données pour enregistrer vos modifications.

   Ou choisissez Retour pour revoir vos modifications, ou choisissez Annuler pour les annuler.

AWS CLI

Pour modifier une instance de base de données à l'aide de l'AWS CLI, appelez la commande modify-db-instance. Spécifiez l'identifiant d'instance de base de données et les valeurs des options que vous souhaitez modifier. Pour de plus amples informations sur chaque option, veuillez consulter Paramètres des instances de base de données (p. 245).

Example

Le code suivant modifie `mydbinstance` en définissant la période de rétention des sauvegardes sur 1 semaine (7 jours). Ce code active la protection contre la suppression en utilisant `--deletion-protection`. Pour désactiver la protection contre la suppression, utilisez `--no-deletion-protection`. Les modifications sont appliquées pendant le créneau de maintenance suivant à l'aide de `--no-apply-immediately`. Pour appliquer les modifications immédiatement, utilisez `--apply-immediately`. Pour plus d'informations, consultez Utilisation du paramètre Appliquer immédiatement (p. 244).

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --backup-retention-period 7 \
    --deletion-protection \
    --no-apply-immediately
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --backup-retention-period 7 ^
    --deletion-protection ^
    --no-apply-immediately
```

API RDS

Pour modifier une instance de base de données à l'aide de l'API Amazon RDS, appelez l'opération ModifyDBInstance. Spécifiez l'identifiant d'instance de base de données et les paramètres que vous souhaitez modifier. Pour plus d'informations sur chaque paramètre, consultez Paramètres des instances de base de données (p. 245).

Utilisation du paramètre Appliquer immédiatement

Quand vous modifiez une instance de base de données, vous pouvez appliquer immédiatement les modifications. Pour appliquer immédiatement les modifications, choisissez l'option Appliquer immédiatement dans l'AWS Management Console. Vous pouvez aussi utiliser le paramètre `--apply-immediately` lors de l'appel de l'AWS CLI ou définir le paramètre `ApplyImmediately` sur `true` lors de l'utilisation de l'API Amazon RDS.

Si vous ne choisissez pas d'appliquer les modifications immédiatement, les modifications sont placées dans la file d'attente des modifications en attente. Au cours de la fenêtre de maintenance suivante, les modifications en attente sont appliquées. Si vous choisissez d'appliquer les modifications immédiatement, vos nouvelles modifications et les modifications placées dans la file d'attente des modifications en attente sont appliquées.

> **Important**
>
> Si des modifications en attente nécessitent une interruption, le choix de l'option Appliquer immédiatement peut entraîner une interruption imprévue.
> Si vous choisissez d'appliquer une modification immédiatement, les modifications en attente sont également appliquées immédiatement, au lieu d'attendre la fenêtre de maintenance suivante.
> Si vous ne souhaitez pas qu'une modification en attente soit appliquée lors de la fenêtre de maintenance suivante, vous pouvez modifier l'instance de base de données de façon à inverser la modification. Vous pouvez le faire en utilisant l'AWS CLI et en spécifiant l'option `--apply-immediately`.

Les modifications de certains paramètres de base de données sont appliquées immédiatement, même si vous choisissez de reporter vos modifications. Pour savoir comment les différents paramètres de base de données interagissent avec le paramètre Appliquer immédiatement, veuillez consulter Paramètres des instances de base de données (p. 245).

Paramètres des instances de base de données

Le tableau suivant contient des détails sur les paramètres que vous pouvez et ne pouvez pas modifier, le moment auquel les modifications peuvent être appliquées et des informations concernant l'interruption de l'instance de base de données.

Vous pouvez modifier une instance de base de données à l'aide de la console, de la commande d'interface de ligne de commande `modify-db-instance` ou de l'opération d'API RDS `ModifyDBInstance`.

Configuration et description de la console	Option de l'interface de ligne de commande et paramètre de l'API RDS	Lorsque la modification a lieu	Remarques sur les temps d'arrêt	Moteurs de base de données pris en charge

Stockage alloué
 	
Volume de stockage en gibioctets que vous voulez allouer pour votre instance de base de données. Vous pouvez uniquement augmenter le stockage alloué. Vous ne pouvez pas le réduire.
 	
Vous ne pouvez pas modifier le stockage de certaines instances de base de données plus anciennes ou les instances de base de données restaurées à partir d'instantanés de bases de données. Le paramètre Stockage alloué est désactivé dans la console si votre instance de base de données n'est pas éligible. Pour savoir si vous pouvez allouer plus de stockage, utilisez la commande d'interface de ligne de commande describe-valid-db-instance-modifications. Cette
	Option de l'interface de ligne de commande :
	
	`--allocated-storage`
	
	Paramètre de l'API RDS :
	
	`AllocatedStorage`
		Si vous choisissez d'appliquer la modification immédiatement, elle se produit immédiatement.
		
		Si vous ne choisissez pas d'appliquer la modification immédiatement, elle se produit lors de la fenêtre de maintenance suivante.
			Aucune interruption de service n'a lieu pendant cette modification. Les performances peuvent se dégrader pendant la modification.	Tous les moteurs de base de données

Configuration et description de la console	Option de l'interface de ligne de commande et paramètre de l'API RDS	Lorsque la modification a lieu	Remarques sur les temps d'arrêt	Moteurs de base de données pris en charge
commande renvoie les options de stockage valides pour votre instance de base de données. Vous ne pouvez pas modifier le stockage alloué si le statut de l'instance de base de données est storage-optimization ou si le stockage alloué pour l'instance de base de données a été modifié au cours des six dernières heures. Le stockage maximal autorisé dépend de votre moteur de base de données et du type de stockage. Pour plus d'informations, consultez Stockage d'instance de base de données Amazon RDS (p. 30).				

Mise à niveau automatique de versions mineures
 	
Oui pour permettre à votre instance de base de données de recevoir automatiquement les mises à niveau de la version mineure préférée du moteur de base de données lorsqu'elles sont disponibles. Amazon RDS effectue les mises à niveau automatiques des versions mineures dans la fenêtre de maintenance. Dans le cas contraire, Non.
 	
Pour plus d'informations, consultez Mise à niveau automatique de la version mineure du moteur (p. 269).
	Option de l'interface de ligne de commande :
	
	`--auto-minor-version-upgrade|--no-auto-minor-version-upgrade`
	
	Paramètre de l'API RDS :
	
	`AutoMinorVersionUpgrade`
		La modification a lieu immédiatement. Ce paramètre ignore le paramètre Appliquer immédiatement.	Aucune interruption de service n'a lieu pendant cette modification.	Uniquement MariaDB, MySQL, Oracle et PostgreSQL

Configuration et description de la console	Option de l'interface de ligne de commande et paramètre de l'API RDS	Lorsque la modification a lieu	Remarques sur les temps d'arrêt	Moteurs de base de données pris en charge

Période de rétention des sauvegardes
 	
Le nombre de jours de conservation des sauvegardes automatiques. Pour désactiver les sauvegardes automatiques, définissez la période de conservation des sauvegardes sur 0.
 	
Pour plus d'informations, consultez Utilisation des sauvegardes (p. 317).
	Option de l'interface de ligne de commande :
	
	`--backup-retention-period`
	
	Paramètre de l'API RDS :
	
	`BackupRetentionPeriod`
		Si vous choisissez d'appliquer la modification immédiatement, elle se produit immédiatement.
		
		Si vous choisissez de ne pas appliquer la modification immédiatement et que vous remplacez la valeur non nulle du paramètre par une autre valeur non nulle, la modification est appliquée de manière asynchrone dès que possible. Sinon, la modification est appliquée pendant la fenêtre de maintenance suivante.
			Une interruption se produit si vous passez de 0 à une valeur non nulle, ou d'une valeur non nulle à 0.	Tous les moteurs de base de données

Fenêtre de sauvegarde
 	
L'intervalle de temps pendant lequel des sauvegardes automatiques de vos bases de données se produisent. Le créneau de sauvegarde correspond à une heure de début en heure UTC (Universal Coordinated Time) et une durée en heures.
 	
Pour plus d'informations, consultez Utilisation des sauvegardes (p. 317).
	Option de l'interface de ligne de commande :
	
	`--preferred-backup-window`
	
	Paramètre de l'API RDS :
	
	`PreferredBackupWindow`
		La modification est appliquée de manière asynchrone, dès que possible.	Aucune interruption de service n'a lieu pendant cette modification.	Tous les moteurs de base de données

Configuration et description de la console	Option de l'interface de ligne de commande et paramètre de l'API RDS	Lorsque la modification a lieu	Remarques sur les temps d'arrêt	Moteurs de base de données pris en charge

Autorité de certification
 	
Certificat que vous souhaitez utiliser pour les connexions SSL/TLS.
 	
Pour plus d'informations, consultez Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).
	Option de l'interface de ligne de commande :
	
	`--ca-certificate-identifier`
	
	Paramètre de l'API RDS :
	
	`CACertificateIdentifier`
		Si vous choisissez d'appliquer la modification immédiatement, elle se produit immédiatement.
		
		Si vous ne choisissez pas d'appliquer la modification immédiatement, elle se produit lors de la fenêtre de maintenance suivante.
			Une interruption de service a lieu pendant cette modification.	Tous les moteurs de base de données

Copier les balises aux instantanés
 	
Si vous avez des balises d'instance de base de données, activez cette option pour les copier lorsque vous créez un instantané de bases de données.
 	
Pour plus d'informations, consultez Balisage de ressources Amazon RDS (p. 293).
	Option de l'interface de ligne de commande :
	
	`--copy-tags-to-snapshot` ou `--no-copy-tags-to-snapshot`
	
	Paramètre de l'API RDS :
	
	`CopyTagsToSnapshot`
		La modification a lieu immédiatement. Ce paramètre ignore le paramètre Appliquer immédiatement.	Aucune interruption de service n'a lieu pendant cette modification.	Tous les moteurs de base de données

Port de la base de données
 	
Port que vous souhaitez utiliser pour accéder à l'instance de bases de données.
 	
La valeur du port ne doit correspondre à aucune des valeurs de port spécifiées pour les options du groupe d'options associé à l'instance de base de données.
 	
Pour plus d'informations, consultez Connexion à une instance de base de données Amazon RDS (p. 169).
	Option de l'interface de ligne de commande :
	
	`--db-port-number`
	
	Paramètre de l'API RDS :
	
	`DBPortNumber`
		La modification a lieu immédiatement. Ce paramètre ignore le paramètre Appliquer immédiatement.	L'instance de base de données est redémarrée immédiatement.	Tous les moteurs de base de données

Configuration et description de la console	Option de l'interface de ligne de commande et paramètre de l'API RDS	Lorsque la modification a lieu	Remarques sur les temps d'arrêt	Moteurs de base de données pris en charge

Version du moteur de base de données
 	
Version du moteur de base de données que vous souhaitez utiliser. Avant de mettre à niveau vos instances de bases de données de production, nous vous recommandons de tester le processus de mise à niveau sur une instance de base de données de test afin de vérifier sa durée et de valider vos applications.
 	
Pour plus d'informations, consultez Mise à niveau d'une version du moteur d'une instance de base de données (p. 267).
	Option de l'interface de ligne de commande :
	
	`--engine-version`
	
	Paramètre de l'API RDS :
	
	`EngineVersion`
		Si vous choisissez d'appliquer la modification immédiatement, elle se produit immédiatement.
		
		Si vous ne choisissez pas d'appliquer la modification immédiatement, elle se produit lors de la fenêtre de maintenance suivante.
			Une interruption de service a lieu pendant cette modification.	Tous les moteurs de base de données

Classe d'instance de base de données
 	
La classe d'instance de base de données que vous souhaitez utiliser.
 	
Pour plus d'informations, consultez Classes d'instances de base de données (p. 6).
	Option de l'interface de ligne de commande :
	
	`--db-instance-class`
	
	Paramètre de l'API RDS :
	
	`DBInstanceClass`
		Si vous choisissez d'appliquer la modification immédiatement, elle se produit immédiatement.
		
		Si vous ne choisissez pas d'appliquer la modification immédiatement, elle se produit lors de la fenêtre de maintenance suivante.
			Une interruption de service a lieu pendant cette modification.	Tous les moteurs de base de données

Configuration et description de la console	Option de l'interface de ligne de commande et paramètre de l'API RDS	Lorsque la modification a lieu	Remarques sur les temps d'arrêt	Moteurs de base de données pris en charge

Identifiant d'instance de base de données
 	
Nouvel identifiant de l'instance de base de données. Cette valeur est stockée sous la forme d'une chaîne en minuscules.
 	
Pour plus d'informations sur les effets du changement de nom d'une instance de base de données, consultez Affectation d'un nouveau nom à une instance DB (p. 270).
	Option de l'interface de ligne de commande :
	
	`--new-db-instance-identifier`
	
	Paramètre de l'API RDS :
	
	`NewDBInstanceIdentifier`
		Si vous choisissez d'appliquer la modification immédiatement, elle se produit immédiatement.
		
		Si vous ne choisissez pas d'appliquer la modification immédiatement, elle se produit lors de la fenêtre de maintenance suivante.
			Une interruption de service a lieu pendant cette modification.	Tous les moteurs de base de données

Groupe de paramètres de base de données
 	
Groupe de paramètres de base de données que vous souhaitez associer à l'instance de base de données.
 	
Pour plus d'informations, consultez Utilisation de groupes de paramètres de base de données (p. 225).
	Option de l'interface de ligne de commande :
	
	`--db-parameter-group-name`
	
	Paramètre de l'API RDS :
	
	`DBParameterGroupName`
		La modification du groupe de paramètres a lieu immédiatement.	Aucune interruption de service n'a lieu pendant cette modification. Toutefois, vous devez redémarrer manuellement l'instance de base de données avant que le nouveau groupe de paramètres de base de données ne soit utilisé par l'instance de base de données.
			
			Pour plus d'informations, consultez Utilisation de groupes de paramètres de base de données (p. 225) et Redémarrage d'une instance de base de données (p. 272).
				Tous les moteurs de base de données

Configuration et description de la console	Option de l'interface de ligne de commande et paramètre de l'API RDS	Lorsque la modification a lieu	Remarques sur les temps d'arrêt	Moteurs de base de données pris en charge

Deletion protection (Protection contre la suppression)
 	
Enable deletion protection (Activer la protection contre la suppression) vise à empêcher la suppression de votre instance de base de données.
 	
Pour plus d'informations, consultez Suppression d'une instance de base de données (p. 313).
	Option de l'interface de ligne de commande :
	
	`--deletion-protection|--no-deletion-protection`
	
	Paramètre de l'API RDS :
	
	`DeletionProtection`
		La modification a lieu immédiatement. Ce paramètre ignore le paramètre Appliquer immédiatement.	Aucune interruption de service n'a lieu pendant cette modification.	Tous les moteurs de base de données

Surveillance améliorée
 	
Activer la surveillance améliorée permet d'activer la collecte des métriques en temps réel pour le système d'exploitation sur lequel votre instance de base de données s'exécute.
 	
Pour plus d'informations, consultez Surveillance améliorée (p. 394).
	Option de l'interface de ligne de commande :
	
	`--monitoring-interval` and `--monitoring-role-arn`
	
	Paramètre de l'API RDS :
	
	`MonitoringInterval` and `MonitoringRoleArn`
		La modification a lieu immédiatement. Ce paramètre ignore le paramètre Appliquer immédiatement.	Aucune interruption de service n'a lieu pendant cette modification.	Tous les moteurs de base de données

Authentification de base de données IAM
 	
Activer l'authentification IAM DB pour authentifier les utilisateurs de base de données via les utilisateurs et les rôles IAM.
 	
Pour plus d'informations, consultez Authentification de base de données IAM pour MySQL et PostgreSQL (p. 1554).
	Option de l'interface de ligne de commande :
	
	`--enable-iam-database-authentication|--no-enable-iam-database-authentication`
	
	Paramètre de l'API RDS :
	
	`EnableIAMDatabaseAuthentication`
		Si vous choisissez d'appliquer la modification immédiatement, elle se produit immédiatement.
		
		Si vous ne choisissez pas d'appliquer la modification immédiatement, elle se produit lors de la fenêtre de maintenance suivante.
			Une brève interruption de service a lieu pendant cette modification.	Uniquement MySQL et PostgreSQL

Configuration et description de la console	Option de l'interface de ligne de commande et paramètre de l'API RDS	Lorsque la modification a lieu	Remarques sur les temps d'arrêt	Moteurs de base de données pris en charge

Authentification Kerberos
 	
Choisissez le répertoire Active Directory vers lequel déplacer l'instance de base de données. Le répertoire doit exister avant cette opération. Si un répertoire est déjà sélectionné, vous pouvez spécifier Aucun pour supprimer l'instance de base de données de son répertoire actuel.
 	
Pour plus d'informations, consultez Authentification Kerberos (p. 1520).
	Option de l'interface de ligne de commande :
	
	`--domain` and `--domain-iam-role-name`
	
	Paramètre de l'API RDS :
	
	`Domain` and `DomainIAMRoleName`
		Si vous choisissez d'appliquer la modification immédiatement, elle se produit immédiatement.
		
		Si vous ne choisissez pas d'appliquer la modification immédiatement, elle se produit lors de la fenêtre de maintenance suivante.
			Une brève interruption de service a lieu pendant cette modification.	Uniquement Microsoft SQL Server, MySQL, Oracle et PostgreSQL

Modèle de licence
 	
Choisissez Réutilisez vos licences pour utiliser votre licence pour Oracle.
 	
Choisissez licence-incluse pour utiliser le contrat de licence général pour Microsoft SQL Server ou Oracle.
 	
Pour plus d'informations, consultez Gestion des licences Microsoft SQL Server sur Amazon RDS (p. 617) et Options de licence Oracle (p. 930).
	Option de l'interface de ligne de commande :
	
	`--license-model`
	
	Paramètre de l'API RDS :
	
	`LicenseModel`
		Si vous choisissez d'appliquer la modification immédiatement, elle se produit immédiatement.
		
		Si vous ne choisissez pas d'appliquer la modification immédiatement, elle se produit lors de la fenêtre de maintenance suivante.
			Une interruption de service a lieu pendant cette modification.	Uniquement Microsoft SQL Server et Oracle

Exportations des journaux
 	
Types de fichiers journaux de base de données à publier sur Amazon CloudWatch Logs.
 	
Pour plus d'informations, consultez Publication des journaux de base de données dans Amazon CloudWatch Logs (p. 493).
	Option de l'interface de ligne de commande :
	
	`--cloudwatch-logs-export-configuration`
	
	Paramètre de l'API RDS :
	
	`CloudwatchLogsExportConfiguration`
		La modification a lieu immédiatement. Ce paramètre ignore le paramètre Appliquer immédiatement.	Aucune interruption de service n'a lieu pendant cette modification.	Tous les moteurs de base de données

Configuration et description de la console	Option de l'interface de ligne de commande et paramètre de l'API RDS	Lorsque la modification a lieu	Remarques sur les temps d'arrêt	Moteurs de base de données pris en charge

Fenêtre de maintenance
 	
L'intervalle de temps pendant lequel la maintenance du système a lieu. La maintenance du système inclut les mises à niveau, le cas échéant. Le fenêtre de maintenance correspond à une heure de début en heure UTC (Universal Coordinated Time) et une durée en heures.
 	
Si vous définissez la fenêtre sur l'heure actuelle, il doit y avoir au moins 30 minutes entre l'heure actuelle et la fin du créneau afin de garantir l'application des modifications en attente.
 	
Pour plus d'informations, consultez Le créneau de maintenance Amazon RDS (p. 264).
	Option de l'interface de ligne de commande :
	
	`--preferred-maintenance-window`
	
	Paramètre de l'API RDS :
	
	`PreferredMaintenanceWindow`
		La modification a lieu immédiatement. Ce paramètre ignore le paramètre Appliquer immédiatement.	Si une ou plusieurs actions en attente entraînent une panne et que la fenêtre de maintenance est modifiée pour inclure l'heure actuelle, les actions en attente sont appliquées immédiatement et une panne se produit.	Tous les moteurs de base de données

déploiement multi-AZ
 	
Oui pour déployer votre instance de base de données dans plusieurs zones de disponibilité. Dans le cas contraire, Non.
 	
Pour plus d'informations, consultez Haute disponibilité (multi-AZ) pour Amazon RDS (p. 43).
	Option de l'interface de ligne de commande :
	
	`--multi-az|--no-multi-az`
	
	Paramètre de l'API RDS :
	
	`MultiAZ`
		Si vous choisissez d'appliquer la modification immédiatement, elle se produit immédiatement.
		
		Si vous ne choisissez pas d'appliquer la modification immédiatement, elle se produit lors de la fenêtre de maintenance suivante.
			Aucune interruption de service n'a lieu pendant cette modification.	Tous les moteurs de base de données

Configuration et description de la console	Option de l'interface de ligne de commande et paramètre de l'API RDS	Lorsque la modification a lieu	Remarques sur les temps d'arrêt	Moteurs de base de données pris en charge

New master password
 	
Le mot de passe de votre utilisateur principal. Le mot de passe doit contenir entre 8 et 41 caractères alphanumériques.
	Option de l'interface de ligne de commande :
	
	`--master-user-password`
	
	Paramètre de l'API RDS :
	
	`MasterUserPassword`
		La modification est appliquée de manière asynchrone, dès que possible. Ce paramètre ignore le paramètre Appliquer immédiatement.	Aucune interruption de service n'a lieu pendant cette modification.	Tous les moteurs de base de données

Groupe d'options
 	
Le groupe d'options que vous voulez associer à l'instance de base de données.
 	
Pour plus d'informations, consultez Utilisation de groupes d'options (p. 209).
	Option de l'interface de ligne de commande :
	
	`--option-group-name`
	
	Paramètre de l'API RDS :
	
	`OptionGroupName`
		Si vous choisissez d'appliquer la modification immédiatement, elle se produit immédiatement.
		
		Si vous ne choisissez pas d'appliquer la modification immédiatement, elle se produit lors de la fenêtre de maintenance suivante.
			Aucune interruption de service n'a lieu pendant cette modification.	Tous les moteurs de base de données

Configuration et description de la console	Option de l'interface de ligne de commande et paramètre de l'API RDS	Lorsque la modification a lieu	Remarques sur les temps d'arrêt	Moteurs de base de données pris en charge

Performance Insights (Analyse des performances)
 	
Activer Performance Insights permet de surveiller la charge de votre instance de base de données et ainsi d'analyser les performances de votre base de données et de résoudre les problèmes associés.
 	
L'analyse des performances n'est pas disponible pour certaines versions de moteurs de base de données et classes d'instance de base de données. La section Performance Insights n'apparaît pas dans la console si elle n'est pas disponible pour votre instance de base de données.
 	
Pour plus d'informations, consultez Utilisation d'Amazon RDS Performance Insights (p. 410).
	Option de l'interface de ligne de commande :
	
	`--enable-performance-insights|--no-enable-performance-insights`
	
	Paramètre de l'API RDS :
	
	`EnablePerformanceInsights`
		La modification a lieu immédiatement. Ce paramètre ignore le paramètre Appliquer immédiatement.	Aucune interruption de service n'a lieu pendant cette modification.	Tous les moteurs de base de données

Performance Insights Master key (Clé principale d'analyse des performances)
 	
Identificateur de clé AWS KMS de la clé principale client (CMK) pour le chiffrement des données Performance Insights. L'ID de clé est l'Amazon Resource Name (ARN), l'identifiant de clé AWS KMS ou l'alias de clé pour la clé CMK.
 	
Pour plus d'informations, consultez Activation et désactivation de Performance Insights (p. 413).
	Option de l'interface de ligne de commande :
	
	`--performance-insights-kms-key-id`
	
	Paramètre de l'API RDS :
	
	`PerformanceInsightsKMSKeyId`
		La modification a lieu immédiatement. Ce paramètre ignore le paramètre Appliquer immédiatement.	Aucune interruption de service n'a lieu pendant cette modification.	Tous les moteurs de base de données

Configuration et description de la console	Option de l'interface de ligne de commande et paramètre de l'API RDS	Lorsque la modification a lieu	Remarques sur les temps d'arrêt	Moteurs de base de données pris en charge

Performance Insights Retention period (Période de rétention des analyses de performances)
 	
Durée de conservation, en jours, des données d'analyse des performances. Les valeurs valides sont 7 ou 731 (2 ans).
 	
Pour plus d'informations, consultez Activation et désactivation de Performance Insights (p. 413).
	Option de l'interface de ligne de commande :
	
	`--performance-insights-retention-period`
	
	Paramètre de l'API RDS :
	
	`PerformanceInsightsRetentionPeriod`
		La modification a lieu immédiatement. Ce paramètre ignore le paramètre Appliquer immédiatement.	Aucune interruption de service n'a lieu pendant cette modification.	Tous les moteurs de base de données

Processor features (Caractéristiques du processeur)
 	
Nombre de cœurs d'UC et nombre de threads par cœur pour la classe à laquelle appartient l'instance de base de données.
 	
Pour plus d'informations, consultez Configuration du processeur pour une classe d'instance de base de données (p. 13).
	Option de l'interface de ligne de commande :
	
	`--processor-features` and `--use-default-processor-features | --no-use-default-processor-features`
	
	Paramètre de l'API RDS :
	
	`ProcessorFeatures` and `UseDefaultProcessorFeatures`
		Si vous choisissez d'appliquer la modification immédiatement, elle se produit immédiatement.
		
		Si vous ne choisissez pas d'appliquer la modification immédiatement, elle se produit lors de la fenêtre de maintenance suivante.
			Une interruption de service a lieu pendant cette modification.	Uniquement Oracle

IOPS provisionnés
 	
Nouvelle valeur d'IOPS provisionnés (opérations d'I/O par seconde) pour l'instance de base de données. Ce paramètre n'est disponible que si l'option IOPS dimensionné (SSD) est choisie pour Type de stockage.
 	
Pour plus d'informations, consultez Stockage SSD d'I/O par seconde provisionnées (p. 33).
	Option de l'interface de ligne de commande :
	
	`--iops`
	
	Paramètre de l'API RDS :
	
	`Iops`
		Si vous choisissez d'appliquer la modification immédiatement, elle se produit immédiatement.
		
		Si vous ne choisissez pas d'appliquer la modification immédiatement, elle se produit lors de la fenêtre de maintenance suivante.
			Aucune interruption de service n'a lieu pendant cette modification.	Tous les moteurs de base de données

Configuration et description de la console	Option de l'interface de ligne de commande et paramètre de l'API RDS	Lorsque la modification a lieu	Remarques sur les temps d'arrêt	Moteurs de base de données pris en charge

Accès public
 	
Publicly accessible (Accessible publiquement) dote l'instance de base de données d'une adresse IP publique, ce qui signifie qu'elle est accessible en dehors du VPC. Pour être accessible au public, l'instance de base de données doit aussi se trouver dans un sous-réseau public du VPC.
 	
Not publicly accessible (Non accessible publiquement) rend l'instance de base de données accessible uniquement à partir de l'intérieur du VPC.
 	
Pour plus d'informations, consultez Masquer une instance de base de données dans un VPC depuis Internet (p. 1622).
 	
Pour se connecter à une instance de base de données hors de son Amazon VPC, l'instance de base de données doit être accessible au public, l'accès doit être accordé en utilisant les règles entrantes du groupe de sécurité de l'instance de base de données et d'autres exigences doivent être respectées. Pour de plus amples informations, veuillez consulter Impossible de se connecter à l'instance de base de données Amazon RDS (p. 1639).
 	
Si votre instance de base de données n'est pas accessible publiquement, vous pouvez également utiliser une connexion VPN site à site AWS ou une connexion AWS Direct Connect pour y accéder à partir d'un réseau privé. Pour de plus amples informations, veuillez
	Option de l'interface de ligne de commande :
	
	`--publicly-accessible|--no-publicly-accessible`
	
	Paramètre de l'API RDS :
	
	`PubliclyAccessible`
		La modification a lieu immédiatement. Ce paramètre ignore le paramètre Appliquer immédiatement.	Aucune interruption de service n'a lieu pendant cette modification.	Tous les moteurs de base de données

Configuration et description de la console	Option de l'interface de ligne de commande et paramètre de l'API RDS	Lorsque la modification a lieu	Remarques sur les temps d'arrêt	Moteurs de base de données pris en charge
consulter Confidentialité du trafic inter-réseaux (p. 1535).				

Groupe de sécurité
 	
Groupe de sécurité de VPC que vous voulez associer à l'instance de base de données.
 	
Pour plus d'informations, consultez Contrôle d'accès par groupe de sécurité (p. 1590).
	Option de l'interface de ligne de commande :
	
	`--vpc-security-group-ids`
	
	Paramètre de l'API RDS :
	
	`VpcSecurityGroupIds`
		La modification est appliquée de manière asynchrone, dès que possible. Ce paramètre ignore le paramètre Appliquer immédiatement.	Aucune interruption de service n'a lieu pendant cette modification.	Tous les moteurs de base de données

Dimensionnement automatique du stockage
 	
Enable storage autoscaling (Activer le dimensionnement automatique du stockage) permet à Amazon RDS d'augmenter automatiquement l'espace de stockage quand cela est nécessaire pour éviter que votre instance de base de données en manque.
 	
Utilisez Maximum storage threshold (Seuil de stockage maximum) pour définir la limite supérieure au-delà de laquelle Amazon RDS augmente automatiquement l'espace de stockage pour votre instance de base de données. La valeur par défaut est 1 000 GiO.
 	
Pour plus d'informations, consultez Gestion automatique de la capacité avec le dimensionnement automatique du stockage Amazon RDS (p. 306).
	Option de l'interface de ligne de commande :
	
	`--max-allocated-storage`
	
	Paramètre de l'API RDS :
	
	`MaxAllocatedStorage`
		La modification a lieu immédiatement. Ce paramètre ignore le paramètre Appliquer immédiatement.	Aucune interruption de service n'a lieu pendant cette modification.	Tous les moteurs de base de données

Configuration et description de la console	Option de l'interface de ligne de commande et paramètre de l'API RDS	Lorsque la modification a lieu	Remarques sur les temps d'arrêt	Moteurs de base de données pris en charge

Type de stockage
 	
Type de stockage que vous souhaitez utiliser.
 	
Une fois qu'Amazon RDS a commencé à modifier votre instance de base de données pour modifier la taille ou le type de stockage, vous ne pouvez pas envoyer d'autre demande de modification de la taille ou du type de stockage pendant six heures.
 	
Pour plus d'informations, consultez Types de stockage Amazon RDS (p. 30).
	Option de l'interface de ligne de commande :
	
	`--storage-type`
	
	Paramètre de l'API RDS :
	
	`StorageType`
		Si vous choisissez d'appliquer la modification immédiatement, elle se produit immédiatement.
		
		Si vous ne choisissez pas d'appliquer la modification immédiatement, elle se produit lors de la fenêtre de maintenance suivante.
			Toutes les modifications suivantes entraînent une brève interruption de service au démarrage du processus. Après cette interruption, vous pouvez utiliser votre base de données normalement pendant les modifications.
			
			• De Usage général à Magnétique.
			• De Usage général (SSD) à IOPS dimensionné (SSD). L'interruption a lieu uniquement si l'instance de base de données est mono-AZ et que vous utilisez un groupe de paramètres personnalisé. Il n'y a aucune interruption de service pour une instance de base de données multi-AZ.
			• De Magnétique à Usage général (SSD).
			• De Magnétique à IOPS dimensionné (SSD).
			• De IOPS dimensionné (SSD) à Magnétique.
			• Des IOPS dimensionné
				Tous les moteurs de base de données

Configuration et description de la console	Option de l'interface de ligne de commande et paramètre de l'API RDS	Lorsque la modification a lieu	Remarques sur les temps d'arrêt	Moteurs de base de données pris en charge
			(SSD) à l'Usage général (SSD). L'interruption a lieu uniquement si l'instance de base de données est mono-AZ et que vous utilisez un groupe de paramètres personnalisé. Il n'y a aucune interruption de service pour une instance de base de données multi-AZ.	

Groupe de sous-réseaux
 	
Le groupe de sous-réseaux pour l'instance de base de données. Vous pouvez utiliser ce paramètre pour déplacer votre instance de base de données vers un autre VPC. Si votre instance de base de données ne se trouve pas dans un VPC, vous pouvez utiliser ce paramètre pour déplacer votre instance de base de données vers un VPC.
 	
Pour plus d'informations, consultez VPC Amazon Virtual Private Cloud et Amazon RDS (p. 1610).
	Option de l'interface de ligne de commande :
	
	`--db-subnet-group-name`
	
	Paramètre de l'API RDS :
	
	`DBSubnetGroupName`
		Si vous choisissez d'appliquer la modification immédiatement, elle se produit immédiatement.
		
		Si vous ne choisissez pas d'appliquer la modification immédiatement, elle se produit lors de la fenêtre de maintenance suivante.
			Une interruption de service a lieu pendant cette modification.	Tous les moteurs de base de données

Entretien d'une instance de base de données

Amazon RDS effectue régulièrement la maintenance des ressources Amazon RDS. La maintenance implique le plus souvent des mises à jour de la version du moteur de base de données, du système d'exploitation sous-jacent ou du matériel sous-jacent de l'instance de base de données. Les mises à jour du système d'exploitation se produisent le plus souvent pour des raisons de sécurité et doivent être réalisées dès que possible.

Certains éléments de maintenance exigent que Amazon RDS mette votre instance de base de données hors ligne pendant un court moment. Parmi les éléments de maintenance qui nécessitent qu'une ressource soit hors ligne figure l'application obligatoire de correctifs au système d'exploitation ou à la base de données. Les mises à jour correctives obligatoires sont planifiées automatiquement uniquement pour les

correctifs associés à la sécurité et à la fiabilité de l'instance. Ce type de mise à jour corrective a lieu peu fréquemment (en général une fois à quelques mois d'intervalle) et nécessite rarement plus d'une fraction de votre créneau de maintenance.

Les modifications différées de l'instance de base de données que vous avez choisi de ne pas appliquer immédiatement le sont pendant la fenêtre de maintenance. Par exemple, vous pouvez choisir de modifier la classe ou le groupe de paramètres de l'instance de base de données pendant la fenêtre de maintenance. Pour plus d'informations sur la modification d'une instance de base de données , consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Vous pouvez voir si une mise à jour de maintenance est disponible pour votre instance de bases de données à l'aide de la console RDS, d'AWS CLI ou de l'API Amazon RDS. Si une mise à jour est disponible, elle est indiquée dans la colonne Maintenance pour l'instance de base de données sur la console Amazon RDS, comme illustré ci-dessous.

Si aucune mise à jour de maintenance n'est disponible pour uneinstance de base de données, la valeur de la colonne est none.

Si une mise à jour de maintenance est disponible pour uneinstance de base de données, les valeurs de colonne suivantes sont possibles :

- required (obligatoire) – L'action de maintenance sera appliquée à la ressource et ne peut pas être reportée indéfiniment.
- available – L'action de maintenance est disponible, mais ne sera pas appliquée automatiquement à la ressource. Vous pouvez l'appliquer manuellement.
- next window – L'action de maintenance sera appliquée à la ressource lors de la prochaine fenêtre de maintenance.
- In progress – L'action de maintenance est en cours d'application à la ressource.

Si une mise à jour est disponible, vous pouvez effectuer une des actions suivantes :

- Si la valeur de maintenance est next window (fenêtre suivante), reportez les éléments de maintenance en choisissant Reporter la mise à niveau dans Actions. Vous ne pouvez pas reporter une action de maintenance en cours.
- Appliquer immédiatement les éléments de maintenance.
- Planifier le démarrage des éléments de maintenance au cours de votre créneau de maintenance suivant.
- Ne rien faire.

> **Note**
>
> Certaines mises à jour de système d'exploitation sont marquées comme obligatoires. Si vous reportez une mise à jour obligatoire, vous recevez une notification d'Amazon RDS vous indiquant quand la mise à jour sera effectuée. Les autres mises à jour sont indiquées comme disponibles et vous pouvez les reporter indéfiniment.

Pour entreprendre une action, choisissez l'instance de base de données pour afficher ses détails, puis choisissez Maintenance & backups (Maintenance et sauvegardes). Les éléments de maintenance en attente apparaissent.

La fenêtre de maintenance détermine quand les opérations en attente démarrent et ne limite pas la durée d'exécution totale de ces opérations. Il n'est pas garanti que les opérations de maintenance seront terminées avant la fin de la fenêtre de maintenance ; elles peuvent continuer au-delà de l'heure de fin spécifiée. Pour plus d'informations, consultez Le créneau de maintenance Amazon RDS (p. 264).

Application des mises à jour pour une instance de base de données

Amazon RDS vous permet de choisir le moment d'application des opérations de maintenance. Vous pouvez décider quand Amazon RDS doit appliquer les mises à jour à l'aide de la console RDS, de l'AWS Command Line Interface (AWS CLI) ou de l'API RDS.

Console

Pour gérer une mise à jour du système d'exploitation pour une instance de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez l'instance de base de données pour lequel une mise à jour obligatoire est disponible.
4. Sous Actions, choisissez une des options suivantes :
   - Mettre à niveau maintenant
   - Mettre à niveau lors du créneau suivant

     Note

     Si vous choisissez Mettre à niveau lors du créneau suivant et souhaitez ensuite retarder la mise à jour, vous pouvez choisir Reporter la mise à niveau. Vous ne pouvez pas reporter une action de maintenance en cours.
     Pour annuler une action de maintenance, modifiez l'instance de base de données et désactivez Mise à niveau automatique des versions mineures.

AWS CLI

Pour appliquer une mise à jour en attente sur une instance de bases de données, utilisez la commande apply-pending-maintenance-action de l'AWS CLI.

Example

Pour Linux, macOS ou 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
```

Pour 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**
>
> Pour différer une action de maintenance, spécifiez `undo-opt-in` pour `--opt-in-type`. Vous ne pouvez pas indiquer`undo-opt-in` pour `--opt-in-type` si l'action de maintenance est en cours. Pour annuler une action de maintenance, exécutez la commande AWS CLI modify-db-instance et spécifiez `--no-auto-minor-version-upgrade`.

Pour renvoyer la liste des ressources qui possèdent au moins une mise à jour en attente, utilisez la commande describe-pending-maintenance-actions de l'AWS CLI.

Example

Pour Linux, macOS ou Unix :

```
aws rds describe-pending-maintenance-actions \
    --resource-identifier arn:aws:rds:us-west-2:001234567890:db:mysql-db
```

Pour Windows :

```
aws rds describe-pending-maintenance-actions ^
    --resource-identifier arn:aws:rds:us-west-2:001234567890:db:mysql-db
```

Vous pouvez également retourner une liste de ressources pour une instance de bases de données en spécifiant le paramètre `--filters` de la commande `describe-pending-maintenance-actions` de l'AWS CLI. Le format de la commande `--filters` est `Name=`*`filter-name`*`,Value=`*`resource-id`*`,...`.

Les valeurs suivantes sont acceptées pour le paramètre `Name` d'un filtre :

- `db-instance-id` – Accepte une liste d'identifiants d'instance de bases de données ou de noms Amazon Resource Name (ARN). La liste renvoyée inclut uniquement les actions de maintenance en attente pour les instances de bases de données identifiées par ces identifiants ou ARN.
- `db-cluster-id` – Accepte une liste d'identificateurs de clusters de bases de données ou d'ARN pour Amazon Aurora. La liste renvoyée inclut uniquement les actions de maintenance en attente pour les clusters de bases de données identifiés par ces identifiants ou ARN.

Par exemple, l'exemple suivant renvoie les actions de maintenance en attente pour les instances de bases de données `sample-instance1` et `sample-instance2`.

Example

Pour Linux, macOS ou Unix :

```
aws rds describe-pending-maintenance-actions \
 --filters Name=db-instance-id,Values=sample-instance1,sample-instance2
```

Pour Windows :

```
aws rds describe-pending-maintenance-actions ^
 --filters Name=db-instance-id,Values=sample-instance1,sample-instance2
```

API RDS

Pour appliquer une mise à jour à une instance de base de données, appelez l'opération d'API Amazon RDS `ApplyPendingMaintenanceAction`.

Pour renvoyer la liste des ressources qui possèdent au moins une mise à jour en attente, appelez l'opération d'API Amazon RDS `DescribePendingMaintenanceActions`.

Maintenance pour les déploiements multi-AZ

L'exécution d'une instance de base de données en tant que déploiement multi-AZ peut encore réduire l'impact d'un événement de maintenance, car Amazon RDS applique les mises à jour du système d'exploitation en suivant les étapes ci-dessous :

1. Réalisation de la maintenance sur l'instance de secours.
2. Promotion de l'instance de secours comme instance principale.
3. Réalisation de la maintenance sur l'ancienne instance principale, qui devient la nouvelle instance de secours.

Lorsque vous modifiez le moteur de base de données pour votre instance de base de données dans un déploiement Multi-AZ, Amazon RDS met à niveau simultanément les deux instances de base de données principale et secondaire. Dans ce cas, le moteur de base de données pour le déploiement Multi-AZ complet est arrêté pendant la mise à niveau.

Pour plus d'informations sur les déploiements Multi-AZ, consultez Haute disponibilité (multi-AZ) pour Amazon RDS (p. 43).

Le créneau de maintenance Amazon RDS

Chaque instance de base de données est associé à un créneau de maintenance hebdomadaire au cours duquel toutes les modifications système sont appliquées. Vous pouvez considérer le créneau de maintenance comme une occasion de contrôler le moment où les modifications et les correctifs logiciels ont lieu, qu'ils aient fait l'objet d'une demande ou qu'ils soient obligatoires. Si un événement de maintenance est planifié pour une semaine donnée, il est déclenché pendant le créneau de maintenance de 30 minutes que vous identifiez. La plupart des événements de maintenance se terminent également au cours du créneau de maintenance de 30 minutes, mais des événements de maintenance plus importants peuvent prendre plus de 30 minutes.

Ce créneau de maintenance de 30 minutes est sélectionné de manière aléatoire sur un bloc horaire de 8 heures par région. Si vous ne spécifiez pas de créneau de maintenance privilégié lors de la création de l'instance de base de données, Amazon RDS attribue un créneau de maintenance de 30 minutes un jour de semaine aléatoire.

RDS consomme certaines des ressources de votre instance de base de données pendant les opérations de maintenance. Vous remarquerez peut-être un effet minimal sur les performances. Dans le cas d'une instance de base de données, en de rares occasions, un basculement Multi-AZ peut être requis pour terminer une mise à jour de maintenance.

Vous trouverez ci-dessous les périodes de chaque région au cours desquelles les créneaux de maintenance par défaut sont attribués.

Nom de la région	Région	Bloc chronologique
USA Est (Ohio)	us-east-2	03:00–11:00 UTC
USA Est (Virginie du Nord)	us-east-1	03:00–11:00 UTC
USA Ouest (Californie du Nord)	us-west-1	06:00–14:00 UTC
USA Ouest (Oregon)	us-west-2	06:00–14:00 UTC
Asie-Pacifique (Hong Kong)	ap us-east-1	06:00–14:00 UTC
Asie-Pacifique (Mumbai)	ap-south-1	17:30–01:30 UTC
Asie-Pacifique (Osaka-Local)	ap-northeast-3	22:00–23:59 UTC
Asie-Pacifique (Séoul)	ap-northeast-2	13:00–21:00 UTC
Asie-Pacifique (Singapour)	ap-southeast-1	14:00–22:00 UTC
Asie-Pacifique (Sydney)	ap-southeast-2	12:00–20:00 UTC
Asie-Pacifique (Tokyo)	ap-northeast-1	13:00–21:00 UTC
Canada (Centre)	ca-central-1	03:00–11:00 UTC
Chine (Pékin)	cn-north-1	06:00–14:00 UTC
Chine (Ningxia)	cn-northwest-1	06:00–14:00 UTC
Europe (Francfort)	eu-central-1	23:00–07:00 UTC
Europe (Irlande)	eu-west-1	22:00–06:00 UTC
Europe (Londres)	eu-west-2	22:00–06:00 UTC
Europe (Paris)	eu-west-3	23:59–07:29 UTC
Europe (Stockholm)	eu-north-1	23:00–07:00 UTC
Moyen-Orient (Bahreïn)	me-south-1	06:00–14:00 UTC
Amérique du Sud (São Paulo)	sa-east-1	00:00–08:00 UTC
AWS GovCloud (US-West)	us-gov-west-1	06:00–14:00 UTC

Ajustement du créneau de maintenance préféré pour une instance de base de données

Le créneau de maintenance doit intervenir au moment où l'utilisation est la plus faible et peut donc nécessiter d'être modifié de temps en temps. Votre instance de base de données sera indisponible pendant ce temps uniquement si des modifications système, telles qu'un changement de classe d'instance de base de données, sont appliquées et nécessitent une interruption, et ce uniquement pendant le délai minimum requis pour apporter les modifications nécessaires.

Dans l'exemple suivant, vous ajustez le créneau de maintenance préféré pour une instance de base de données.

Pour illustrer cet exemple, nous supposons que l'instance DB nommée mydbinstance existe et est associée à un créneau de maintenance préféré comme suit : « Sun:05:00-Sun:06:00 » UTC.

Console

Pour ajuster le créneau de maintenance préféré

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Bases de données, puis sélectionnez l'instance de base de données que vous souhaitez modifier.
3. Sélectionnez Modify. La page Modifier l'instance de base de données s'affiche.
4. Dans la section Maintenance, mettez à jour la fenêtre de maintenance.

   Note

   Le créneau de maintenance et le créneau de sauvegarde de l'instance de base de données ne peuvent pas se chevaucher. Si la valeur que vous entrez pour le créneau de maintenance chevauche le créneau de sauvegarde, un message d'erreur s'affiche.
5. Choisissez Continue.

   Sur la page de confirmation, examinez vos modifications.
6. Pour appliquer immédiatement les modifications à la fenêtre de maintenance, sélectionnez Appliquer immédiatement.
7. Choisissez Modifier l'instance de base de données pour enregistrer vos modifications.

   Sinon, choisissez Retour pour modifier vos modifications, ou choisissez Annuler pour les annuler.

AWS CLI

Pour ajuster le créneau de maintenance préféré, utilisez la commande AWS CLI `modify-db-instance` avec les paramètres suivants :

- `--db-instance-identifier`
- `--preferred-maintenance-window`

Example

L'exemple de code suivant définit le créneau de maintenance sur Tuesdays from 4:00-4:30AM UTC.

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
--db-instance-identifier mydbinstance \
--preferred-maintenance-window Tue:04:00-Tue:04:30
```

Pour Windows :

```
aws rds modify-db-instance ^
--db-instance-identifier mydbinstance ^
--preferred-maintenance-window Tue:04:00-Tue:04:30
```

API RDS

Pour ajuster le créneau de maintenance préféré, utilisez l'opération `ModifyDBInstance` de l'API Amazon RDS avec les paramètres suivants :

- `DBInstanceIdentifier = mydbinstance`
- `PreferredMaintenanceWindow = Tue:04:00-Tue:04:30`

Example

L'exemple de code suivant définit le créneau de maintenance sur Tuesdays from 4:00-4:30AM UTC.

```
https://rds.us-west-2.amazonaws.com/
?Action=ModifyDBInstance
&DBInstanceIdentifier=mydbinstance
&PreferredMaintenanceWindow=Tue:04:00-Tue:04:30
&SignatureMethod=HmacSHA256
&SignatureVersion=4
&Version=2014-09-01
&X-Amz-Algorithm=AWS4-HMAC-SHA256
&X-Amz-Credential=AKIADQKE4SARGYLE/20140425/us-east-1/rds/aws4_request
&X-Amz-Date=20140425T192732Z
&X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
&X-Amz-Signature=1dc9dd716f4855e9bdf188c70f1cf9f6251b070b68b81103b59ec70c3e7854b3
```

Mise à niveau d'une version du moteur d'une instance de base de données

Amazon RDS fournit des versions plus récentes de chaque moteur de base de données pris en charge pour que vous puissiez maintenir à jour votre instance de base de données. Ces versions plus récentes peuvent contenir des correctifs de bogues, des améliorations de sécurité et d'autres améliorations pour le moteur de base de données. Lorsque Amazon RDS prend en charge une nouvelle version d'un moteur de base de données, vous pouvez choisir comment et quand mettre à niveau vos instances de base de données.

Il existe deux types de mises à niveau : les mises à niveau de versions majeures et les mises à niveau de versions mineures. En général, une mise à niveau d'une version majeure du moteur peut introduire des modifications non compatibles avec les applications existantes. En revanche, une mise à niveau de version mineure contient uniquement des modifications rétrocompatibles avec les applications existantes.

La séquence de numérotation des versions est spécifique à chaque moteur de base de données. Par exemple, Amazon RDS MySQL 5.7 et 8.0 sont des versions majeures du moteur et la mise à niveau de la version 5.7 vers la version 8.0 constitue une mise à niveau de version majeure. Amazon RDS MySQL

version 5.7.22 et 5.7.23 sont des versions mineures et la mise à niveau de la version 5.7.22 vers la version 5.7.23 constitue une mise à niveau de version mineure.

Pour plus d'informations sur les mises à niveau de versions majeures et mineures pour un moteur de base de données spécifique, consultez la documentation ci-après correspondant à votre moteur de base de données :

- Mise à niveau du moteur de base de données MariaDB (p. 564)
- Mise à niveau du moteur de base de données Microsoft SQL Server (p. 629)
- Mise à niveau du moteur de base de données MySQL (p. 804)
- Mise à niveau du moteur de base de données Oracle (p. 975)
- Mise à niveau du moteur de base de données PostgreSQL pour Amazon RDS (p. 1373)

Pour les mises à niveau de version majeures, vous devez modifier manuellement la version du moteur de base de données par le biais d'AWS Management Console, de l'AWS CLI ou de l'API RDS. Pour les mises à niveau de versions mineures, vous pouvez modifier manuellement la version du moteur ou choisir d'activer les mises à niveau automatiques des versions mineures.

Rubriques

- Mise à niveau manuelle de la version du moteur (p. 268)
- Mise à niveau automatique de la version mineure du moteur (p. 269)

Mise à niveau manuelle de la version du moteur

Pour mettre manuellement à niveau la version du moteur d'une instance de base de données, vous pouvez utiliser AWS Management Console, l'AWS CLI ou l'API RDS.

Console

Pour mettre à niveau la version du moteur d'une instance de base de données à l'aide de la console

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Bases de données, puis l'instance de base de données que vous souhaitez mettre à niveau.
3. Sélectionnez Modify. La page Modifier l'instance de base de données s'affiche.
4. Dans le champ Version du moteur de base de données, sélectionnez la nouvelle version.
5. Choisissez Continuer et vérifiez le récapitulatif des modifications.
6. Pour appliquer les modifications immédiatement, choisissez Appliquer immédiatement. La sélection de cette option peut entraîner une interruption de service dans certains cas. Pour plus d'informations, consultez Utilisation du paramètre Appliquer immédiatement (p. 244).
7. Sur la page de confirmation, examinez vos modifications. Si elles sont correctes, choisissez Modification d'une instance de base de données pour enregistrer vos modifications.

   Sinon, choisissez Retour pour modifier vos modifications, ou choisissez Annuler pour les annuler.

AWS CLI

Pour mettre à niveau la version du moteur d'une instance de base de données, utilisez la commande modify-db-instance de l'interface de ligne de commande. Spécifiez les paramètres suivants :

- `--db-instance-identifier` – le nom de l'instance de base de données.
- `--engine-version` – numéro de version du moteur de base de données vers lequel effectuer la mise à niveau.

  Pour obtenir des informations sur les versions de moteur valides, utilisez la commande describe-db-engine-versions de l'AWS CLI.
- `--allow-major-version-upgrade` – pour mettre à niveau la version majeure.
- `--no-apply-immediately` – pour appliquer les modifications au cours de la fenêtre de maintenance suivante. Pour appliquer les modifications immédiatement, utilisez `--apply-immediately`.

Example

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --engine-version new_version \
    --allow-major-version-upgrade \
    --no-apply-immediately
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --engine-version new_version ^
    --allow-major-version-upgrade ^
    --no-apply-immediately
```

API RDS

Pour mettre à niveau la version du moteur d'une instance de base de données, utilisez l'action ModifyDBInstance. Spécifiez les paramètres suivants :

- `DBInstanceIdentifier` – nom de l'instance de base de données, par exemple *`mydbinstance`*.
- `EngineVersion` – numéro de version du moteur de base de données vers lequel effectuer la mise à niveau. Pour obtenir des informations sur les versions de moteur valides, utilisez l'opération DescribeDBEngineVersions.
- `AllowMajorVersionUpgrade` – pour autoriser une mise à niveau de version majeure. Pour ce faire, définissez la valeur sur `true`.
- `ApplyImmediately` – si des modifications doivent être appliquées immédiatement ou au cours du prochain créneau de maintenance. Pour appliquer les modifications immédiatement, définissez la valeur sur `true`. Pour appliquer les modifications pendant le créneau de maintenance suivant, définissez la valeur sur `false`.

Mise à niveau automatique de la version mineure du moteur

Une version mineure du moteur est une mise à jour de la version du moteur de base de données au sein d'une version majeure du moteur. Par exemple, une version majeure du moteur peut porter le numéro 9.6 et les versions mineures les numéros 9.6.11 et 9.6.12.

Si vous voulez que Amazon RDS mette automatiquement à niveau la version du moteur d'une base de données, vous pouvez activer les mises à niveau automatiques de versions mineures pour cette base de données.

Lorsque Amazon RDS désigne une version mineure du moteur en tant que version préférée, chaque base de données respectant les conditions suivantes est automatiquement mise à niveau vers cette version mineure :

- La base de données exécute une version mineure du moteur inférieure à la version préférée.
- La mise à niveau automatique des versions mineures est activée pour la base de données.

Vous pouvez vérifier si la mise à niveau automatique des versions mineures est activée pour une instance de base de données lorsque vous effectuez les tâches suivantes :

- Création d'une instance de base de données (p. 146)
- Modification d'une instance de base de données (p. 243)
- Création d'un réplica en lecture (p. 280)
- Restauration d'un d'une instance de base de données à partir d'un instantané (p. 329)
- Restauration d'un instance de base de données à une date déterminée (p. 365)
- Importation d'une instance de base de données à partir de Amazon S3 (p. 821) (pour une sauvegarde MySQL sur Amazon S3)

Lorsque vous effectuez ces tâches, vous pouvez vérifier si la mise à niveau automatique des versions mineures est activée pour l'instance de base de données comme suit :

- À l'aide de la console, définissez l'option Mise à niveau automatique des versions mineures.
- À l'aide de l'AWS CLI, définissez l'option `--auto-minor-version-upgrade|--no-auto-minor-version-upgrade`.
- À l'aide de l'API RDS, définissez le paramètre `AutoMinorVersionUpgrade`.

Pour déterminer si une mise à jour de maintenance (mise à niveau de la version du moteur de base de données, par exemple) est disponible pour votre instance de base de données, vous pouvez utiliser la console, l'AWS CLI ou l'API RDS. Vous pouvez également mettre à niveau la version du moteur de base de données manuellement et ajustez la fenêtre de maintenance. Pour plus d'informations, consultez Entretien d'une instance de base de données (p. 260).

Affectation d'un nouveau nom à une instance DB

Vous pouvez renommer une instance de base de données à l'aide de la AWS Management Console, de la commande `modify-db-instance` de l'AWS CLI ou de l'action d'API Amazon RDS `ModifyDBInstance`. Renommer une instance de base de données peut avoir des effets considérables ; la liste suivante correspond à ce que vous devez savoir avant de renommer une instance de base de données.

- Lorsque vous renommez une instance de base de données, le point de terminaison de l'instance de base de données change, parce que l'URL inclut le nom que vous avez attribué à l'instance de base de données. Vous devez toujours rediriger le trafic de l'ancienne URL vers la nouvelle.
- Lorsque vous renommez une instance de base de données, l'ancien nom DNS qui a été utilisé par l'instance de base de données est immédiatement supprimé, même s'il peut demeurer dans le cache quelques minutes. Le nouveau nom DNS de l'instance de base de données renommée devient effectif au bout de 10 minutes environ. L'instance de base de données renommée n'est pas disponible jusqu'à ce que le nouveau nom ne devienne effectif.
- Vous ne pouvez pas utiliser un nom d'instance de base de données existant lorsque vous renommez une instance.
- Tous les réplicas en lecture associés à une instance de base de données demeurent associés à cette instance une fois qu'elle a été renommée. Par exemple, supposons que vous ayez une instance

de base de données qui traite votre base de données de production et que l'instance ait plusieurs réplicas en lecture associés. Si vous renommez l'instance de base de données, puis la remplacez dans l'environnement de production par un instantané de base de données, l'instance de base de données que vous avez renommée continue de conserver les réplicas en lecture qui lui sont associés.

- Les métriques et les événements associés au nom d'une instance de base de données sont conservés si vous réutilisez un nom d'instance de base de données. Par exemple, si vous effectuez la promotion d'un réplica en lecture et le renommez avec le nom de l'instance de base de données principale précédente, les événements et les métriques associés à l'instance de base de données principale sont associés à l'instance renommée.
- Les balises de l'instance de base de données demeurent avec l'instance de base de données, quel que soit le changement de nom.
- Les snapshots DB sont conservés pour une instance de base de données renommée.

Renommer pour remplacer une instance de base de données existante

Deux raisons principales motivent le fait de renommer une instance de base de données : promouvoir un réplica en lecture ou restaurer des données provenant d'un instantané de bases de données ou d'un PITR. En renommant la base de données, vous pouvez remplacer l'instance de base de données sans avoir à changer un quelconque code d'application qui référence l'instance de base de données. Dans ces cas-là, vous effectuerez les opérations suivantes :

1. Arrêter tout le trafic en direction de l'instance de base de données principale. Cela peut impliquer la redirection du trafic à partir de l'accès aux bases de données sur l'instance de base de données ou toute autre solution que vous voudriez utiliser afin d'empêcher le trafic d'accéder à vos bases de données sur l'instance de base de données.
2. Renommez l'instance de base de données principale avec un nom indiquant qu'elle n'est plus l'instance de base de données principale comme décrit plus loin dans cette rubrique.
3. Créer une instance de base de données principale en la restaurant à partir d'un instantané de base de données ou en promouvant un réplica en lecture, puis attribuer à la nouvelle instance le nom de l'instance de base de données principale précédente.
4. Associer les réplicas en lecture à la nouvelle instance de base de données principale.

Si vous supprimez l'ancienne instance de base de données principale, vous êtes responsable de la suppression des instantanés de base de données indésirables de l'ancienne instance principale.

Pour de plus amples informations sur la promotion d'un réplica en lecture, veuillez consulter Promotion d'un réplica en lecture en instance de bases de données autonome (p. 282).

Console

Pour renommer une instance de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez l'instance de base de données que vous souhaitez renommer.
4. Sélectionnez Modify.
5. Dans Paramètres, saisissez un nouveau nom pour Identifiant de l'instance DB.
6. Choisissez Continue.

7. Pour appliquer les modifications immédiatement, choisissez Appliquer immédiatement. La sélection de cette option peut entraîner une interruption de service dans certains cas. Pour de plus amples informations, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).
8. Sur la page de confirmation, examinez vos modifications. Si elles sont correctes, choisissez Modification d'une instance de base de données pour enregistrer vos modifications.

   Sinon, choisissez Retour pour modifier vos modifications, ou choisissez Annuler pour les annuler.

AWS CLI

Pour renommer une instance de base de données, utilisez la commande `modify-db-instance` de l'AWS CLI. Fournissez la valeur `--db-instance-identifier` actuelle et le paramètre `--new-db-instance-identifier` avec le nouveau nom de l'instance de base de données.

Example

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier DBInstanceIdentifier \
    --new-db-instance-identifier NewDBInstanceIdentifier
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier DBInstanceIdentifier ^
    --new-db-instance-identifier NewDBInstanceIdentifier
```

API RDS

Pour renommer une instance de base de données, appelez la fonction d'API Amazon RDS `ModifyDBInstance` avec les paramètres suivants :

- `DBInstanceIdentifier` = nom existant de l'instance
- `NewDBInstanceIdentifier` = nouveau nom de l'instance

```
https://rds.amazonaws.com/
 ?Action=ModifyDBInstance
 &DBInstanceIdentifier=mydbinstance
 &NewDBInstanceIdentifier=mynewdbinstanceidentifier
 &Version=2012-01-15
 &SignatureVersion=2
 &SignatureMethod=HmacSHA256
 &Timestamp=2012-01-20T22%3A06%3A23.624Z
 &AWSAccessKeyId=<AWS Access Key ID>
 &Signature=<Signature>
```

Redémarrage d'une instance de base de données

Vous pouvez avoir besoin de redémarrer votre instance de bases de données, en général pour des raisons de maintenance. Par exemple, si vous effectuez certaines modifications, ou si vous changez un groupe de paramètres de base de données associé à l'instance de bases de données, ou son , vous devez redémarrer l'instance pour que les modifications prennent effet.

> **Note**
>
> Par exemple, si l'instance de base de données n'utilise pas les dernières modifications apportées à son groupe de paramètres de base de données associé, la AWS Management Console affiche le groupe de paramètres de base de données avec le statut pending-reboot. Le statut de groupe de paramètres pending-reboot n'entraîne pas de redémarrage automatique lors de la fenêtre de maintenance suivante. Pour appliquer les modifications de paramètre les plus récentes de cette instance de base de données, redémarrez-la manuellement. Pour plus d'informations sur les groupes de paramètres, consultez Utilisation de groupes de paramètres de base de données (p. 225).

Le redémarrage d'une instance de base de données entraîne celui du service du moteur de base de données. Le redémarrage d'une instance de bases de données entraîne une interruption momentanée, au cours de laquelle le statut de l'instance de bases de données est défini sur redémarrage.

Si l'instance Amazon RDS est configurée pour Multi-AZ, vous pouvez effectuer le redémarrage. Un événement Amazon RDS est créé lorsque le redémarrage est terminé. Si votre instance de base de données est un déploiement multi-AZ, vous pouvez imposer un basculement d'une zone de disponibilité (AZ) vers une autre lors du redémarrage. Lorsque vous forcez un basculement de votre instance de bases de données, Amazon RDS passe automatiquement sur un réplica de secours dans une autre zone de disponibilité et met à jour l'enregistrement DNS pour que l'instance de bases de données pointe vers l'instance de bases de données de secours. Par conséquent, vous devez nettoyer et rétablir toutes les connexions existantes à votre instance de bases de données. Le redémarrage avec basculement présente un avantage lorsque vous souhaitez simuler une défaillance d'une instance de bases de données à des fins de test, ou restaurer l'AZ d'origine des opérations après un basculement. Pour plus d'informations, consultez Haute disponibilité (multi-AZ) pour Amazon RDS (p. 43).

> **Note**
>
> Lorsque vous forcez un basculement d'une zone de disponibilité à une autre lors d'un démarrage, le changement de zone de disponibilité peut ne pas être reflété dans la AWS Management Console ni dans les appels à l'AWS CLI et à l'API RDS, pendant plusieurs minutes.

Vous ne pouvez pas redémarre votre instance de base de données si elle n'est pas dans l'état Disponible. Votre base de données peut ne pas être disponible pour plusieurs raisons, par exemple une sauvegarde en cours ou une modification demandée précédemment par le client, ou encore une action de créneau de maintenance.

Le temps requis pour redémarrer votre instance de base de données dépend du processus de récupération sur incident, de l'activité de la base de données au moment du redémarrage et du comportement de votre moteur de base de données spécifique. Pour améliorer le délai de redémarrage, nous vous recommandons de réduire l'activité de base de donnée autant que possible pendant le processus de redémarrage. Cela a pour effet de réduire l'activité de restauration pour les transactions en transit.

Pour une instance de base de données avec des réplicas en lecture, vous pouvez redémarrer indépendamment l'instance de base de données source et ses réplicas en lecture. Une fois le redémarrage terminé, la réplication reprend automatiquement.

Console

Pour redémarrer une instance de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Bases de données, puis l'instance de base de données à redémarrer.
3. Pour Actions, choisissez Redémarrer.

   La page Redémarrer l'instance de bases de données s'affiche.

4. (Facultatif) Sélectionnez Redémarrer avec basculement ? pour imposer un basculement d'une zone de disponibilité vers une autre.
5. Choisissez Redémarrer pour redémarrer votre instance de bases de données.

   Sinon, choisissez Annuler.

AWS CLI

Pour redémarrer une instance de bases de données à l'aide de l'AWS CLI, appelez la commande `reboot-db-instance`.

Example Redémarrage simple

Pour Linux, macOS ou Unix :

```
aws rds reboot-db-instance \
    --db-instance-identifier mydbinstance
```

Pour Windows :

```
aws rds reboot-db-instance ^
    --db-instance-identifier mydbinstance
```

Example Redémarrer avec basculement

Pour forcer un basculement d'un AZ à l'autre, utilisez le paramètre `--force-failover`.

Pour Linux, macOS ou Unix :

```
aws rds reboot-db-instance \
    --db-instance-identifier mydbinstance \
    --force-failover
```

Pour Windows :

```
aws rds reboot-db-instance ^
    --db-instance-identifier mydbinstance ^
    --force-failover
```

API RDS

Pour redémarrer une instance de bases de données à l'aide de l'API Amazon RDS, appelez l'action `RebootDBInstance`.

Example Redémarrage simple

```
https://rds.amazonaws.com/
 ?Action=RebootDBInstance
    &DBInstanceIdentifier=mydbinstance
    &Version=2014-10-31
    &X-Amz-Algorithm=AWS4-HMAC-SHA256
    &X-Amz-Credential=AKIADQKE4SARGYLE/20131016/us-west-1/rds/aws4_request
    &X-Amz-Date=20131016T233051Z
    &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
    &X-Amz-Signature=087a8eb41cb1ab5f99e81575f23e73757ffc6a1e42d7d2b30b9cc0be988cff97
```

Example Redémarrer avec basculement

Pour forcer un basculement d'une zone de disponibilité vers une autre, définissez le paramètre `ForceFailover` sur `true`.

```
https://rds.amazonaws.com/
    ?Action=RebootDBInstance
    &DBInstanceIdentifier=mydbinstance
    &ForceFailover=true
    &Version=2014-10-31
    &X-Amz-Algorithm=AWS4-HMAC-SHA256
    &X-Amz-Credential=AKIADQKE4SARGYLE/20131016/us-west-1/rds/aws4_request
    &X-Amz-Date=20131016T233051Z
    &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
    &X-Amz-Signature=087a8eb41cb1ab5f99e81575f23e73757ffc6a1e42d7d2b30b9cc0be988cff97
```

Utilisation des réplicas en lecture

Amazon RDS utilise aussi la fonctionnalité de réplication intégrée des moteurs de base de données MariaDB, MySQL, Oracle, PostgreSQL et Microsoft SQL Server pour créer un type particulier d'instance de base de données appelé réplica en lecture à partir d'une instance de base de données source. L'instance de base de données source devient l'instance de base de données principale. Les mises à jour apportées à l'instance de base de données principale sont copiées de façon asynchrone sur le réplica en lecture. Vous pouvez réduire la charge sur votre instance de base de données principale en acheminant les requêtes en lecture depuis vos applications vers le réplica en lecture. Les réplicas en lecture permettent une montée en puissance basée sur Elastic au-delà des contraintes de capacité d'une seule instance de base de données dans le cas de charges de travail de base de données à lecture intensive.

> **Note**
>
> Les informations suivantes s'appliquent à la création de réplicas en lecture Amazon RDS dans la même région AWS que l'instance de bases de données source ou dans une autre région AWS. Les informations suivantes ne s'appliquent pas à la configuration de la réplication avec une instance qui s'exécute sur une instance Amazon EC2 ou sur site.

Lorsque vous créez un réplica en lecture, vous commencez par spécifier une instance de base de données existante en tant que source. Ensuite, Amazon RDS prend un instantané de l'instance de source et crée une instance en lecture seule à partir de l'instantané. Amazon RDS utilise ensuite la méthode de réplication asynchrone pour le moteur de base de données afin de mettre à jour le réplica en lecture lorsqu'un changement se produit dans l'instance de base de données principale. Le réplica en lecture fonctionne comme une instance de bases de données qui autorise uniquement les connexions en lecture seule. Les applications se connectent à un réplica en lecture de la même façon qu'à toute instance de base de données. Amazon RDS réplique toutes les bases de données dans l'instance de base de données source.

> **Note**
>
> Le moteur Oracle DB prend en charge les bases de données de réplica en mode monté. Un réplica monté n'accepte pas les connexions utilisateur et ne peut donc pas servir de charge de travail en lecture seule. L'utilisation principale des réplicas montés est la reprise après sinistre inter-région. Pour plus d'informations, consultez Utilisation des réplicas Oracle pour Amazon RDS (p. 1003).

Dans certains cas, un réplica en lecture se trouve dans une région AWS différente de celle de son instance de base de données principale. Dans ces cas, Amazon RDS configure un canal de communication sécurisé entre l'instance de base de données principale et un réplica en lecture. Amazon RDS règle toute configuration de sécurité AWS nécessaire pour activer le canal sécurisé, tel que l'ajout des entrées de groupe de sécurité.

Les réplicas en lecture sont pris en charge par les moteurs MariaDB, MySQL, Oracle, PostgreSQL et Microsoft SQL Server. Cette section fournit des informations générales sur l'utilisation des réplicas en lecture avec ces moteurs. Pour de plus amples informations sur l'utilisation de réplicas en lecture avec un moteur spécifique, veuillez consulter les sections suivantes :

- Utilisation de réplicas en lecture MariaDB (p. 574)
- Utilisation des réplicas en lecture pour Microsoft SQL Server dans Amazon RDS (p. 662)
- Utilisation de réplicas en lecture MySQL (p. 851)
- Utilisation des réplicas Oracle pour Amazon RDS (p. 1003)
- Utilisation de réplicas en lecture PostgreSQL dans Amazon RDS (p. 1384)

Présentation des réplicas en lecture Amazon RDS

Le déploiement d'un ou de plusieurs réplicas en lecture pour une instance de bases de données source donnée peut être judicieux dans divers scénarios, notamment dans les suivants :

- Dimensionnement au-delà de la capacité de calcul ou d'E/S d'une instance de bases de données individuelle pour des charges de travail de base de données à lecture intensive. Vous pouvez diriger ce trafic en lecture excessif vers un ou plusieurs réplicas en lecture.
- Service du trafic en lecture alors que l'instance de bases de données source est indisponible. Dans certains, cas, votre instance de bases de données source ne peut pas prendre en charge les demandes d'E/S, par exemple en raison d'une suspension des E/S pour des sauvegardes ou la maintenance planifiée. Vous pouvez alors diriger le trafic de lecture vers vos réplicas en lecture. Dans ce cas d'utilisation, gardez à l'esprit que les données sur le réplica en lecture peuvent être « périmées » car l'instance de bases de données source est indisponible.
- Scénarios de création de rapports commerciaux ou d'entreposage de données, dans lesquels vous pouvez souhaiter que les requêtes de rapports commerciaux s'exécutent sur un réplica en lecture, plutôt que sur votre instance de bases de données de production.
- Mise en œuvre de la reprise après sinistre. Vous pouvez effectuez la promotion d'un réplica en lecture en instance autonome comme plan de reprise après sinistre en cas de défaillance de l'instance de base de données principale.

Par défaut, un réplica en lecture est créé avec le même type de stockage que l'instance de bases de données source. Toutefois, vous pouvez créer un réplica en lecture disposant d'un autre type de stockage que l'instance de bases de données source, en fonction des options répertoriées dans le tableau suivant.

Type de stockage de l'instance de bases de données source	Allocation de stockage d'instance de bases de données source	Options de type de stockage du réplica en lecture
PIOPS	100 Gio–32 Tio	PIOPS, GP2, Standard
GP2	100 Gio–32 Tio	PIOPS, GP2, Standard
GP2	<100 Gio	GP2, Standard
Standard	100 Gio - 6 Tio	PIOPS, GP2, Standard
Standard	<100 Gio	GP2, Standard

Amazon RDS ne prend pas en charge la réplication circulaire. Vous ne pouvez pas configurer une instance de base de données afin de l'utiliser comme source de réplication pour une instance de base de données existante. Vous pouvez uniquement créer un nouveau réplica en lecture à partir d'une instance de base de données existante. Par exemple, si **`MyDBInstance`** est répliqué sur **`ReadReplica1`**, vous ne pouvez pas

configurer **ReadReplica1** de façon à ce qu'il soit répliqué sur **MyDBInstance**. Pour MariaDB et MySQL, vous pouvez créer un réplica en lecture à partir d'un réplica en lecture existant. Par exemple, à partir de **ReadReplica1**, vous pouvez créer un nouveau réplica en lecture, comme **ReadReplica2**. Pour Oracle, PostgreSQL et SQL Server, vous ne pouvez pas créer de réplica en lecture à partir d'un réplica en lecture existant.

Si vous n'avez plus besoin de réplicas en lecture, vous pouvez les supprimer explicitement en utilisant les mêmes mécanismes que pour la suppression d'une instance de base de données. Si vous supprimez une instance de base de données source sans supprimer ses réplicas en lecture dans la même région AWS, chaque réplica en lecture est promu en instance de base de données autonome. Pour de plus amples informations sur la création d'une instance de base de données, veuillez consulter Suppression d'une instance de base de données (p. 313). Pour de plus amples informations sur la promotion d'un réplica en lecture, veuillez consulter Promotion d'un réplica en lecture en instance de bases de données autonome (p. 282). Si vous avez des réplicas en lecture entre régions, veuillez consulter Considérations liées à la réplication entre régions (p. 288) pour connaître les considérations relatives à la suppression de la source d'un réplica en lecture entre régions.

Différences entre les réplicas en lecture pour les différents moteurs de bases de données

Dans la mesure où les moteurs de bases de données Amazon RDS implémentent la réplication différemment, plusieurs différences importantes sont à noter :

Fonction ou comportement	MySQL et MariaDB	Oracle	PostgreSQL	SQL Server
Quelle est la méthode de réplication ?	Réplication logique	Réplication physique	Réplication physique	Réplication physique
Comment les journaux de transactions sont-ils purgés ?	RDS MySQL et RDS MariaDB conservent les journaux binaires qui n'ont pas été appliqués.	Si une instance de base de données principale ne possède aucun réplica en lecture entre régions, Amazon RDS for Oracle conserve un minimum de deux heures de journaux de transactions sur l'instance de base de données source. Les journaux sont purgés de l'instance de base de données source au bout de deux heures ou une fois que le paramètre d'heures de conservation du journal d'archive est passé, le plus long des deux. Les journaux sont purgés du réplica en lecture une fois que le paramètre d'heures	PostgreSQL dispose du paramètre `wal_keep_segments`, qui indique le nombre de fichiers WAL (write-ahead log) à conserver pour fournir les données aux réplicas en lecture. La valeur de ce paramètre spécifie le nombre de journaux à conserver.	Le fichier journal virtuel (VLF) du fichier journal des transactions sur le réplica principal peut être tronqué une fois qu'il n'est plus nécessaire pour les réplicas secondaires. Le VLF ne peut être marqué comme inactif que lorsque les enregistrements de journaux ont été sécurisés

Fonction ou comportement	MySQL et MariaDB	Oracle	PostgreSQL	SQL Server
		de conservation du journal d'archive est passé, uniquement s'ils ont été appliqués correctement à la base de données. Dans certains cas, une instance de base de données principale peut avoir un ou plusieurs réplicas en lecture entre régions. Dans ce cas, Amazon RDS for Oracle conserve les journaux de transaction sur l'instance de base de données source jusqu'à ce qu'ils aient été transmis et appliqués à tous les réplicas en lecture entre régions. Pour de plus amples informations sur la définition des heures de conservation des journaux d'archivage, veuillez consulter Conservation des journaux redo archivés (p. 1134).		dans les réplicas. Quelle que soit la vitesse à laquelle les sous-systèmes de disque se trouvent dans le réplica principal, le journal des transactions conserve les VLF jusqu'à ce que le réplica le plus lent l'ait sécurisé.

Fonction ou comportement	MySQL et MariaDB	Oracle	PostgreSQL	SQL Server
Est-il possible de rendre un réplica accessible en écriture ?	Oui. Vous pouvez permettre au réplica en lecture MySQL ou MariaDB d'être accessible en écriture.	Non. Un réplica en lecture Oracle est une copie physique et Oracle n'autorise pas les écritures dans un réplica en lecture. Vous pouvez promouvoir un réplica en lecture afin de le rendre inscriptible. Le réplica en lecture promu a les données répliquées jusqu'au moment où la demande a été faite pour le promouvoir.	Non. Un réplica en lecture PostgreSQL est une copie physique et PostgreSQL ne permet pas de rendre accessible en écriture un réplica en lecture.	Non. Un réplica en lecture SQL Server est une copie physique et n'autorise pas les écritures. Vous pouvez promouvoir un réplica en lecture afin de le rendre inscriptible. Le réplica en lecture promu a les données répliquées jusqu'au moment où la demande a été faite pour le promouvoir.
Des sauvegardes peuvent-elles être effectuées sur le réplica ?	Oui. Vous pouvez autoriser des sauvegardes automatiques sur un réplica en lecture MySQL ou MariaDB.	Non. Vous ne pouvez pas créer d'instantanés manuels de Amazon RDS pour les réplicas en lecture Oracle ni activer les sauvegardes automatiques pour eux.	Oui, vous pouvez créer un instantané manuel d'un réplica en lecture PostgreSQL, mais vous ne pouvez pas activer les sauvegardes automatiques.	Non. Vous ne pouvez pas créer d'instantanés manuels de Amazon RDS pour les réplicas en lecture SQL Server ni activer les sauvegardes automatiques pour eux.
Est-il possible d'utiliser la réplication parallèle ?	Oui. MySQL versions 5.6 et ultérieures, ainsi que toutes les versions de MariaDB prises en charge autorisent les threads de réplication parallèles.	Oui. Les données des journaux redo sont toujours transmises en parallèle de la base de données principale vers tous ses réplicas en lecture.	Non. PostgreSQL dispose d'un processus unique de réplication.	Oui. Les données des journaux redo sont toujours transmises en parallèle de la base de données principale vers tous ses réplicas en lecture.

Fonction ou comportement	MySQL et MariaDB	Oracle	PostgreSQL	SQL Server
Pouvez-vous maintenir un réplica dans un état monté plutôt qu'en lecture seule ?	Non.	Oui. L'utilisation principale des réplicas montés est la reprise après sinistre inter-région. Une licence Active Data Guard n'est pas requise pour les réplicas montés. Pour plus d'informations, consultez Utilisation des réplicas Oracle pour Amazon RDS (p. 1003).	Non.	Non.

Création d'un réplica en lecture

Vous pouvez créer un réplica en lecture à partir d'une instance de base de données MySQL, MariaDB, Oracle, PostgreSQL ou SQL Server existante à l'aide de l'AWS Management Console, de l'AWS CLI ou de l'API RDS. Vous créez un réplica en lecture en spécifiant `SourceDBInstanceIdentifier`, qui est l'identifiant de l'instance de base de données source à partir de laquelle vous souhaitez répliquer les données.

Lorsque vous créez un réplica en lecture, Amazon RDS prend un instantané de votre instance de base de données source et commence la réplication. En conséquence, vous connaissez une brève suspension des E/S sur votre instance de base de données source pendant la réalisation de l'instantané de base de données. La suspension d'E/S dure généralement environ une minute. Vous pouvez éviter la suspension d'E/S si l'instance de base de données source est un déploiement multi-AZ, car dans ce cas l'instantané est pris à partir de l'instance de base de données secondaire. Une transaction de longue durée active peut ralentir le processus de création du réplica en lecture. Nous vous recommandons d'attendre que les transactions de longue durée se terminent pour créer un réplica en lecture. Si vous créez plusieurs réplicas en lecture en parallèle à partir de la même instance de base de données source, Amazon RDS prend un seul instantané au début de la première action de création.

Lors de la création d'un réplica en lecture, il convient de prendre en considération plusieurs éléments. Tout d'abord, vous devez activer les sauvegardes automatiques sur l'instance de bases de données source en affectant à la période de rétention des sauvegardes une valeur différente de 0. Cette exigence s'applique également à un réplica en lecture qui serait l'instance de base de données source d'un autre réplica en lecture. Pour les instances de base de données MySQL, les sauvegardes automatiques sont prises en charge uniquement pour les réplicas en lecture exécutant une version de MySQL 5.6 ou ultérieure, mais non pour les versions de MySQL 5.5. Pour activer les sauvegardes automatiques sur un réplica en lecture Amazon RDS MySQL version 5.6 ou ultérieure, commencez par créer le réplica en lecture, puis modifiez-le pour activer les sauvegardes automatiques.

> Note
>
> Dans une région AWS, nous vous recommandons fortement de créer tous les réplicas en lecture dans le même Virtual Private Cloud (VPC) basé sur Amazon VPC en tant qu'instance de base de données source. Si vous créez un réplica en lecture dans un VPC différent de l'instance de base de données source, les plages d'adresses CIDR (classless inter-domain routing) peuvent se chevaucher entre le réplica et le système RDS. Le chevauchement CIDR rend le réplica instable, ce qui peut avoir un impact négatif sur les applications qui s'y connectent. Si vous recevez une erreur lors de la création du réplica en lecture, choisissez un autre groupe de sous-réseaux de

base de données de destination. Pour de plus amples informations, veuillez consulter Utilisation d'une instance de base de données dans un VPC (p. 1620).
Vous ne pouvez pas créer de réplica en lecture dans un compte AWS différent à partir de l'instance de base de données source.

Console

Pour créer un réplica en lecture à partir d'une instance de base de données MySQL, MariaDB, Oracle, PostgreSQL ou SQL Server source

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez l'instance de base de données MySQL, MariaDB, Oracle, PostgreSQL ou SQL Server que vous souhaitez utiliser comme source pour un réplica en lecture.
4. Sous Actions, choisissez Créer des réplicas en lecture.
5. Sous Identifiant de l'instance DB, saisissez un nom pour le réplica en lecture.
6. Choisissez les spécifications de votre instance. Nous vous recommandons d'utiliser le même type de stockage et la même classe d'instance de base de données que l'instance de base de données source pour le réplica en lecture.
7. Pour Déploiement Multi-AZ, choisissez Oui afin de créer une instance de secours de votre réplica dans une autre zone de disponibilité pour la prise en charge du basculement pour le réplica.

   Note

   La création de votre réplica en lecture en tant qu'instance de base de données multi-AZ est indépendante du fait que la base de données source soit ou non une instance de base de données multi-AZ.
8. Pour créer un réplica en lecture chiffré :
   a. Choisissez Activer le chiffrement.
   b. Pour Clé principale, choisissez l'identifiant de clé AWS Key Management Service (AWS KMS) de la clé CMK.

   Note

   L'instance de base de données source doit être chiffrée. Pour en savoir plus sur le chiffrement de l'instance de bases de données source, consultez Chiffrement des ressources Amazon RDS (p. 1522).
9. Choisissez les autres paramètres que vous voulez utiliser.
10. Choisissez Créer un réplica en lecture.

AWS CLI

Pour créer un réplica en lecture à partir d'une instance de base de données source MySQL, MariaDB, Oracle, PostgreSQL ou SQL Server, utilisez la commande `create-db-instance-read-replica` de l'AWS CLI.

Example

Pour Linux, macOS ou Unix :

```
aws rds create-db-instance-read-replica \
```

```
    --db-instance-identifier myreadreplica \
    --source-db-instance-identifier mydbinstance
```

Pour Windows :

```
aws rds create-db-instance-read-replica ^
    --db-instance-identifier myreadreplica ^
    --source-db-instance-identifier mydbinstance
```

API RDS

Pour créer un réplica en lecture à partir d'une instance de bases de données MySQL, MariaDB, Oracle, PostgreSQL ou SQL Server source, appelez la fonction d'API Amazon RDS `CreateDBInstanceReadReplica`.

```
https://rds.amazonaws.com/
 ?Action=CreateDBInstanceReadReplica
 &DBInstanceIdentifier=myreadreplica
 &SourceDBInstanceIdentifier=mydbinstance
 &Version=2012-01-15
 &SignatureVersion=2
 &SignatureMethod=HmacSHA256
 &Timestamp=2012-01-20T22%3A06%3A23.624Z
 &AWSAccessKeyId=<AWS Access Key ID>
 &Signature=<Signature>
```

Promotion d'un réplica en lecture en instance de bases de données autonome

Vous pouvez promouvoir un réplica en lecture MySQL, MariaDB, Oracle, PostgreSQL ou SQL Server en une instance de base de données autonome. Lorsque vous effectuez la promotion d'un réplica en lecture, l'instance de bases de données est redémarrée avant de devenir disponible.

Il existe plusieurs raisons pour lesquelles vous pouvez souhaiter promouvoir un réplica en lecture en une instance de base de données autonome :

- Exécution d'opérations DDL (MySQL et MariaDB uniquement) – Les opérations DDL, telles que la création ou la reconstruction d'index, peuvent prendre du temps et imposer une pénalité importante de performances à votre instance de base de données. Vous pouvez exécuter ces opérations sur un réplica en lecture MySQL ou MariaDB une fois que ce réplica en lecture est synchronisé avec son instance de bases de données principale. Ensuite, vous pouvez promouvoir le réplica en lecture et indiquer à vos applications d'utiliser l'instance promue.
- Partitionnement – Le partitionnement incarne l'architecture « ne rien partager » et implique essentiellement la décomposition d'une grande base de données en plusieurs bases de données plus petites. Pour fractionner une base de données, l'une des méthodes consiste à fractionner les tables qui ne sont pas jointes dans la même requête sur différents hôtes. L'autre méthode consiste à dupliquer une table entre plusieurs hôtes, puis à utiliser un algorithme de hachage pour déterminer l'hôte qui reçoit une mise à jour donnée. Vous pouvez créer des réplicas en lecture correspondant à chacune de vos partitions (bases de données plus petites) et les promouvoir quand vous décidez de les convertir en partitions autonomes. Vous pouvez alors extraire l'espace clé (si vous fractionnez les lignes) ou la distribution des tables pour chaque partitionnement selon vos besoins.
- Implémentation d'une récupération en cas de défaillance – Vous pouvez utiliser la promotion de réplica en lecture comme plan de récupération de données en cas de défaillance de l'instance de base de données principale. Cette approche complète la réplication synchrone, la détection automatique d'échec et le basculement.

Si vous êtes conscient des ramifications et des limitations de la réplication asynchrone et que vous souhaitez toujours utiliser la promotion de réplica en lecture pour la récupération des données, vous pouvez le faire. Pour cela, commencez par créer un réplica en lecture, puis surveillez l'instance de base de données principale pour détecter les pannes. En cas de panne, procédez comme suit :

1. Promouvez le réplica en lecture.
2. Dirigez le trafic de base de données vers l'instance de bases de données promue.
3. Créez un réplica en lecture de remplacement avec l'instance de base de données promue comme source.

Lorsque vous effectuez la promotion d'un réplica en lecture, la nouvelle instance de base de données qui est créée conserve la période de rétention des sauvegardes, la fenêtre de sauvegarde et le groupe de paramètres de l'ancienne source de réplica en lecture. Le processus de promotion peut prendre plusieurs minutes ou plus longtemps, selon la taille du réplica en lecture. Une fois le réplica en lecture promu en une nouvelle instance de base de données, il est similaire à toute autre instance de base de données. Par exemple, vous pouvez créer des réplicas en lecture à partir de la nouvelle instance de base de données et effectuer des opérations de restauration à un moment donné. Comme l'instance de bases de données promue n'est plus un réplica en lecture, vous ne pouvez pas l'utiliser comme cible de réplication. Si une instance de base de données source possède plusieurs réplicas en lecture, la promotion d'un des réplicas en lecture en instance de base de données n'a aucun effet sur les autres réplicas.

La durée de la sauvegarde dépend du nombre de modifications apportées à la base de données depuis la dernière sauvegarde. Si vous souhaitez promouvoir un réplica en lecture en instance autonome, nous vous recommandons d'activer les sauvegardes et d'en effectuer au moins une avant la promotion. En outre, vous ne pouvez pas promouvoir un réplica en lecture en une instance autonome lorsque son état est `backing-up`. Si vous avez activé des sauvegardes sur votre réplica en lecture, configurez la fenêtre de sauvegarde automatique afin que les sauvegardes quotidiennes n'interfèrent pas avec la promotion du réplica en lecture.

Les étapes suivantes montrent le processus général de promotion d'un réplica en lecture en instance de base de données :

1. Arrêtez l'écriture de toute transaction sur l'instance de base de données principale, puis attendez que toutes les mises à jour soient effectuées sur le réplica en lecture. Les mises à jour de la base de données ont lieu sur les réplica en lecture après avoir eu lieu sur l'instance de base de données principale, et cette latence de réplication peut varier de façon significative. Utilisez la métrique `Replica Lag` pour déterminer à quel moment toutes les mises à jour ont été effectuées sur le réplica en lecture.
2. Pour MySQL et MariaDB uniquement : si vous avez besoin d'apporter des modifications au réplica en lecture MySQL ou MariaDB, vous devez affecter au paramètre `read_only` la valeur `0` dans le groupe de paramètres de base de données du réplica en lecture. Vous pouvez alors effectuer toutes les opérations DDL requises, telles que la création d'index, sur le réplica en lecture. Les actions entreprises sur le réplica en lecture n'affectent pas la performance de l'instance de base de données principale.
3. Promouvez le réplica en lecture en utilisant l'option Promouvoir sur la console Amazon RDS, la commande de l'AWS CLI `promote-read-replica` ou l'opération d'API Amazon RDS `PromoteReadReplica`.

   Note

   Le processus de promotion dure quelques minutes. Lorsque vous promouvez un réplica en lecture, la réplication est arrêtée et le réplica en lecture est redémarré. Une fois le redémarrage terminé, le réplica en lecture est disponible en tant que nouvelle instance de base de données.
4. (Facultatif) Modifiez la nouvelle instance de base de données pour en faire un déploiement multi-AZ. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243) et Haute disponibilité (multi-AZ) pour Amazon RDS (p. 43).

Console

Pour promouvoir un réplica en lecture en instance de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la console Amazon RDS, choisissez Bases de données.

   Le volet Bases de données s'affiche. Chaque réplica en lecture affiche Réplica dans la colonne Rôle.
3. Choisissez le réplica en lecture que vous voulez promouvoir.
4. Pour Actions, choisissez Promote (Promouvoir).
5. Dans la page Promouvoir le réplica en lecture, saisissez la période de rétention des sauvegardes et la fenêtre de sauvegarde pour l'instance de base de données nouvellement promue.
6. Lorsque les paramètres vous conviennent, choisissez Continue.
7. Dans la page de confirmation, choisissez Promouvoir le réplica en lecture.

AWS CLI

Pour promouvoir un réplica en lecture en instance de base de données, utilisez la commande `promote-read-replica` de l'AWS CLI.

Example

Pour Linux, macOS ou Unix :

```
aws rds promote-read-replica \
    --db-instance-identifier myreadreplica
```

Pour Windows :

```
aws rds promote-read-replica ^
    --db-instance-identifier myreadreplica
```

API RDS

Pour promouvoir un réplica en lecture en instance de base de données, appelez `PromoteReadReplica`.

```
https://rds.amazonaws.com/
 ?Action=PromoteReadReplica
 &DBInstanceIdentifier=myreadreplica
 &Version=2012-01-15
 &SignatureVersion=2
 &SignatureMethod=HmacSHA256
 &Timestamp=2012-01-20T22%3A06%3A23.624Z
 &AWSAccessKeyId=<AWS Access Key ID>
 &Signature=<Signature>
```

Création d'un réplica en lecture dans une autre région AWS

Avec Amazon RDS, vous pouvez créer un réplica en lecture MariaDB, MySQL, Oracle ou PostgreSQL dans une autre région AWS à partir de l'instance de base de données source. La création d'un réplica en lecture entre plusieurs régions n'est pas prise en charge pour SQL Server sur Amazon RDS.

Vous créez un réplica en lecture dans une autre région AWS pour effectuer les opérations suivantes :

- Améliorer vos capacités de reprise après sinistre.
- Mettre à l'échelle des opérations de lecture dans une région AWS plus proche de vos utilisateurs.
- Faciliter la migration d'un centre de données d'une région AWS vers un centre de données d'une autre région AWS.

La création d'un réplica en lecture dans une région AWS différente de celle de l'instance source est similaire à la création d'un réplica dans la même région AWS. Vous pouvez utiliser l'AWS Management Console, exécuter la commande `create-db-instance-read-replica` ou appeler l'opération d'API `CreateDBInstanceReadReplica`.

Pour que vous puissiez créer un réplica en lecture chiffré dans une autre région AWS à partir de l'instance de base de données source, cette instance de base de données source doit être chiffrée.

Les réplicas en lecture entre régions ne sont pas pris en charge dans les régions d'adhésion AWS suivantes :

- Afrique (Le Cap)
- Asie-Pacifique (Hong Kong)
- Europe (Milan)
- Moyen-Orient (Bahreïn)

Les procédures suivantes expliquent comment créer un réplica en lecture à partir d'une instance de base de données MariaDB, MySQL, Oracle ou PostgreSQL source dans une autre région AWS.

Console

Vous pouvez créer un réplica en lecture entre régions AWS à l'aide de l'AWS Management Console.

Pour créer un réplica en lecture entre régions AWS avec la console

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez l'instance de base de données MariaDB, MySQL, Oracle ou PostgreSQL que vous souhaitez utiliser comme source pour un réplica en lecture.
4. Sous Actions, choisissez Créer des réplicas en lecture.
5. Sous Identifiant de l'instance DB, saisissez un nom pour le réplica en lecture.
6. Choisissez la région de destination.
7. Choisissez les spécifications de l'instance que vous souhaitez utiliser. Nous vous recommandons d'utiliser le même type de stockage et la même classe d'instance de base de données pour le réplica en lecture.
8. Pour créer un réplica en lecture chiffré dans une autre région AWS :

   a. Choisissez Activer le chiffrement.
   b. Pour Clé principale, choisissez l'identifiant de clé AWS Key Management Service (AWS KMS) de la clé CMK de la région AWS de destination.

   > **Note**
   >
   > L'instance de base de données source doit être chiffrée pour que vous puissiez créer un réplica en lecture chiffré. Pour en savoir plus sur le chiffrement de l'instance de bases de données source, consultez Chiffrement des ressources Amazon RDS (p. 1522).
9. Choisissez les autres paramètres que vous voulez utiliser.

10. Choisissez Créer un réplica en lecture.

AWS CLI

Pour créer un réplica en lecture à partir d'une instance de base de données MySQL, MariaDB, Oracle ou PostgreSQL source dans une autre région AWS, vous pouvez utiliser la commande `create-db-instance-read-replica`. Dans ce cas, vous utilisez `create-db-instance-read-replica` à partir de la région AWS où vous voulez placer le réplica en lecture et vous spécifiez l'Amazon Resource Name (ARN) pour l'instance de base de données source. Un ARN identifie de façon unique une ressource créée dans Amazon Web Services.

Par exemple, si votre instance de base de données se trouve dans la région USA Est (Virginie du Nord), l'ARN ressemble à l'exemple suivant :

```
arn:aws:rds:us-east-1:123456789012:db:my-mysql-instance
```

Pour en savoir plus sur les ARN, consultez Utilisation des Amazon Resource Names (ARN) dans Amazon RDS (p. 298).

Pour créer un réplica en lecture chiffré dans une autre région AWS que l'instance de base de données source, vous pouvez utiliser la commande AWS CLI `create-db-instance-read-replica` de la région AWS destinataire. Les paramètres suivants sont utilisés pour créer un réplica en lecture chiffré dans une autre région AWS :

- `--source-region` — La région AWS dans laquelle le réplica en lecture chiffré est créé. Si `source-region` n'est pas spécifié, vous devez spécifier une valeur `pre-signed-url`. Une valeur `pre-signed-url` est une URL qui contient une demande signée via Signature Version 4 pour l'opération `CreateDBInstanceReadReplica` qui est appelée dans la région AWS source à partir de laquelle le réplica en lecture est créé. Pour de plus amples informations sur `pre-signed-url`, veuillez consulter `CreateDBInstanceReadReplica`.
- `--source-db-instance-identifier` — L'identifiant d'instance de base de données du réplica en lecture chiffré qui est créé. Cet identifiant doit être au format de nom ARN pour la région AWS source. La région AWS spécifiée dans `source-db-instance-identifier` doit correspondre à la région AWS spécifiée en tant que `source-region`.
- `--db-instance-identifier` — L'identifiant du réplica en lecture chiffré dans la région AWS de destination.
- `--kms-key-id` — L'identifiant de clé AWS KMS pour la clé principale client (CMK) à utiliser pour chiffrer le réplica en lecture dans la région AWS de destination.

Le code suivant crée un réplica en lecture dans la région `us-west-2`.

Example

Pour Linux, macOS ou Unix :

```
aws rds create-db-instance-read-replica \
    --db-instance-identifier DBInstanceIdentifier \
    --region us-west-2 \
    --source-db-instance-identifier arn:aws:rds:us-east-1:123456789012:db:my-mysql-instance
```

Pour Windows :

```
aws rds create-db-instance-read-replica ^
    --db-instance-identifier DBInstanceIdentifier ^
    --region us-west-2 ^
```

```
    --source-db-instance-identifier arn:aws:rds:us-east-1:123456789012:db:my-mysql-instance
```

Le code suivant crée un réplica en lecture dans une autre région AWS que celle de l'instance de base de données source. La région AWS où vous appelez la commande `create-db-instance-read-replica` correspond à la région AWS de destination du réplica en lecture chiffré.

Example

Pour Linux, macOS ou Unix :

```
aws rds create-db-instance-read-replica \
    --db-instance-identifier DBInstanceIdentifier \
    --region us-west-2 \
    --source-db-instance-identifier arn:aws:rds:us-east-1:123456789012:db:my-mysql-instance
 \
    --source-region us-east-1 \
    --kms-key-id my-us-east-1-key
```

Pour Windows :

```
aws rds create-db-instance-read-replica ^
    --db-instance-identifier DBInstanceIdentifier ^
    --region us-west-2 ^
    --source-db-instance-identifier arn:aws:rds:us-east-1:123456789012:db:my-mysql-instance
 ^
    --source-region us-east-1 ^
    --kms-key-id my-us-east-1-key
```

API RDS

Pour créer un réplica en lecture à partir d'une instance de base de données MySQL, MariaDB, Oracle ou PostgreSQL source dans une autre région AWS, vous pouvez appeler la fonction d'API Amazon RDS CreateDBInstanceReadReplica. Dans ce cas, vous appelez CreateDBInstanceReadReplica à partir de la région AWS où vous voulez placer le réplica en lecture et vous spécifiez l'Amazon Resource Name (ARN) pour l'instance de base de données source. Un ARN identifie de façon unique une ressource créée dans Amazon Web Services.

Pour créer un réplica en lecture chiffré dans une autre région AWS que celle de l'instance de base de données source, vous pouvez utiliser l'opération d'API Amazon RDS `CreateDBInstanceReadReplica` de la région AWS destinataire. Pour créer un réplica en lecture chiffré dans une autre région AWS, vous devez spécifier une valeur pour `PreSignedURL`. `PreSignedURL` doit contenir une demande pour l'opération `CreateDBInstanceReadReplica` à appeler dans la région AWS source dans laquelle le réplica en lecture est créé. Pour en savoir plus sur `PreSignedUrl`, consultez `CreateDBInstanceReadReplica`.

Par exemple, si votre instance de bases de données se trouve dans la région USA Est (Virginie du Nord), l'ARN ressemble à ce qui suit.

```
arn:aws:rds:us-east-1:123456789012:db:my-mysql-instance
```

Pour en savoir plus sur les ARN, consultez Utilisation des Amazon Resource Names (ARN) dans Amazon RDS (p. 298).

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%253D CreateDBInstanceReadReplica
         %2526DestinationRegion%253Dus-east-1
         %2526KmsKeyId%253Dmy-us-east-1-key
         %2526SourceDBInstanceIdentifier%253Darn%25253Aaws%25253Ards%25253Aus-
west-2%1234567890
12%25253Adb%25253Amy-mysql-instance
         %2526SignatureMethod%253DHmacSHA256
         %2526SignatureVersion%253D4%2526SourceDBInstanceIdentifier%253Darn%25253Aaws
%25253Ards%25253Aus-west-2%25253A123456789012%25253Ainstance%25253Amysql-instance1-
instance-20161115
         %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=arn:aws:rds:us-east-1:123456789012:db:my-mysql-instance
    &Version=2012-01-15
    &SignatureVersion=2
    &SignatureMethod=HmacSHA256
    &Timestamp=2012-01-20T22%3A06%3A23.624Z
    &AWSAccessKeyId=<AWS Access Key ID>
    &Signature=<Signature>
```

Considérations liées à la réplication entre régions

Toutes les considérations liées à la réplication au sein d'une région AWS s'appliquent à la réplication entre régions. Les considérations supplémentaires suivantes s'appliquent lors d'une réplication entre régions AWS :

- Vous pouvez uniquement répliquer entre des régions AWS lorsque vous utilisez les instances de base de données Amazon RDS suivantes.
  - MariaDB (toutes les versions).
  - MySQL version 5.6 et supérieures.
  - Oracle Enterprise Edition (EE) version moteur 12.1.0.2.v10 et versions 12.1 supérieures, toutes les versions de 12.2 et toutes les versions de 18.0.

    Une licence Active Data Guard est obligatoire. Pour de plus amples informations sur les limites des réplicas en lecture entre régions Oracle, veuillez consulter Exigences de réplica pour Oracle (p. 1004).
  - PostgreSQL (toutes versions).
- Une instance de bases de données source peut avoir des réplicas en lecture entre régions dans plusieurs régions AWS.
- Vous ne pouvez créer un réplica en lecture entre régions Amazon RDS qu'à partir d'une instance de base de données Amazon RDS qui n'est pas un réplica en lecture d'une autre instance de base de données Amazon RDS.
- Vous ne pouvez pas configurer un canal de réplication à l'intérieur ou à l'extérieur de la région AWS GovCloud (US-West).
- Vous pouvez vous attendre à un degré supérieur de latence pour tout réplica en lecture figurant dans une autre région AWS que celle de l'instance source. Cette latence vient des canaux de réseau plus longs entre les centres de données régionaux.

- Pour ces réplicas en lecture entre régions, toutes les commandes de création de réplica en lecture qui spécifient le paramètre `--db-subnet-group-name` doivent spécifier un groupe de sous-réseaux DB du même VPC.
- Vous pouvez créer un réplica en lecture entre régions :
  - Dans un VPC à partir d'une instance de base de données source se trouvant dans un VPC d'une autre région AWS
  - Dans un VPC à partir d'une instance de base de données source ne se trouvant pas dans un VPC
  - En dehors d'un VPC à partir d'une instance de base de données source se trouvant dans un VPC
- En raison de la limite du nombre d'entrées de liste de contrôle d'accès (ACL) pour un VPC, nous ne pouvons pas garantir plus de cinq instances de réplica en lecture inter-régions.
- Le réplica en lecture utilise le groupe de paramètres de base de données par défaut pour le moteur de base de données spécifié.
- Le réplica en lecture utilise le groupe de sécurité par défaut.
- Pour les instances de base de données MariaDB, MySQL et Oracle, lorsque la source d'un réplica en lecture entre régions est supprimée, le réplica en lecture est promu.
- Pour les instances de base de données PostgreSQL, lorsque la source d'un réplica en lecture entre régions est supprimée, le statut de réplication du réplica en lecture est défini sur `terminated`. Le réplica en lecture n'est pas promu.

Coûts de la réplication entre régions

Les données transférées pour la réplication entre régions génèrent des frais de transfert de données Amazon RDS. Ces actions de réplication entre régions génèrent des frais pour les données transférées hors de la région AWS source :

- Lorsque vous créez un réplica en lecture, Amazon RDS prend un instantané de l'instance source et transfère cet instantané vers la région AWS du réplica en lecture.
- Pour chaque modification des données effectuée dans les bases de données source, Amazon RDS transfère les données de la région AWS source vers la région AWS du réplica en lecture.

Pour de plus amples informations sur la tarification du transfert des données, veuillez consulter la Tarification Amazon RDS.

Pour les instances MySQL et MariaDB, vous pouvez réduire les coûts de transfert de données en réduisant le nombre de réplicas en lecture entre régions que vous créez. Par exemple, supposons si vous possédiez une instance de base de données source dans une région AWS et que vous souhaitiez disposer de trois réplicas en lecture dans une autre région AWS. Dans ce cas, vous créez uniquement l'un des réplicas en lecture à partir de l'instance de base de données source. Ensuite, vous créez les deux autres réplicas à partir du premier réplica en lecture plutôt qu'à partir de l'instance de base de données source.

Par exemple, si vous avez `source-instance-1` dans une région AWS, vous pouvez procéder comme suit :

- Créez `read-replica-1` dans la nouvelle région AWS en spécifiant `source-instance-1` comme source.
- Créez `read-replica-2` à partir de `read-replica-1`.
- Créez `read-replica-3` à partir de `read-replica-1`.

Dans cet exemple, seules les données transférées de `source-instance-1` vers `read-replica-1` vous sont facturées. Les données transférées de `read-replica-1` vers les deux autres réplicas ne vous sont pas facturées, car ils figurent tous dans la même région AWS. Si vous créez les trois réplicas directement à partir de `source-instance-1`, les transferts de données vers les trois réplicas vous sont facturés.

Processus de réplication entre régions au sein d'Amazon RDS

Amazon RDS utilise le processus ci-dessous pour créer un réplica en lecture entre régions. Selon les régions AWS impliquées et le volume de données figurant dans les bases de données, ce processus peut durer des heures. Vous pouvez utiliser ces informations pour déterminer l'avancement du processus lorsque vous créez un réplica en lecture entre régions :

1. Amazon RDS commence par configurer l'instance DB source comme source de réplication et définit le statut sur modifying (modification).
2. Amazon RDS commence à configurer le réplica en lecture spécifié dans la région AWS destinataire et définit le statut sur creating (création).
3. Amazon RDS crée un instantané de base de données automatisé de l'instance de bases de données source dans la région AWS source. Le format du nom de l'instantané de base de données est : `rds:<InstanceID>-<timestamp>`, où `<InstanceID>` est l'identifiant de l'instance source, et `<timestamp>` est la date et l'heure du début de la copie. Par exemple, `rds:mysourceinstance-2013-11-14-09-24` a été créé à partir de l'instance `mysourceinstance` le `2013-11-14-09-24`. Pendant la création de l'instantané de base de données automatique, le statut de l'instance de base de données source reste modifying (modification), le statut du réplica en lecture reste creating (création) et le statut de l'instantané de base de données est creating (création). La colonne d'avancement de la page de l'instantané de base de données dans la console indique le niveau d'avancement de la création de l'instantané de base de données. Une fois l'instantané de base de données terminé, le statut de l'instantané de base de données et celui de l'instance de base de données source sont définis sur available (disponible).
4. Amazon RDS commence une copie de l'instantané entre régions pour le transfert de données initial. La copie de l'instantané est répertoriée en tant qu'instantané automatisé dans la région AWS destinataire avec un statut creating (création). Elle porte le même nom que l'instantané de base de données source. La colonne d'avancement de l'affichage de l'instantané de base de données indique le niveau d'avancement de la copie. Une fois la copie terminée, le statut de la copie de l'instantané de base de données est défini sur available (disponible).
5. Amazon RDS utilise alors l'instantané de base de données copié pour le chargement initial des données sur le réplica en lecture. Au cours de cette phase, le réplica en lecture figure dans la liste des instances de bases de données de la destination, avec le statut creating (création). Une fois le chargement terminé, le statut du réplica en lecture est défini sur available (disponible) et la copie de l'instantané de base de données est supprimée.
6. Lorsque le réplica en lecture atteint le statut disponible, Amazon RDS commence par répliquer les modifications apportées à l'instance source depuis le début de l'opération de création du réplica en lecture. Durant cette phase, la durée du retard de réplication pour le réplica en lecture est supérieure à 0.

   Pour de plus amples informations sur la durée du retard de réplication, veuillez consulter Supervision de la réplication en lecture (p. 291).

Exemples de réplication entre régions

Example Création d'un réplica en lecture entre régions en dehors de tout VPC

L'exemple suivant illustre la création d'un réplica en lecture dans la région us-west-2 à partir d'une instance de base de données source dans la région us-east-1. Ce réplica en lecture est créé en dehors de tout VPC :

Pour Linux, macOS ou Unix :

```
aws rds create-db-instance-read-replica \
    --db-instance-identifier SimCoProd01Replica01 \
    --region us-west-2
```

```
    --source-db-instance-identifier arn:aws:rds:us-east-1:123456789012:db:SimcoProd01
```

Pour Windows :

```
aws rds create-db-instance-read-replica ^
    --db-instance-identifier SimCoProd01Replica01 ^
    --region us-west-2
    --source-db-instance-identifier arn:aws:rds:us-east-1:123456789012:db:SimcoProd01
```

Example Créer un réplica en lecture entre régions dans un VPC

Cet exemple illustre la création d'un réplica en lecture dans la région us-west-2 à partir d'une instance de base de données source dans la région us-east-1. Le réplica en lecture est créé dans le VPC associé au groupe de sous-réseaux de bases de données spécifié :

Pour Linux, macOS ou Unix :

```
aws rds create-db-instance-read-replica \
    --db-instance-identifier SimCoProd01Replica01 \
    --region us-west-2
    --db-subnet-group-name my-us-west-2-subnet
    --source-db-instance-identifier arn:aws:rds:us-east-1:123456789012:db:SimcoProd01
```

Pour Windows :

```
aws rds create-db-instance-read-replica ^
    --db-instance-identifier SimCoProd01Replica01 ^
    --region us-west-2
    --db-subnet-group-name my-us-west-2-subnet
    --source-db-instance-identifier arn:aws:rds:us-east-1:123456789012:db:SimcoProd01
```

Supervision de la réplication en lecture

Vous pouvez superviser le statut d'un réplica en lecture de différentes manières. La console Amazon RDS affiche le statut d'un réplica en lecture dans la section Disponibilité et durabilité des détails du réplica en lecture. Pour consulter les détails d'un réplica en lecture, cliquez sur son nom dans la liste des instances de la console Amazon RDS.

Vous pouvez également consulter le statut d'un réplica en lecture à l'aide de la commande AWS CLI `describe-db-instances` ou de l'opération d'API Amazon RDS `DescribeDBInstances`.

Le statut d'un réplica en lecture peut avoir les valeurs suivantes :

- replicating (réplication en cours) – Le réplica en lecture réplique correctement.
- réplication dégradée (SQL Server uniquement)– Les réplicas reçoivent des données de l'instance principale, mais une ou plusieurs bases de données peuvent ne pas recevoir de mises à jour. Cela peut se produire, par exemple, lorsqu'un réplica est en train de configurer des bases de données nouvellement créées.

  L'état ne passe pas de `replication degraded` à `error`, à moins qu'une erreur ne se produise pendant l'état dégradé.
- error (erreur) – Une erreur s'est produite dans le cadre de la réplication. Examinez le champ Replication Error (Erreur de réplication) dans la console Amazon RDS ou le journal des événements pour déterminer l'erreur exacte. Pour plus d'informations sur la résolution d'une erreur de réplication, consultez Résolution d'un problème de réplica en lecture MySQL (p. 856).
- terminated (arrêté) (MariaDB, MySQL ou PostgreSQL uniquement) – La réplication est arrêtée. Cela se produit si la réplication est arrêtée pendant plus de trente jours consécutifs, manuellement ou en raison d'une erreur de réplication. Dans ce cas, Amazon RDS met fin à la réplication entre l'instance de base de données principale et tous les réplicas en lecture. Amazon RDS procède ainsi afin d'éviter des besoins en stockage accrus sur l'instance de base de données source et de longues durées de basculement.

  Une réplication interrompue peut affecter le stockage, car les journaux peuvent croître en taille et en nombre en raison du volume élevé des messages d'erreur consignés dans le journal. Une réplication interrompue peut également affecter la récupération en cas de défaillance en raison du temps dont a besoin Amazon RDS pour conserver et traiter le grand nombre de journaux au cours de la récupération.
- stopped (interrompue) (MariaDB ou MySQL uniquement) – La réplication s'est interrompue en raison d'une demande initiée par le client.
- replication stop point set (point d'arrêt de réplication réglé) (MySQL uniquement) – Un point d'arrêt de réplication a été réglé par le client à l'aide de la procédure stockée mysql.rds_start_replication_until (p. 914) et la réplication est en cours.
- replication stop point reached (point d'arrêt de réplication atteint) (MySQL uniquement) – Un point d'arrêt de réplication a été réglé par le client à l'aide de la procédure stockée mysql.rds_start_replication_until (p. 914) et la réplication est arrêtée, car le point d'arrêt est atteint.

Surveillance du retard de réplication

Vous pouvez surveiller le retard de réplication dans Amazon CloudWatch en consultant la métrique Amazon RDS `ReplicaLag`.

Pour MySQL et MariaDB, la métrique `ReplicaLag` contient la valeur du champ `Seconds_Behind_Master` de la commande `SHOW SLAVE STATUS`. Les causes courantes du retard de réplication pour MySQL et MariaDB sont les suivantes :

- Une indisponibilité du réseau.
- L'écriture dans des tables avec des index sur un réplica en lecture. Si le paramètre `read_only` n'a pas pour valeur 0 sur le réplica en lecture, il peut interrompre la réplication.
- Utilisation d'un moteur de stockage non transactionnel tel que MyISAM. La réplication est prise en charge uniquement pour le moteur de stockage InnoDB sur MySQL et pour le moteur de stockage XtraDB sur MariaDB.

Lorsque la métrique `ReplicaLag` atteint 0, le réplica a rattrapé l'instance de bases de données principale. Si la métrique `ReplicaLag` retourne `-1`, la réplication n'est actuellement pas active. `ReplicaLag = -1` est équivalent à `Seconds_Behind_Master = NULL`.

Pour Oracle, la métrique `ReplicaLag` correspond à la somme de la valeur `Apply Lag` et à la différence entre la durée actuelle et la valeur `DATUM_TIME` du retard appliqué. La valeur `DATUM_TIME` correspond

à la dernière heure à laquelle le réplica en lecture a reçu des données de son instance de base de données source. Pour de plus amples informations, veuillez consulter V$DATAGUARD_STATS dans la documentation d'Oracle.

Pour SQL Server, la métrique `ReplicaLag` correspond au décalage maximal des bases de données qui ont pris du retard, en secondes. Par exemple, si vous avez deux bases de données qui accusent respectivement un retard de 5 secondes et 10 secondes, alors `ReplicaLag` a pour valeur 10 secondes. La métrique `ReplicaLag` renvoie la valeur de la requête suivante.

```
select ag.name name, MAX(hdrs.secondary_lag_seconds) max_lag from
 sys.dm_hadr_database_replica_state
```

Pour de plus amples informations, veuillez consulter secondary_lag_seconds dans la documentation Microsoft.

`ReplicaLag` renvoie `-1` si RDS ne peut pas déterminer le retard, par exemple lors de la configuration du réplica, ou lorsque le réplica en lecture est à l'état `error`.

> **Note**
>
> Les nouvelles bases de données ne sont pas incluses dans le calcul du retard tant qu'elles ne sont pas accessibles sur le réplica en lecture.

Pour PostgreSQL, la métrique `ReplicaLag` renvoie la valeur de la requête suivante.

```
SELECT extract(epoch from now() - pg_last_xact_replay_timestamp()) AS slave_lag
```

PostgreSQL versions 9.5.2 et ultérieures utilise des emplacements physiques de réplication pour gérer la rétention WAL (Write Ahead Log) sur l'instance source. Pour chaque instance de réplica en lecture entre régions, Amazon RDS crée un emplacement de réplication physique et l'associe à l'instance. Deux métriques Amazon CloudWatch, `Oldest Replication Slot Lag` et `Transaction Logs Disk Usage`, indiquent le retard du dernier réplica en termes de données WAL reçues et le volume de stockage utilisé pour les données WAL. La valeur `Transaction Logs Disk Usage` peut considérablement augmenter lorsqu'un réplica en lecture entre régions présente un retard important.

Pour de plus amples informations sur la surveillance d'un cluster de bases de données avec CloudWatch, veuillez consulter Surveillance avec Amazon CloudWatch (p. 376).

Balisage de ressources Amazon RDS

Vous pouvez utiliser des balises Amazon RDS pour ajouter des métadonnées à vos ressources Amazon RDS. Vous pouvez également utiliser ces balises avec des stratégies IAM pour gérer l'accès aux ressources Amazon RDS et contrôler les actions qui peuvent être appliquées aux ressources Amazon RDS. Enfin, vous pouvez utiliser ces balises pour suivre les coûts en regroupant les dépenses pour des ressources balisées de la même façon.

Toutes les ressources Amazon RDS peuvent être balisées

- Instances DB
- Clusters DB
- Réplicas en lecture
- Instantanés de base de données
- Instantanés de cluster DB

- Instances DB réservées
- Abonnements aux événements
- Groupes d'options DB
- Groupes de paramètres DB
- Groupes de paramètres de cluster DB
- Groupes de sécurité DB
- Groupes de sous-réseaux DB

Pour plus d'informations sur la gestion de l'accès aux ressources balisées avec des stratégies IAM, consultez Identity and Access Management dans Amazon RDS (p. 1536).

Présentation des balises des ressources Amazon RDS

Une balise Amazon RDS est une paire nom-valeur que vous définissez et associez avec une ressource Amazon RDS. Le nom s'appelle la clé. Fournir une valeur pour la clé est facultatif. Vous pouvez utiliser des balises pour assigner des informations arbitraires à une ressource Amazon RDS. Vous pouvez utiliser une clé de balise, par exemple, pour définir une catégorie, et la valeur de balise peut être un élément de cette catégorie. Par exemple, vous pouvez définir une clé de balise « projet » et une valeur de balise « Salix », indiquant que la ressource Amazon RDS est assignée au projet Salix. Vous pouvez également utiliser des balises pour désigner des ressources Amazon RDS destinées aux tests ou à la production en utilisant une clé telle que `environment=test` ou `environment=production`. Nous vous recommandons d'utiliser un ensemble cohérent de clés de balise pour faciliter le suivi des métadonnées associées aux ressources Amazon RDS.

Utilisez des balises pour organiser votre facture AWS afin de refléter votre propre structure de coût. Pour ce faire, inscrivez-vous pour obtenir votre facture de compte AWS avec les valeurs de clé de balise incluses. Ensuite, pour voir le coût de vos ressources combinées, organisez vos informations de facturation en fonction des ressources possédant les mêmes valeurs de clé de balise. Par exemple, vous pouvez baliser plusieurs ressources avec un nom d'application spécifique, puis organiser vos informations de facturation pour afficher le coût total de cette application dans plusieurs services. Pour de plus amples informations, veuillez consulter Répartition et balisage des coûts dans À propos de la facturation et de la gestion des coûts AWS.

Chaque ressource Amazon RDS possède un ensemble de balises qui contient toutes les balises assignées à cette ressource Amazon RDS. Un ensemble de balises peut contenir jusqu'à 50 balises ou n'en contenir aucune. Si vous ajoutez une balise à une ressource Amazon RDS ayant la même clé qu'une balise existante sur cette ressource, la nouvelle valeur remplace l'ancienne valeur.

AWS n'applique aucune signification sémantique aux balises ; celles-ci sont strictement interprétées comme des chaînes de caractères. Amazon RDS peut configurer des balises sur une instance de base de données ou d'autres ressources Amazon RDS, en fonction des paramètres que vous utilisez lors de la création de la ressource. Par exemple, Amazon RDS peut ajouter une balise indiquant qu'une instance de bases de données est destinée à la production ou aux tests.

- La clé de balise correspond au nom obligatoire de la balise. La valeur de la chaîne peut comporter de 1 à 128 caractères Unicode et ne peut pas être précédée de « aws: » ou « rds: ». La chaîne peut uniquement contenir l'ensemble de lettres, de chiffres et d'espaces Unicode, '_', '.', ':', '/', '=', '+', '-', '@' (regex Java : "^([\\p{L}\\p{Z}\\p{N}_.:/=+\\-@]*)$").

- La valeur de balise correspond à la valeur de chaîne facultative de la balise. La valeur de la chaîne peut comporter de 1 à 256 caractères Unicode et ne peut pas être précédée de « aws: ». La chaîne peut uniquement contenir l'ensemble de lettres, de chiffres et d'espaces Unicode, '_', '.', ':', '/', '=', '+', '-', '@' (regex Java : "^([\\p{L}\\p{Z}\\p{N}_.:/=+\\-@]*)$").

Les valeurs comprises dans un ensemble de balises ne doivent pas nécessairement être uniques et peuvent être null. Par exemple, vous pouvez avoir une paire clé-valeur dans un ensemble de balises `project=Trinity` et `cost-center=Trinity`.

> **Note**
>
> Vous pouvez ajouter une balise à un instantané, toutefois, votre facture ne reflètera pas ce groupement.

Vous pouvez utiliser la AWS Management Console, l'interface de ligne de commande ou l'API Amazon RDS pour ajouter, répertorier et supprimer les balises sur les ressources Amazon RDS. Lorsque vous utilisez l'interface de ligne de commande ou l'API Amazon RDS, vous devez fournir l'Amazon Resource Name (ARN) pour la ressource Amazon RDS avec laquelle vous souhaitez travailler. Pour plus d'informations sur la création d'un ARN, consultez Création d'un ARN pour Amazon RDS (p. 298).

Les balises sont mises en cache à des fins d'autorisation. Pour cette raison, les ajouts et les mises à jour sur les balises sur les ressources Amazon RDS peuvent prendre plusieurs minutes avant d'être disponibles.

Copie de balises

Lorsque vous créez ou restaurez une instance de base de données, vous pouvez spécifier que les balises de l'instance de base de données soient copiées vers les snapshots de l'instance de base de données. La copie des balises garantit que les métadonnées pour les instantanés de base de données correspondent à celles de l'instance de base de données source et que toutes les stratégies d'accès pour l'instantané de base de données correspondent également à l'instance de base de données source. Les balises ne sont pas copiées par défaut.

Vous pouvez spécifier que les balises soient copiées vers des snapshots DB pour les actions suivantes :

- Création d'une instance de base de données.
- Restauration d'une instance de base de données.
- Création d'un réplica en lecture.
- Copie d'un instantané de base de données.

> **Note**
>
> Si vous incluez une valeur pour le paramètre `--tag-key` de la commande create-db-snapshot de l'interface AWS CLI (ou fournissez au moins une balise à l'opération d'API CreateDBSnapshot), RDS ne copie pas les balises de l'instance de bases de données source vers le nouvel instantané de base de données. Cette fonctionnalité s'applique même si l'option `--copy-tags-to-snapshot` (`CopyTagsToSnapshot`) est activée sur l'instance de base de données source. Si vous optez pour cette approche, vous pouvez créer une copie d'une instance de bases de données depuis un instantané de base de données sans avoir à ajouter de balises qui ne s'appliquent pas à la nouvelle instance de bases de données. Une fois que vous avez créé votre instantané de base de données à l'aide de la commande `create-db-snapshot` de l'interface AWS CLI (ou l'opération d'API Amazon RDS `CreateDBSnapshot`), vous pouvez ajouter des balises comme décrit plus loin dans cette rubrique.

Console

La processus de balisage d'une ressource Amazon RDS est semblable pour toutes les ressources. La procédure suivante indique comment baliser une instance de base de données Amazon RDS.

Pour ajouter une balise à une instance de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).

   Note

   Pour filtrer la liste des instances de base de données dans le volet Bases de données, saisissez une chaîne de texte dans Filter databases (Filtrer les bases de données). Seules les instances de base de données qui contiennent la chaîne apparaissent.
3. Sélectionnez le nom de l'instance de base de données que vous souhaitez baliser pour afficher ses détails.
4. Dans la section des détails, faites défiler jusqu'à la section Balises.
5. Choisissez Ajouter. La fenêtre Ajouter des balises s'affiche.

6. Saisissez une valeur pour Tag key (Clé de balise) et Valeur.
7. Pour ajouter une autre balise, vous pouvez choisir Ajouter une autre balise et saisir une valeur pour Tag key (Clé de balise) et Valeur.

   Répétez cette étape autant de fois que nécessaire.
8. Choisissez Ajouter.

Pour supprimer une balise d'une instance de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).

   Note

   Pour filtrer la liste des instances de base de données dans le volet Bases de données, saisissez une chaîne de texte dans la zone Filter databases (Filtrer les bases de données). Seules les instances de base de données qui contiennent la chaîne apparaissent.
3. Sélectionnez le nom de l'instance de base de données pour afficher ses détails.
4. Dans la section des détails, faites défiler jusqu'à la section Balises.

5. Choisissez la balise que vous souhaitez supprimer.

6. Choisissez Supprimer, puis Supprimer dans la fenêtre Supprimer les balises.

AWS CLI

Vous pouvez ajouter, répertorier ou supprimer des balises pour une instance de base de données à l'aide de l'AWS CLI.

- Pour ajouter une ou plusieurs balises à une ressource Amazon RDS, utilisez la commande `add-tags-to-resource` d'AWS CLI.
- Pour répertorier les balises sur une ressource Amazon RDS, utilisez la commande `list-tags-for-resource` dAWS CLI.
- Pour supprimer une ou plusieurs balises d'une ressource Amazon RDS, utilisez la commande `remove-tags-from-resource` d'AWS CLI.

Pour en savoir sur la création de l'ARN requis, consultez Création d'un ARN pour Amazon RDS (p. 298).

API RDS

Vous pouvez ajouter, répertorier ou supprimer des balises pour une instance de base de données à l'aide de l'API Amazon RDS.

- Pour ajouter une balise à une ressource Amazon RDS, utilisez l'opération `AddTagsToResource`.
- Pour répertorier des balises assignées à une ressource Amazon RDS, utilisez l'opération `ListTagsForResource`.
- Pour supprimer des balises d'une ressource Amazon RDS, utilisez l'opération `RemoveTagsFromResource`.

Pour en savoir sur la création de l'ARN requis, consultez Création d'un ARN pour Amazon RDS (p. 298).

Lorsque vous travaillez avec XML à l'aide de l'API Amazon RDS, les balises utilisent le schéma suivant :

```
<Tagging>
    <TagSet>
        <Tag>
            <Key>Project</Key>
            <Value>Trinity</Value>
        </Tag>
        <Tag>
            <Key>User</Key>
            <Value>Jones</Value>
        </Tag>
    </TagSet>
```

```
</Tagging>
```

Le tableau suivant fournit une liste des balises XML autorisées et leurs caractéristiques. Les valeurs pour la clé et la valeur sont sensibles à la casse. Par exemple, projet=Trinity et PROJET=Trinity sont deux balises différentes.

Elément de balisage	Description
TagSet	Un ensemble de balises contient toutes les balises assignées à une ressource Amazon RDS. Il ne peut y avoir qu'un ensemble de balises par ressource. Vous travaillez avec un TagSet uniquement via l'API Amazon RDS.
Tag	Une balise est une paire clé-valeur définie par l'utilisateur. Il peut y avoir de 1 à 50 balises dans un ensemble de balises.
Key	Une clé est le nom obligatoire de la balise. La valeur de la chaîne peut comporter de 1 à 128 caractères Unicode et ne peut pas être précédée de « rds: » ou « aws: ». La chaîne peut uniquement contenir l'ensemble de lettres, de chiffres et d'espaces Unicode, '_', '.', '/', '=', '+', '-' (regex Java : "^([\ \p{L}\\p{Z}\\p{N}_.:/=+\\-]*)$"). Les clés doivent être propres à un ensemble de balises. Par exemple, vous ne pouvez pas avoir une paire-clé dans un ensemble de balises avec la clé identique mais des valeurs différentes comme projet/Trinity et projet/Xanadu.
Value	Une valeur est la valeur facultative de la balise. La valeur de la chaîne peut comporter de 1 à 256 caractères Unicode et ne peut pas être précédée de « rds: » ou « aws: ». La chaîne peut uniquement contenir l'ensemble de lettres, de chiffres et d'espaces Unicode, '_', '.', '/', '=', '+', '-' (regex Java : "^([\ \p{L}\\p{Z}\\p{N}_.:/=+\\-]*)$"). Les valeurs comprises dans un ensemble de balises ne doivent pas nécessairement être uniques et peuvent être null. Par exemple, vous pouvez avoir une paire clé-valeur dans un ensemble de balises appelé projet/Trinity et centre-de-coûts/Trinity.

Utilisation des Amazon Resource Names (ARN) dans Amazon RDS

Les ressources créées dans Amazon Web Services sont chacune identifiées de façon unique par un Amazon Resource Name (ARN). Pour certaines opérations Amazon RDS, vous devez identifier une ressource Amazon RDS de manière unique en spécifiant son ARN. Par exemple, lorsque vous créez un réplica en lecture d'instance de base de données RDS, vous devez fournir l'ARN pour l'instance de base de données source.

Création d'un ARN pour Amazon RDS

Les ressources créées dans Amazon Web Services sont chacune identifiées de façon unique par un Amazon Resource Name (ARN). Vous pouvez construire un ARN pour une ressource Amazon RDS en utilisant la syntaxe suivante.

```
arn:aws:rds:<region>:<account number>:<resourcetype>:<name>
```

Nom de la région	Région	Point de terminaison	Protocole	
USA Est (Ohio)	us-east-2	rds.us-east-2.amazonaws.com rds-fips.us-east-2.amazonaws.com	HTTPS HTTPS	
USA Est (Virginie du Nord)	us-east-1	rds.us-east-1.amazonaws.com rds-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
USA Ouest (Californie du Nord)	us-west-1	rds.us-west-1.amazonaws.com rds-fips.us-west-1.amazonaws.com	HTTPS HTTPS	
USA Ouest (Oregon)	us-west-2	rds.us-west-2.amazonaws.com rds-fips.us-west-2.amazonaws.com	HTTPS HTTPS	
Afrique (Le Cap)	af-south-1	rds.af-south-1.amazonaws.com	HTTPS	
Asie-Pacifique (Hong Kong)	ap-east-1	rds.ap-east-1.amazonaws.com	HTTPS	
Asie-Pacifique (Mumbai)	ap-south-1	rds.ap-south-1.amazonaws.com	HTTPS	
Asie-Pacifique (Osaka-Local)	ap-northeast-3	rds.ap-northeast-3.amazonaws.com	HTTPS	
Asie-Pacifique (Séoul)	ap-northeast-2	rds.ap-northeast-2.amazonaws.com	HTTPS	
Asie-Pacifique (Singapour)	ap-southeast-1	rds.ap-southeast-1.amazonaws.com	HTTPS	
Asie-Pacifique (Sydney)	ap-southeast-2	rds.ap-southeast-2.amazonaws.com	HTTPS	
Asie-Pacifique (Tokyo)	ap-northeast-1	rds.ap-northeast-1.amazonaws.com	HTTPS	
Canada (Centre)	ca-central-1	rds.ca-central-1.amazonaws.com rds-fips.ca-central-1.amazonaws.com	HTTPS HTTPS	
Chine (Pékin)	cn-north-1	rds.cn-north-1.amazonaws.com.cn	HTTPS	

Nom de la région	Région	Point de terminaison	Protocole	
Chine (Ningxia)	cn-northwest-1	rds.cn-northwest-1.amazonaws.com.cn	HTTPS	
Europe (Francfort)	eu-central-1	rds.eu-central-1.amazonaws.com	HTTPS	
Europe (Irlande)	eu-west-1	rds.eu-west-1.amazonaws.com	HTTPS	
Europe (Londres)	eu-west-2	rds.eu-west-2.amazonaws.com	HTTPS	
Europe (Milan)	eu-south-1	rds.eu-south-1.amazonaws.com	HTTPS	
Europe (Paris)	eu-west-3	rds.eu-west-3.amazonaws.com	HTTPS	
Europe (Stockholm)	eu-north-1	rds.eu-north-1.amazonaws.com	HTTPS	
Moyen-Orient (Bahreïn)	me-south-1	rds.me-south-1.amazonaws.com	HTTPS	
Amérique du Sud (São Paulo)	sa-east-1	rds.sa-east-1.amazonaws.com	HTTPS	
AWS GovCloud (USA Est)	us-gov-east-1	rds.us-gov-east-1.amazonaws.com rds.us-gov-east-1.amazonaws.com	HTTPS HTTPS	
AWS GovCloud (US)	us-gov-west-1	rds.us-gov-west-1.amazonaws.com rds.us-gov-west-1.amazonaws.com	HTTPS HTTPS	

Le tableau suivant indique le format à utiliser lors de la création d'un ARN pour un type de ressource Amazon RDS particulier.

Type de ressource	Format ARN
instance de base de données	arn:aws:rds:*<region>*:*<account>*:db:*<name>* Par exemple : `arn:aws:rds:us-east-2:123456789012:db:my-mysql-instance-1`
Abonnement aux événements	arn:aws:rds:*<region>*:*<account>*:es:*<name>* Par exemple :

Type de ressource	Format ARN
	`arn:aws:rds:us-east-2:123456789012:es:my-subscription`
Groupe d'options DB	arn:aws:rds:*<region>*:*<account>*:og:*<name>* Par exemple : `arn:aws:rds:us-east-2:123456789012:og:my-og`
Groupe de paramètres de base de données	arn:aws:rds:*<region>*:*<account>*:pg:*<name>* Par exemple : `arn:aws:rds:us-east-2:123456789012:pg:my-param-enable-logs`
instance de base de données réservée	arn:aws:rds:*<region>*:*<account>*:ri:*<name>* Par exemple : `arn:aws:rds:us-east-2:123456789012:ri:my-reserved-postgresql`
Security Group DB	arn:aws:rds:*<region>*:*<account>*:secgrp:*<name>* Exemples : `arn:aws:rds:us-east-2:123456789012:secgrp:my-public`
Instantané de base de données automatique	arn:aws:rds:*<region>*:*<account>*:snapshot:rds:*<name>* Exemples : `arn:aws:rds:us-east-2:123456789012:snapshot:rds:my-mysql-db-2019-07-22-07-23`
Instantané de base de données manuel	arn:aws:rds:*<region>*:*<account>*:snapshot:*<name>* Exemples : `arn:aws:rds:us-east-2:123456789012:snapshot:my-mysql-db-snap`
Groupe de sous-réseaux DB	arn:aws:rds:*<region>*:*<account>*:subgrp:*<name>* Exemples : `arn:aws:rds:us-east-2:123456789012:subgrp:my-subnet-10`

Obtention d'un ARN existant

Vous pouvez obtenir l'ARN d'une ressource RDS en utilisant la AWS Management Console, l'AWS Command Line Interface (AWS CLI) ou l'API RDS.

Console

Pour obtenir un ARN depuis l'AWS Management Console, accédez à la ressource pour laquelle vous souhaitez obtenir un ARN, puis consultez les détails de cette ressource. Par exemple, vous pouvez obtenir l'ARN d'une instance de base de données dans l'onglet Configuration des détails de cette instance, comme illustré ci-après.

AWS CLI

Pour obtenir un ARN depuis l'AWS CLI pour une ressource RDS particulière, utilisez la commande `describe` pour cette ressource. Le tableau suivant illustre chaque commande de l'interface de ligne de commande AWS CLI et la propriété d'ARN utilisée avec la commande pour obtenir un ARN.

AWS CLI commande	Propriété d'ARN
describe-event-subscriptions	EventSubscriptionArn
describe-certificates	CertificateArn
describe-db-parameter-groups	DBParameterGroupArn
describe-db-instances	DBInstanceArn

AWS CLI commande	Propriété d'ARN
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

Par exemple, la commande AWS CLI suivante permet d'obtenir l'ARN pour une instance de base de données.

Example

Pour Linux, macOS ou Unix :

```
aws rds describe-db-instances \
--db-instance-identifier DBInstanceIdentifier \
--region us-west-2 \
--query "*[].{DBInstanceIdentifier:DBInstanceIdentifier,DBInstanceArn:DBInstanceArn}"
```

Pour Windows :

```
aws rds describe-db-instances ^
--db-instance-identifier DBInstanceIdentifier ^
--region us-west-2 ^
--query "*[].{DBInstanceIdentifier:DBInstanceIdentifier,DBInstanceArn:DBInstanceArn}"
```

La sortie de cette commande se présente comme suit :

```
[
    {
        "DBInstanceArn": "arn:aws:rds:us-west-2:account_id:db:instance_id",
        "DBInstanceIdentifier": "instance_id"
    }
]
```

API RDS

Pour obtenir un ARN pour une ressource RDS particulière, vous pouvez appeler les opérations d'API RDS suivantes et utiliser les propriétés d'ARN illustrées ci-après.

Opération d'API RDS	Propriété d'ARN
DescribeEventSubscriptions	EventSubscriptionArn
DescribeCertificates	CertificateArn
DescribeDBParameterGroups	DBParameterGroupArn
DescribeDBInstances	DBInstanceArn

Opération d'API RDS	Propriété d'ARN
DescribeDBSecurityGroups	DBSecurityGroupArn
DescribeDBSnapshots	DBSnapshotArn
DescribeEvents	SourceArn
DescribeReservedDBInstances	ReservedDBInstanceArn
DescribeDBSubnetGroups	DBSubnetGroupArn
DescribeOptionGroups	OptionGroupArn

Utilisation du stockage pour les instances de base de données Amazon RDS

Pour préciser la façon dont vous voulez que vos données soient stockées dans Amazon RDS, vous choisissez un type de stockage et vous fournissez une taille de stockage lorsque vous créez ou modifiez une instance de base de données. Ensuite, vous pouvez augmenter le volume ou modifier le type de stockage en changeant l'instance de base de données. Pour plus d'informations sur le type de stockage à utiliser pour votre charge de travail, consultez Types de stockage Amazon RDS (p. 30).

Rubriques

- Augmentation de la capacité de stockage d'une instance de base de données (p. 304)
- Gestion automatique de la capacité avec le dimensionnement automatique du stockage Amazon RDS (p. 306)
- Modification des paramètres de stockage SSD pour les E/S par seconde provisionnées (p. 311)

Augmentation de la capacité de stockage d'une instance de base de données

Si vous avez besoin d'espace pour des données supplémentaires, vous pouvez augmenter l'espace de stockage d'une instance de base de données existante. Pour cela, vous pouvez utiliser la Console de gestion Amazon RDS, l'API Amazon RDS ou l'AWS Command Line Interface (AWS CLI). Pour de plus amples informations sur les limites de stockage, veuillez consulter Stockage d'instance de base de données Amazon RDS (p. 30).

> **Note**
>
> Le dimensionnement du stockage pour Amazon RDS pour les instances de base de données SQL Server est pris en charge uniquement pour les types de stockage Usage général (SSD) et IOPS dimensionné (SSD).

Pour surveiller la quantité de stockage disponible pour votre instance de base de données et prendre des mesures quand cela est nécessaire, nous vous recommandons de créer une alarme Amazon CloudWatch. Pour de plus amples informations sur la configuration des alarmes CloudWatch, veuillez consulter Utilisation des alarmes CloudWatch.

Dans la plupart des cas, le dimensionnement du stockage ne requiert pas d'interruption et ne dégrade pas les performances du serveur. Après la modification de la taille de stockage d'une instance de base de données, l'instance passe à l'état storage-optimization. L'instance de base de données est totalement opérationnelle après modification du stockage.

> **Note**
>
> Vous ne pouvez pas effectuer de modifications de la taille de stockage pendant six (6) heures après la fin de l'optimisation du stockage sur l'instance.

Toutefois, il existe un cas spécial si vous avez une instance de base de données SQL Server et que vous n'avez pas modifié la configuration du stockage depuis novembre 2017. Dans ce cas, lorsque vous modifiez votre instance de base de données afin d'augmenter le volume de stockage alloué, une brève interruption de quelques minutes peut se produire. Après l'interruption, l'instance de base de données est en ligne, mais dans l'état `storage-optimization`. Les performances peuvent se dégrader pendant l'optimisation du stockage.

> **Note**
>
> Vous ne pouvez pas réduire le volume de stockage d'une instance de base de données une fois qu'il a été alloué.

Console

Pour augmenter le stockage d'une instance de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez l'instance de bases de données que vous souhaitez modifier.
4. Sélectionnez Modify.
5. Saisissez une nouvelle valeur pour Stockage alloué. Elle doit être supérieure à la valeur actuelle.

> **Note**
>
> Lorsque vous augmentez la valeur du stockage alloué, vous devez le faire d'au moins 10 %. Si vous tentez d'augmenter la valeur de moins de 10 %, une erreur s'affiche.

6. Choisissez Continuer pour passer à l'écran suivant.
7. Choisissez Appliquer immédiatement dans la section Planification des modifications pour appliquer immédiatement les modifications du stockage à l'instance de base de données. Ou choisissez Appliquer lors de la prochaine fenêtre de maintenance planifiée pour appliquer les modifications pendant la prochaine fenêtre de maintenance.
8. Lorsque les paramètres vous conviennent, choisissez Modifier l'instance de base de données.

AWS CLI

Pour augmenter le stockage d'une instance de base de données, utilisez la commande `modify-db-instance` de l'AWS CLI. Définissez les paramètres suivants :

- `--allocated-storage` – Volume de stockage à allouer pour l'instance de base de données, en gibioctets.
- `--apply-immediately` – Utilisez `--apply-immediately` pour passer immédiatement au nouveau type de stockage. Ou utiliser `--no-apply-immediately` (valeur par défaut) pour appliquer les modifications au cours de la prochaine fenêtre de maintenance. Une interruption immédiate a lieu lorsque les modifications sont appliquées.

Pour plus d'informations sur le stockage, consultez Stockage d'instance de base de données Amazon RDS (p. 30).

API Amazon RDS

Pour accroître l'espace de stockage d'une instance de base de données, utilisez l'opération d'API Amazon RDS `ModifyDBInstance`. Définissez les paramètres suivants :

- `AllocatedStorage` – Volume de stockage à allouer pour l'instance de base de données, en gibioctets.
- `ApplyImmediately` – Définissez cette option sur `True` pour appliquer immédiatement les modifications relatives au dimensionnement. Définissez cette option sur `False` (valeur par défaut) pour appliquer les modifications relatives au dimensionnement au cours de la prochaine fenêtre de maintenance. Une interruption immédiate a lieu lorsque les modifications sont appliquées.

Pour plus d'informations sur le stockage, consultez Stockage d'instance de base de données Amazon RDS (p. 30).

Gestion automatique de la capacité avec le dimensionnement automatique du stockage Amazon RDS

Si votre charge de travail est imprévisible, vous pouvez activer la scalabilité automatique du stockage pour une instance de base de données Amazon RDS. Pour cela, vous pouvez utiliser la console Amazon RDS, l'API Amazon RDS ou l'AWS CLI.

Par exemple, vous pouvez utiliser cette fonctionnalité pour une nouvelle application mobile de jeu que les utilisateurs adoptent rapidement. Dans ce cas, une charge de travail qui augmente rapidement peut dépasser le stockage de base de données disponible. Pour éviter d'avoir à augmenter manuellement la capacité de stockage d'une base de données, vous pouvez utiliser le dimensionnement automatique du stockage Amazon RDS.

Si le dimensionnement automatique du stockage est activé et que Amazon RDS détecte que vous êtes à court d'espace de stockage, il augmente automatiquement la capacité de votre stockage. Amazon RDS modifie le stockage d'une instance de base de données pour laquelle le dimensionnement automatique est activé si les conditions suivantes sont réunies :

- L'espace disponible est inférieur à 10 % du stockage alloué.
- La condition de stockage faible dure au moins cinq minutes.
- Au moins six heures se sont écoulées depuis la dernière modification du stockage.

Le stockage supplémentaire s'effectue par incréments de la valeur la plus élevée parmi les suivantes :

- 5 GiO
- 10 % du stockage actuellement alloué

- Prévision de croissance du stockage sur 7 heures basée sur la variation des métriques `FreeStorageSpace` au cours de la dernière heure. Pour de plus amples informations sur les métriques, consultez Surveillance avec Amazon CloudWatch.

Le seuil de stockage maximal est la limite au-delà de laquelle l'instance de base de données peut être mise à l'échelle. Vous ne pouvez pas définir un seuil de stockage maximal supérieur à la quantité maximale de stockage alloué à des instances pour lesquelles le dimensionnement automatique est activé.

Par exemple, SQL Server Standard Edition on db.m5.xlarge possède un stockage alloué par défaut pour l'instance de 20 GiB (le minimum) et un stockage alloué maximum de 16 384 GiB. Le seuil de stockage maximum par défaut pour la scalabilité automatique est de 1 000 GiB. Si vous utilisez ce paramètre par défaut, l'instance ne se met pas automatiquement à l'échelle au-dessus de 1 000 GiB. Ceci est vrai même si le stockage alloué maximum pour l'instance est de 16 384 GiB.

> Note
>
> Nous vous recommandons de choisir soigneusement le seuil de stockage maximal en fonction des habitudes d'utilisation et des besoins des clients. En cas d'aberrations au niveau des habitudes d'utilisation, le seuil de stockage maximal peut empêcher la mise à l'échelle du stockage à une valeur trop élevée lorsque la mise à l'échelle automatique prédit un seuil très élevé. Une fois qu'une instance de base de données a été mise à l'échelle automatique, son stockage alloué ne peut pas être réduit.

Les limitations suivantes s'appliquent à la mise à l'échelle automatique du stockage :

- Le dimensionnement automatique ne se produit pas si le seuil de stockage maximum peut être dépassé par l'incrémentation du stockage.
- Le dimensionnement automatique ne peut pas empêcher complètement les situations de stockage plein pour les chargements de données volumineux. En effet, aucune autre modification de stockage ne peut être apportée dans une période suivant la fin de l'optimisation du stockage sur l'instance inférieure à six heures. Si vous effectuez un chargement de données volumineux et que le dimensionnement automatique ne fournit pas suffisamment d'espace, la base de données peut rester à l'état de stockage plein pendant plusieurs heures. Cela peut nuire à la base de données.
- Si vous lancez une opération de dimensionnement du stockage en même temps qu'Amazon RDS, votre modification du stockage est prioritaire. L'opération de dimensionnement automatique est annulée.
- La mise à l'échelle automatique ne peut pas être utilisée avec le stockage magnétique.
- La mise à l'échelle automatique ne peut pas être utilisée avec les classes d'instance de génération précédente suivantes qui ont moins de 6 Tio de stockage ordonnable : db.m3.large, db.m3.xlarge et db.m3.2xlarge.

Bien que le dimensionnement automatique vous permette d'accroître l'espace de stockage de votre instance de base de données Amazon RDS de façon dynamique, vous devez quand même attribuer à votre instance de base de données une taille de stockage initiale adaptée à votre charge de travail habituelle.

Activation du dimensionnement automatique du stockage pour une nouvelle instance de base de données

Lorsque vous créez une nouvelle instance de base de données Amazon RDS, vous pouvez choisir d'activer ou non le dimensionnement automatique du stockage. Vous pouvez également définir une limite supérieure sur le stockage qu'Amazon RDS peut allouer pour l'instance de base de données.

> Note
>
> Lorsque vous clonez une instance de base de données Amazon RDS pour laquelle le dimensionnement automatique du stockage est activé, ce paramètre n'est pas hérité

automatiquement par l'instance clonée. La nouvelle instance de base de données a la même quantité de stockage alloué que l'instance d'origine. Vous pouvez activer à nouveau le dimensionnement automatique pour la nouvelle instance si l'instance clonée continue à augmenter ses exigences de stockage.

Console

Pour activer le dimensionnement automatique du stockage pour une nouvelle instance de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le coin supérieur droit de la console Amazon RDS, choisissez la région AWS dans laquelle vous voulez créer l'instance de base de données.
3. Dans la panneau de navigation, choisissez Databases (Bases de données).
4. Choisissez Create database (Créer une base de données). Sur la page Sélectionner un moteur, choisissez votre moteur de base de données et spécifiez les informations de votre instance de base de données comme décrit dans Mise en route avec Amazon RDS (p. 69).
5. Dans la section Storage autoscaling (Dimensionnement automatique du stockage), définissez la valeur de Maximum storage threshold (Limite de stockage maximum) pour l'instance de base de données.
6. Spécifiez le reste des informations de l'instance de base de données comme décrit dans Mise en route avec Amazon RDS (p. 69).

AWS CLI

Pour activer le dimensionnement automatique du stockage pour une nouvelle instance de base de données, utilisez la commande AWS CLI `create-db-instance`. Définissez le paramètre suivant :

- `--max-allocated-storage` – Active le dimensionnement automatique du stockage et définit la limite supérieure de la taille du stockage, en gigaoctets.

Pour vérifier que le dimensionnement automatique du stockage Amazon RDS est disponible pour votre instance de base de données, utilisez la commande AWS CLI `describe-valid-db-instance-modifications`. Pour vérifier en fonction de la classe de l'instance avant sa création, utilisez la commande `describe-orderable-db-instance-options`. Vérifiez le champ suivant dans la valeur de retour :

- `SupportsStorageAutoscaling` – Indique si l'instance de base de données ou la classe d'instance prend en charge le dimensionnement automatique du stockage.

Pour plus d'informations sur le stockage, consultez Stockage d'instance de base de données Amazon RDS (p. 30).

API Amazon RDS

Pour activer la mise à l'échelle automatique du stockage pour une nouvelle instance de base de données, utilisez l'opération d'API Amazon RDS `CreateDBInstance`. Définissez le paramètre suivant :

- `MaxAllocatedStorage` – Active le dimensionnement automatique du stockage Amazon RDS et définit la limite supérieure de la taille du stockage, en gigaoctets.

Pour vérifier que la mise à l'échelle automatique du stockage Amazon RDS est disponible pour votre instance de base de données, utilisez l'opération d'API Amazon RDS

`DescribeValidDbInstanceModifications` pour une instance existante ou l'opération `DescribeOrderableDBInstanceOptions` avant de créer une instance. Vérifiez le champ suivant dans la valeur de retour :

- `SupportsStorageAutoscaling` – Indique si l'instance de base de données prend en charge le dimensionnement automatique du stockage.

Pour plus d'informations sur le stockage, consultez Stockage d'instance de base de données Amazon RDS (p. 30).

Modification du paramètre de dimensionnement automatique du stockage pour une instance de base de données

Vous pouvez activer le dimensionnement automatique du stockage pour une instance de base de données Amazon RDS existante. Vous pouvez également modifier la limite de stockage supérieure qu'Amazon RDS peut allouer pour l'instance de base de données.

Console

Pour modifier les paramètres de dimensionnement automatique du stockage pour une instance de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez l'instance de base de données que vous souhaitez modifier, puis sélectionnez Modifier. La page Modifier l'instance de base de données s'affiche.
4. Modifiez la limite de stockage dans la section Dimensionnement automatique. Pour de plus amples informations, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).
5. Lorsque tous les changements vous conviennent, choisissez Continuer et vérifiez les modifications.
6. Sur la page de confirmation, examinez vos modifications. Si elles sont correctes, choisissez Modification d'une instance de base de données pour enregistrer vos modifications. Sinon, choisissez Retour pour modifier vos modifications, ou choisissez Annuler pour les annuler.

   La modification de la limite de scalabilité automatique du stockage prend effet immédiatement. Ce paramètre ignore le paramètre Appliquer immédiatement.

AWS CLI

Pour modifier les paramètres de dimensionnement automatique du stockage pour une instance de base de données, utilisez la commande AWS CLI `modify-db-instance`. Définissez le paramètre suivant :

- `--max-allocated-storage` – Définit la limite de stockage supérieure, en gigaoctets. Si la valeur est supérieure au paramètre `--allocated-storage`, le dimensionnement automatique du stockage est activé. Si la valeur est égale au paramètre `--allocated-storage`, le dimensionnement automatique du stockage est désactivé.

Pour vérifier que le dimensionnement automatique du stockage Amazon RDS est disponible pour votre instance de base de données, utilisez la commande AWS CLI `describe-valid-db-instance-modifications`. Pour vérifier en fonction de la classe de l'instance avant sa création, utilisez la commande `describe-orderable-db-instance-options`. Vérifiez le champ suivant dans la valeur de retour :

- `SupportsStorageAutoscaling` – Indique si l'instance de base de données prend en charge le dimensionnement automatique du stockage.

Pour plus d'informations sur le stockage, consultez Stockage d'instance de base de données Amazon RDS (p. 30).

API Amazon RDS

Pour modifier les paramètres de mise à l'échelle automatique du stockage pour une instance de base de données, utilisez l'opération d'API Amazon RDS `ModifyDBInstance`. Définissez le paramètre suivant :

- `MaxAllocatedStorage` – Définit la limite de stockage supérieure, en gibioctets.

Pour vérifier que la mise à l'échelle automatique du stockage Amazon RDS est disponible pour votre instance de base de données, utilisez l'opération d'API Amazon RDS `DescribeValidDbInstanceModifications` pour une instance existante ou l'opération `DescribeOrderableDBInstanceOptions` avant de créer une instance. Vérifiez le champ suivant dans la valeur de retour :

- `SupportsStorageAutoscaling` – Indique si l'instance de base de données prend en charge le dimensionnement automatique du stockage.

Pour plus d'informations sur le stockage, consultez Stockage d'instance de base de données Amazon RDS (p. 30).

Désactivation du dimensionnement automatique du stockage pour une instance de base de données

Si vous n'avez plus besoin qu'Amazon RDS augmente automatiquement le capacité de stockage d'une instance de base de données Amazon RDS, vous pouvez désactiver le dimensionnement automatique du stockage. Après avoir désactivé le dimensionnement automatique, vous pouvez toujours augmenter manuellement le volume de stockage de votre instance de base de données.

Console

Pour désactiver le dimensionnement automatique du stockage pour une instance de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez l'instance de base de données que vous souhaitez modifier, puis sélectionnez Modifier. La page Modifier l'instance DB s'affiche.
4. Cochez la case Enable storage autoscaling (Activer le dimensionnement automatique du stockage) dans la section Storage autoscaling (Dimensionnement automatique du stockage. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).
5. Lorsque tous les changements vous conviennent, choisissez Continuer et vérifiez les modifications.
6. Sur la page de confirmation, examinez vos modifications. Si elles sont correctes, choisissez Modification d'une instance de base de données pour enregistrer vos modifications. Sinon, choisissez Retour pour modifier vos modifications, ou choisissez Annuler pour les annuler.

La modification de la limite de scalabilité automatique du stockage prend effet immédiatement. Ce paramètre ignore le paramètre Appliquer immédiatement.

AWS CLI

Pour désactiver le dimensionnement automatique du stockage pour une instance de base de données, utilisez la commande AWS CLI `modify-db-instance` et le paramètre suivant :

- `--max-allocated-storage` – Spécifiez une valeur égale au paramètre `--allocated-storage` pour empêcher un dimensionnement automatique du stockage Amazon RDS supplémentaire pour l'instance de base de données spécifiée.

Pour plus d'informations sur le stockage, consultez Stockage d'instance de base de données Amazon RDS (p. 30).

API Amazon RDS

Pour désactiver la mise à l'échelle automatique du stockage pour une instance de base de données, utilisez l'opération d'API Amazon RDS `ModifyDBInstance`. Définissez le paramètre suivant :

- `MaxAllocatedStorage` – Spécifiez une valeur égale au paramètre `AllocatedStorage` pour empêcher un dimensionnement automatique du stockage Amazon RDS supplémentaire pour l'instance de base de données spécifiée.

Pour plus d'informations sur le stockage, consultez Stockage d'instance de base de données Amazon RDS (p. 30).

Modification des paramètres de stockage SSD pour les E/S par seconde provisionnées

Vous pouvez modifier les paramètres d'une instance de base de données qui utilise le stockage SSD des IOPS provisionnées en utilisant la console Amazon RDS, l'AWS CLI ou l'API Amazon RDS. Spécifiez le type de stockage, le stockage alloué et le volume d'E/S par seconde provisionnées dont vous avez besoin. Vous pouvez choisir une plage de stockage située entre 1 000 IOPS et 100 Gio et 80 000 IOPS et 64 Tio (64 000 Gio). La plage dépend du moteur de base de données et du type d'instance

Bien que vous puissiez réduire la quantité d'IOPS provisionnés pour votre instance, vous ne pouvez pas réduire le volume de stockage SSD à usage général ou de stockage magnétique alloué.

Dans la plupart des cas, le dimensionnement du stockage ne requiert pas d'interruption et ne dégrade pas les performances du serveur. Après la modification des IOPS de stockage d'une instance de base de données, l'instance passe à l'état Optimisation du stockage. L'instance de base de données est totalement opérationnelle après modification du stockage.

> **Note**
>
> Vous ne pouvez pas effectuer de modifications de la taille de stockage pendant six (6) heures après la fin de l'optimisation du stockage sur l'instance.

Console

Pour modifier les paramètres d'E/S par seconde provisionnées pour une instance de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).

Note

Pour filtrer la liste des instances de bases de données, pour Filter databases (Filtrer les bases de donnée), saisissez une chaîne de texte pour Amazon RDS à utiliser pour filtrer les résultats. Seules les instances de bases de données dont les noms contiennent cette chaîne apparaissent.

3. Choisissez l'instance de base de données avec les E/S par seconde provisionnées que vous souhaitez modifier.
4. Sélectionnez Modify.
5. Sur la page Modify DB Instance (Modifier l'instance de base de données), choisissez les IOPS provisionnés pour Storage type (Type de stockage), puis fournissez une valeur d'IOPS provisionnés.

   Si la valeur que vous spécifiez pour Allocated Storage (Stockage alloué) ou IOPS provisionnées sort des limites prises en charge par l'autre paramètre, un message d'avertissement s'affiche. Ce message indique la plage de valeurs requise pour l'autre paramètre.
6. Choisissez Continue.
7. Pour appliquer immédiatement les modifications de l'instance de base de données, choisissez Appliquer immédiatement dans la section Scheduling of modifications (Planification des modifications). Ou choisissez Appliquer lors de la prochaine fenêtre de maintenance planifiée pour appliquer les modifications pendant la prochaine fenêtre de maintenance.

   Une interruption immédiate a lieu lorsque le type de stockage change. Pour plus d'informations sur le stockage, consultez Stockage d'instance de base de données Amazon RDS (p. 30).
8. Passez en revue les paramètres à modifier et choisissez Modification d'une instance de base de données pour terminer la modification.

   La nouvelle valeur définie pour le stockage alloué ou pour le stockage des IOPS provisionnées apparaît dans la colonne Statut.

AWS CLI

Pour modifier le paramètre de stockage des IOPS provisionnées pour une instance de base de données, utilisez la commande `modify-db-instance` de l'AWS CLI. Définissez les paramètres suivants :

- `--storage-type` – Attribuez la valeur `io1` pour les IOPS provisionnés.
- `--allocated-storage` – Volume de stockage à allouer pour l'instance de base de données, en gibioctets.
- `--iops` – Nouveau volume de stockage des IOPS provisionnées pour l'instance de base de données, exprimé en opérations d'I/O par seconde.
- `--apply-immediately` – Utilisez `--apply-immediately` pour appliquer les modifications immédiatement. Utilisez `--no-apply-immediately` (valeur par défaut) pour appliquer les modifications pendant la prochaine fenêtre de maintenance.

API Amazon RDS

Pour modifier les paramètres des IOPS provisionnées pour une instance de base de données, utilisez l'opération d'API Amazon RDS `ModifyDBInstance`. Définissez les paramètres suivants :

- `StorageType` – Attribuez la valeur `io1` pour les IOPS provisionnés.
- `AllocatedStorage` – Volume de stockage à allouer pour l'instance de base de données, en gibioctets.
- `Iops` – Nouveau débit IOPS pour l'instance de bases de données, exprimé en opérations d'I/O par seconde.
- `ApplyImmediately` – Définissez cette option sur `True` pour appliquer les modifications immédiatement. Définissez cette option sur `False` (valeur par défaut) pour appliquer les modifications au cours de la prochaine fenêtre de maintenance.

Suppression d'une instance de base de données

Pour supprimer une instance de base de données, procédez comme suit :

- Fournissez le nom de l'instance.
- Activez ou désactivez l'option permettant de créer un instantané de base de données final de l'instance.
- Activez ou désactivez l'option de conservation des sauvegardes automatiques.

Si l'instance de base de données que vous souhaitez supprimer possède un réplica en lecture, vous devez promouvoir ce dernier ou le supprimer. Pour plus d'informations, consultez Promotion d'un réplica en lecture en instance de bases de données autonome (p. 282).

> **Note**
>
> Lorsque le statut d'une instance de base de données est `deleting`, sa valeur de certificat d'autorité de certification n'apparaît pas dans la console RDS ou dans la sortie pour les commandes AWS CLI ou les opérations d'API RDS. Pour de plus amples informations sur les certificats d'autorité de certification, veuillez consulter Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).

Protection contre la suppression

Vous pouvez uniquement supprimer des instances dont la protection contre la suppression n'est pas activée. Lorsque vous créez ou modifiez une instance de base de données, vous avez la possibilité d'activer la protection contre la suppression de façon à ce que les utilisateurs ne puissent pas supprimer cette instance. La protection contre la suppression est désactivée par défaut pour vous lorsque vous utilisez des commandes de l'AWS CLI et de l'API. La protection contre la suppression est activée lorsque vous utilisez AWS Management Console pour créer une instance de base de données de production. Cependant, Amazon RDS applique la protection contre la suppression lorsque vous utilisez la console, l'interface de ligne de commande ou l'API pour supprimer une instance de base de données. Pour supprimer une instance de base de données dont la protection contre la suppression est activée, modifiez d'abord l'instance et désactivez la protection contre la suppression. L'activation ou la désactivation de la protection contre la suppression n'entraîne pas d'interruption de service.

Création d'un instantané final et conservation des sauvegardes automatiques

Lorsque vous supprimez une instance de base de données, vous pouvez choisir d'effectuer l'une des opérations suivantes ou les deux :

- Création d'un instantané de base de données final.
  - Pour pouvoir restaurer ultérieurement votre instance de base de données supprimée, créez un instantané de bases de données final. L'instantané final est conservé, ainsi que tous les instantanés manuels qui ont été pris.
  - Pour supprimer rapidement une instance de base de données, vous pouvez ignorer la création d'un instantané de base de données final.

    Note

    Il est impossible de créer un instantané de base de données final de votre instance de base de données s'il se trouve dans un des états suivants : `creating`, `failed`, `incompatible-restore` ou `incompatible-network`. Pour de plus amples informations, veuillez consulter Statut d'instance de bases de données (p. 386).
- Conservation des sauvegardes automatiques.
  - Vos sauvegardes automatiques sont conservées pendant la période de conservation définie sur l'instance de base de données au moment où vous la supprimez. Cette période de conservation définie intervient que vous choisissiez ou non de créer un instantané de bases de données final.
  - Si vous ne choisissez pas de conserver les sauvegardes automatiques, elles sont effacées et ne peuvent pas être récupérées après la suppression de l'instance de base de données.
  - Vous n'avez généralement pas besoin de conserver les sauvegardes automatiques si vous créez un instantané de base de données final.
  - Pour supprimer une sauvegarde automatique conservée, suivez les instructions définies dans Suppression des sauvegardes automatisées conservées (p. 325)

    Important

    Si vous ignorez l'instantané de base de données final, effectuez l'une des opérations suivantes pour restaurer votre instance de base de données :

    - Utilisation d'un ancien instantané manuel de l'instance de base de données pour restaurer celle-ci à l'instant précis de cet instantané de base de données.
    - Conservation des sauvegardes automatiques. Vous pouvez les utiliser pour restaurer votre instance de base de données pendant la période de conservation, mais pas après cette dernière.

    Note

    Quel que soit votre choix, les instantanés de base de données manuels ne sont pas supprimés. Pour plus d'informations sur les instantanés, consultez Création d'un instantané de base de données (p. 327).

Suppression d'une instance DB

Vous pouvez supprimer une instance de base de données à l'aide de la AWS Management Console, de l'AWS CLI ou de l'API RDS. Le temps nécessaire à la suppression d'une instance de base de données peut varier en fonction de la période de conservation de la sauvegarde (c'est-à-dire du nombre de sauvegardes à supprimer), de la quantité de données supprimées et de la réalisation d'un instantané final.

Note

Vous ne pouvez pas supprimer une instance de base de données lorsque la protection contre la suppression est activée pour celle-ci. Pour plus d'informations, consultez Protection contre la suppression (p. 313).

Vous pouvez désactiver la protection contre la suppression en modifiant l'instance de base de données. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Console

Pour supprimer une instance de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Bases de données, puis l'instance de base de données que vous souhaitez supprimer.
3. Pour Actions, choisissez Supprimer.
4. Pour créer un instantané de base de données final pour l'instance de base de données, choisissez Create final snapshot? (Créer un instantané final ?).
5. Si vous avez choisi de créer un instantané final, entrez le paramètre Final snapshot name (Nom de l'instantané final).
6. Pour conserver les sauvegardes automatiques, choisissez Conserver les sauvegardes automatiques.
7. Saisissez **`delete me`** dans la zone.
8. Sélectionnez Delete.

AWS CLI

Pour supprimer une instance de base de données à l'aide de l'AWS CLI, appelez la commande delete-db-instance avec les options suivantes :

- `--db-instance-identifier`
- `--final-db-snapshot-identifier` ou `--skip-final-snapshot`

Example Avec un instantané final et sans conservation des sauvegardes automatiques

Pour Linux, macOS ou Unix :

```
aws rds delete-db-instance \
    --db-instance-identifier mydbinstance \
    --final-db-snapshot-identifier mydbinstancefinalsnapshot \
    --delete-automated-backups
```

Pour Windows :

```
aws rds delete-db-instance ^
    --db-instance-identifier mydbinstance ^
    --final-db-snapshot-identifier mydbinstancefinalsnapshot ^
    --delete-automated-backups
```

Example Avec conservation des sauvegardes automatiques et pas d'instantané final

Pour Linux, macOS ou Unix :

```
aws rds delete-db-instance \
    --db-instance-identifier mydbinstance \
    --skip-final-snapshot \
    --no-delete-automated-backups
```

Pour Windows :

```
aws rds delete-db-instance ^
    --db-instance-identifier mydbinstance ^
    --skip-final-snapshot ^
    --no-delete-automated-backups
```

API RDS

Pour arrêter une instance de base de données à l'aide l'API Amazon RDS, appelez l'opération `DeleteDBInstance` avec les paramètres suivants :

- `DBInstanceIdentifier`
- `FinalDBSnapshotIdentifier` ou `SkipFinalSnapshot`

Example Avec un instantané final et sans conservation des sauvegardes automatiques

```
https://rds.amazonaws.com/
    ?Action=DeleteDBInstance
    &DBInstanceIdentifier=mydbinstance
    &FinalDBSnapshotIdentifier=mydbinstancefinalsnapshot
    &DeleteAutomatedBackups=true
    &SignatureMethod=HmacSHA256
    &SignatureVersion=4
    &Version=2014-10-31
    &X-Amz-Algorithm=AWS4-HMAC-SHA256
    &X-Amz-Credential=AKIADQKE4SARGYLE/20140305/us-west-1/rds/aws4_request
    &X-Amz-Date=20140305T185838Z
    &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
    &X-Amz-Signature=b441901545441d3c7a48f63b5b1522c5b2b37c137500c93c45e209d4b3a064a3
```

Example Avec conservation des sauvegardes automatiques et pas d'instantané final

```
https://rds.amazonaws.com/
    ?Action=DeleteDBInstance
    &DBInstanceIdentifier=mydbinstance
    &SkipFinalSnapshot=true
    &DeleteAutomatedBackups=false
    &SignatureMethod=HmacSHA256
    &SignatureVersion=4
    &Version=2014-10-31
    &X-Amz-Algorithm=AWS4-HMAC-SHA256
    &X-Amz-Credential=AKIADQKE4SARGYLE/20140305/us-west-1/rds/aws4_request
    &X-Amz-Date=20140305T185838Z
    &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
    &X-Amz-Signature=b441901545441d3c7a48f63b5b1522c5b2b37c137500c93c45e209d4b3a064a3
```

Sauvegarde et restauration d'une instance de base de données Amazon RDS

Cette section indique comment sauvegarder et restaurer une instance de base de données.

Rubriques

- Utilisation des sauvegardes (p. 317)
- Création d'un instantané de base de données (p. 327)
- Restauration à partir d'un instantané de base de données (p. 329)
- Copie d'un instantané (p. 332)
- Partage d'un instantané de de base de données (p. 342)
- Exportation de données d'instantanés de bases de données vers Amazon S3 (p. 349)
- Restauration d'une instance de base de données à une date spécifiée (p. 365)
- Suppression d'un instantané (p. 367)
- Didacticiel : restaurer une instance de base de données à partir d'un instantané de base de données (p. 368)

Utilisation des sauvegardes

Amazon RDS crée et enregistre des sauvegardes automatiques de votre instance de base de données pendant la fenêtre de sauvegarde de votre instance de base de données. RDS crée un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière et non pas seulement les bases de données individuelles. RDS enregistre les sauvegardes automatiques de votre instance de base de données selon la période de rétention des sauvegardes que vous spécifiez. Le cas échéant, vous pouvez récupérer votre base de données à tout moment pendant la période de rétention des sauvegardes.

Les sauvegardes automatiques suivent ces règles :

- Votre instance de base de données doit être dans l'état `AVAILABLE` pour que des sauvegardes automatiques soient exécutées. Les sauvegardes automatiques ne sont pas exécutées si vos instances de base de données sont dans un état autre que `AVAILABLE`, par exemple `STORAGE_FULL`.
- Les sauvegardes automatiques et les instantanés automatiques ne sont pas exécutés pendant l'exécution d'une copie dans la même région pour la même instance de base de données.

Vous pouvez également sauvegarder votre instance de base de données manuellement, en créant manuellement un instantané de bases de données. Pour plus d'informations sur la création d'un instantané de base de données, consultez Création d'un instantané de base de données (p. 327).

Le premier instantané d'une instance de base de données contient les données de l'instance de base de données complète. Les instantanés suivants de la même instance de base de données incrémentés, ce qui signifie que seules les données qui ont changé depuis l'instantané le plus récent sont enregistrées.

Vous pouvez copier des instantanés de base de données automatiques et manuels, et partager les instantanés de base de données manuels. Pour plus d'informations sur la copie des instantanés de base de données, consultez Copie d'un instantané (p. 332). Pour de plus amples informations sur le

partage des instantanés de base de données, veuillez consulter Partage d'un instantané de de base de données (p. 342).

> Note
>
> Vous pouvez aussi utiliser AWS Backup pour gérer les sauvegardes des instances de base de données Amazon RDS. Les sauvegardes gérées par AWS Backup sont considérées comme des instantanés de base de données manuels, mais ne sont pas prises en compte dans le quota d'instantanés de base de données pour RDS. Les noms des sauvegardes créées avec AWS Backup se terminent par `awsbackup:AWS-Backup-job-number`. Pour de plus amples informations sur AWS Backup, veuillez consulter le Manuel du développeur AWS Backup.

Stockage de sauvegarde

Votre stockage de sauvegarde Amazon RDS pour chaque région est composé des sauvegardes automatiques et de snapshots DB manuels pour cette région. L'espace de stockage de sauvegarde total est égal à la somme des ressources de stockage de toutes les sauvegardes de cette région. Le déplacement d'un instantané de base de données vers une autre région augmente le stockage de sauvegarde dans la région de destination. Les sauvegardes sont stockées dans Amazon S3.

Pour de plus amples informations sur les coûts de stockage des sauvegardes, veuillez consulter Tarification Amazon RDS.

Si vous avez choisi de conserver les sauvegardes automatiques lorsque vous supprimez une instance de base de données, les sauvegardes automatiques sont stockées pour toute la période de rétention. Si vous ne choisissez pas Conserver les sauvegardes automatiques lors de la suppression d'une instance de base de données, toutes les sauvegardes automatiques sont supprimées en même temps que l'instance. Une fois supprimées, les sauvegardes automatiques ne peuvent pas être récupérées. Si Amazon RDS crée un instantané de base de données final avant de supprimer votre instance de base de données, vous pouvez l'utiliser pour récupérer votre instance de base de données. Vous pouvez également utiliser un instantané manuel créé précédemment. Les instantanés manuels ne sont pas supprimés. Vous pouvez avoir jusqu'à 100 instantanés manuels par région.

Fenêtre de sauvegarde

Les sauvegardes automatiques sont exécutées chaque jour pendant la fenêtre de sauvegarde préférée. Si la sauvegarde a besoin de plus de temps que la durée allouée par la fenêtre de sauvegarde, elle continue après la fin de la fenêtre jusqu'à ce qu'elle soit terminée. La fenêtre de sauvegarde ne peut pas chevaucher la fenêtre de maintenance hebdomadaire pour l'instance de base de données.

Pendant la fenêtre de sauvegarde automatique, les E/S de stockage peuvent être suspendues brièvement tandis que le processus de sauvegarde s'initialise (généralement en quelques secondes). Vous pouvez rencontrer des latences élevées pendant quelques minutes lors de sauvegardes de déploiements multi-AZ. Pour MariaDB, MySQL, Oracle et PostgreSQL, l'activité E/S n'est pas suspendue sur votre instance principale lors de la sauvegarde pour les déploiements multi-AZ, car la sauvegarde est prise à partir de l'instance de secours. Pour SQL Server, l'activité E/S est suspendue brièvement pendant la sauvegarde pour les déploiements multi-AZ.

Si vous ne spécifiez pas une fenêtre de sauvegarde préférée lorsque vous créez l'instance de base de données, Amazon RDS attribue une fenêtre de sauvegarde par défaut de 30 minutes. Cette fenêtre est sélectionnée de manière aléatoire sur un bloc horaire de 8 heures pour chaque région AWS. Le tableau suivant répertorie les blocs de temps de chaque région, à partir desquels les fenêtres de sauvegardes par défaut sont affectées.

Région	Bloc chronologique
Région USA Est (Ohio)	03:00–11:00 UTC

Région	Bloc chronologique
Région USA Est (Virginie du N.)	03:00–11:00 UTC
Région USA Ouest (Californie du Nord)	06:00–14:00 UTC
Région USA Ouest (Oregon)	06:00–14:00 UTC
Région Asie-Pacifique (Hong Kong)	06:00–14:00 UTC
Région Asie-Pacifique (Mumbai)	16:30–00:30 UTC
Région Asie-Pacifique (Osaka-Local)	00:00–08:00 UTC
Région Asie-Pacifique (Séoul)	13:00–21:00 UTC
Région Asie-Pacifique (Singapour)	14:00–22:00 UTC
Région Asie-Pacifique (Sydney)	12:00–20:00 UTC
Région Asie-Pacifique (Tokyo)	13:00–21:00 UTC
Région Canada (Centre)	06:29–14:29 UTC
Région Chine (Pékin)	06:00–14:00 UTC
Région Chine (Ningxia)	06:00–14:00 UTC
Région Europe (Francfort)	20:00–04:00 UTC
Région Europe (Irlande)	22:00–06:00 UTC
Région Europe (Londres)	06:00–14:00 UTC
Région Europe (Paris)	07:29–14:29 UTC
Région Europe (Stockholm)	23:00–07:00 UTC
Région Moyen-Orient (Bahrain)	06:00–14:00 UTC
Région Amérique du Sud (São Paulo)	23:00–07:00 UTC
AWS GovCloud (USA Ouest)	03:00–11:00 UTC

Période de rétention des sauvegardes

Vous pouvez configurer une période de rétention des sauvegardes lorsque vous créez une instance de base de données. Si vous ne configurez pas la période de rétention des sauvegardes, la période par défaut est d'un jour si vous créez l'instance de base de données à l'aide de l'API Amazon RDS ou de l'AWS CLI. La période de rétention des sauvegardes par défaut est de sept jours si vous créez l'instance de base de

données à l'aide de la console. Après avoir créé une instance de base de données, vous pouvez modifier la période de rétention des sauvegardes. Vous pouvez définir la période de rétention des sauvegardes entre 0 et 35 jours. Le réglage de la période de rétention des sauvegardes sur 0 désactive les sauvegardes automatisées. La limite des snapshots manuels (100 par région) ne s'applique pas aux sauvegardes automatiques.

> **Important**
>
> Une interruption se produit si vous modifiez la période de rétention des sauvegardes de 0 à une valeur non nulle, ou d'une valeur non nulle à 0.

Désactivation des sauvegardes automatiques

Vous pouvez avoir besoin de désactiver temporairement les sauvegardes automatiques dans certains cas, par exemple lorsque vous chargez un important volume de données.

> **Important**
>
> Nous vous déconseillons vivement de désactiver les sauvegardes automatiques car cela désactive la restauration à un instant dans le passé. Le fait de désactiver les sauvegardes automatiques pour une instance de base de données supprime toutes les sauvegardes automatiques existantes pour l'instance. Si vous désactivez puis réactivez les sauvegardes automatiques, vous ne pourrez faire de restauration que lorsque ces dernières seront réactivées.

Dans cet exemple, vous désactivez les sauvegardes automatiques pour une instance de base de données nommée mydbinstance en définissant le paramètre de rétention des sauvegardes sur 0.

Console

Pour désactiver immédiatement les sauvegardes automatiques

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Bases de données, puis l'instance de base de données que vous souhaitez modifier.
3. Sélectionnez Modify. La page Modifier l'instance de base de données s'affiche.
4. Pour Période de rétention des sauvegardes, choisissez 0 jours.
5. Choisissez Continue.
6. Choisissez Appliquer immédiatement.
7. Sur la page de confirmation, choisissez Modifier l'instance de base de données pour enregistrer vos modifications et désactiver les sauvegardes automatiques.

AWS CLI

Pour désactiver immédiatement les sauvegardes automatiques, utilisez la commande modify-db-instance et configurez la période de rétention des sauvegardes sur 0 avec `--apply-immediately`.

Example

L'exemple suivant désactive immédiatement les sauvegardes automatiques.

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
```

```
    --db-instance-identifier mydbinstance \
    --backup-retention-period 0 \
    --apply-immediately
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --backup-retention-period 0 ^
    --apply-immediately
```

Pour savoir quand la modification est appliquée, appelez la commande `describe-db-instances` pour l'instance de base de données jusqu'à ce que la valeur pour la période de rétention des sauvegardes soit à 0 et que l'état mydbinstance soit disponible.

```
aws rds describe-db-instances --db-instance-identifier mydbinstance
```

API RDS

Pour désactiver immédiatement les sauvegardes automatisées, appelez l'opération ModifyDBInstance avec les paramètres suivants :

- `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>
```

Activation des sauvegardes automatiques

Si les sauvegardes automatiques ne sont pas activées pour votre instance de base de données, vous pouvez les activer à tout moment. Vous activez les sauvegardes automatiques en définissant la période de rétention des sauvegardes sur une valeur positive différente de zéro. Lorsque les sauvegardes automatiques sont activées, votre instance et votre base de données RDS sont mises hors ligne, et une sauvegarde est immédiatement créée.

Dans cet exemple, vous activez les sauvegardes automatiques pour une instance de bases de données nommée mydbinstance en définissant la période de rétention des sauvegardes sur une valeur positive différente de zéro (dans ce cas, 3).

Console

Pour activer immédiatement les sauvegardes automatiques

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.

2. Dans le panneau de navigation, choisissez Bases de données, puis l'instance de base de données que vous souhaitez modifier.
3. Sélectionnez Modify. La page Modifier l'instance de base de données s'affiche.
4. Pour Période de rétention des sauvegardes, choisissez une valeur positive différente de zéro, par exemple 3 jours.
5. Choisissez Continue.
6. Choisissez Appliquer immédiatement.
7. Sur la page de confirmation, choisissez Modifier l'instance de bases de données pour enregistrer vos modifications et activer les sauvegardes automatiques.

AWS CLI

Pour activer immédiatement les sauvegardes automatiques, utilisez la commande `modify-db-instance` de l'AWS CLI.

Dans cet exemple, nous activons les sauvegardes automatiques en configurant la période de rétention des sauvegardes sur trois jours.

Incluez les paramètres suivants :

- `--db-instance-identifier`
- `--backup-retention-period`
- `--apply-immediately` ou `--no-apply-immediately`

Example

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance  \
    --backup-retention-period 3 \
    --apply-immediately
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance  ^
    --backup-retention-period 3 ^
    --apply-immediately
```

API RDS

Pour activer immédiatement les sauvegardes automatiques, utilisez l'opération `ModifyDBInstance` de l'API RDS.

Dans cet exemple, nous activons les sauvegardes automatiques en configurant la période de rétention des sauvegardes sur trois jours.

Incluez les paramètres suivants :

- `DBInstanceIdentifier`
- `BackupRetentionPeriod`

- `ApplyImmediately = true`

Example

```
https://rds.amazonaws.com/
 ?Action=ModifyDBInstance
 &DBInstanceIdentifier=mydbinstance
 &BackupRetentionPeriod=3
 &ApplyImmediately=true
 &SignatureVersion=2
 &SignatureMethod=HmacSHA256
 &Timestamp=2009-10-14T17%3A48%3A21.746Z
 &AWSAccessKeyId=<AWS Access Key ID>
 &Signature=<Signature>
```

Conservation des sauvegardes automatiques

Lorsque vous supprimez une instance de base de données, vous pouvez choisir de conserver les sauvegardes automatiques.

Les sauvegardes automatiques conservées contiennent des instantanés système et des journaux de transactions d'une instance de base de données. Elles incluent également les propriétés de votre instance de base de données (stockage alloué et classe de l'instance, par exemple) nécessaires pour la restaurer en tant qu'instance active.

Vous pouvez conserver des sauvegardes automatiques pour des instances RDS qui exécutent les moteurs suivants : MySQL, MariaDB, PostgreSQL, Oracle et Microsoft SQL Server.

Vous pouvez restaurer ou supprimer des sauvegardes automatiques conservées à l'aide d'AWS Management Console, de l'API RDS et de l'AWS CLI.

Rubriques

- Période de conservation (p. 323)
- Restauration (p. 324)
- Coûts de conservation (p. 324)
- Limitations et recommandations (p. 324)
- Suppression des sauvegardes automatisées conservées (p. 325)

Période de conservation

Les instantanés système et les journaux de transactions contenus dans une sauvegarde automatique conservée expirent de la même façon que pour l'instance de base de données source. Dans la mesure où aucun nouvel instantané ni journal n'est créé pour cette instance, les sauvegardes automatiques conservées finissent par toutes expirer. En effet, elles perdurent aussi longtemps que l'aurait fait leur dernier instantané système, sur la base des paramètres définis pour la période de rétention de l'instance source au moment où vous l'avez supprimée. Les sauvegardes automatiques conservées sont supprimées par le système après expiration de leur dernier instantané système.

Vous pouvez supprimer une sauvegarde automatique conservée de la même manière que vous supprimez une instance de base de données. Vous pouvez supprimer des sauvegardes automatiques conservées à l'aide de la console ou de l'opération `DeleteDBInstanceAutomatedBackup` de l'API RDS.

Les instantanés finaux sont indépendants des sauvegardes automatiques conservées. Nous vous recommandons vivement de réaliser un instantané final même si vous conservez les sauvegardes automatiques car celles-ci finissent par expirer. L'instantané final n'expire jamais.

Restauration

Pour afficher les sauvegardes automatiques conservées, basculez sur la page des sauvegardes automatiques. Vous pouvez afficher les instantanés individuels associés à une sauvegarde automatique conservée sur la page des instantanés de bases de données de la console. Vous pouvez également décrire les instantanés individuels associés à une sauvegarde automatique conservée. À partir de là, vous pouvez restaurer une instance de base de données directement à partir d'un de ces instantanés.

Les instances de base de données restaurées sont automatiquement associées aux groupes de paramètres et d'options par défaut. Cependant, vous pouvez appliquer un groupe de paramètres ou d'options personnalisé en le définissant au moment de la restauration.

Dans cet exemple, vous restaurez une instance de base de données à un moment donné dans le temps à l'aide de la sauvegarde automatique conservée. Pour commencer, décrivez vos sauvegardes automatiques conservées afin d'identifier celles à restaurer.

Pour décrire vos sauvegardes automatiques conservées à l'aide de l'API RDS, appelez l'action `DescribeDBInstanceAutomatedBackups` avec un des paramètres suivants :

- `DBInstanceIdentifier`
- `DbiResourceId`

```
aws rds describe-db-instance-automated-backups --db-instance-
identifier DBInstanceIdentifier
OR
aws rds describe-db-instance-automated-backups --dbi-resource-idDbiResourceId
```

Ensuite, pour restaurer votre sauvegarde automatique conservée à un moment donné dans le temps, à l'aide de l'API RDS, appelez l'action `RestoreDBInstanceToPointInTime` avec les paramètres suivants :

- `SourceDbiResourceId`
- `TargetDBInstanceIdentifier`

```
aws rds restore-db-instance-to-point-in-time --source-dbi-resource-id SourceDbiResourceId
 --target-db-instance-identifier TargetDBInstanceIdentifier --use-latest-restorable-time
```

Coûts de conservation

Le coût d'une sauvegarde automatique conservée correspond au coût du stockage total des instantanés système associés à la sauvegarde. Il n'y a pas de frais supplémentaires pour les journaux de transactions ou les métadonnées de l'instance. Toutes les autres règles de tarification des sauvegardes s'appliquent aux instances restaurables.

Par exemple, imaginons que l'espace de stockage total alloué pour les instances en cours d'exécution soit de 100 Go. Supposons également que vous ayez 50 Go d'instantanés manuels plus 75 Go d'instantanés système associés à une sauvegarde automatique conservée. Dans ce cas, seuls les 25 Go supplémentaires de stockage de sauvegarde vous sont facturés, comme suit : (50 Go + 75 Go) – 100 Go = 25 Go.

Limitations et recommandations

Les limitations suivantes s'appliquent aux sauvegardes automatiques conservées :

- Le nombre maximum de sauvegardes automatiques conservées dans une région AWS est de 40. Ce nombre n'est pas inclus dans la limite des instances de base de données. Vous pouvez avoir 40 instances de base de données en cours d'exécution et 40 sauvegardes automatiques conservées supplémentaires en même temps.
- Les sauvegardes automatiques conservées ne contiennent pas d'informations sur les paramètres ou les groupes d'options.
- Vous pouvez restaurer une instance supprimée jusqu'à une date déterminée dans le passé comprise dans la période de rétention au moment de la suppression.
- Une sauvegarde automatique conservée ne peut pas être modifiée car elle contient des sauvegardes système, des journaux de transactions et des propriétés d'instance de base de données qui existaient au moment de la suppression de l'instance source.

Suppression des sauvegardes automatisées conservées

Vous pouvez supprimer les sauvegardes automatiques conservées quand elles ne sont plus nécessaires.

Console

Pour supprimer une sauvegarde automatisée conservée

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Automated backups (Sauvegardes automatisées).
3. Choisissez Retained (Conservées).

4. Choisissez la sauvegarde automatisée conservée que vous souhaitez supprimer.
5. Pour Actions, choisissez Supprimer.
6. Dans la page de confirmation, entrez **`delete me`** et choisissez Delete (Supprimer).

AWS CLI

Vous pouvez supprimer une sauvegarde automatisée conservée à l'aide de la commande de l'AWS CLI delete-db-instance-automated-backup.

Les options suivantes sont utilisées pour supprimer une sauvegarde automatisée conservée.

- `--dbi-resource-id` – Identifiant de la ressource de l'instance de base de données source.

Vous pouvez rechercher l'identifiant ressource de l'instance de base de données source d'une sauvegarde automatisée conservée en exécutant la commande de l'AWS CLI describe-db-instance-automated-backups.

Example

L'exemple suivant supprime la sauvegarde automatisée conservée avec l'identifiant de ressource d'instance de base de données `db-123ABCEXAMPLE`.

Pour Linux, macOS ou Unix :

```
aws rds delete-db-instance-automated-backup \
    --dbi-resource-id db-123ABCEXAMPLE
```

Pour Windows :

```
aws rds delete-db-instance-automated-backup ^
    --dbi-resource-id db-123ABCEXAMPLE
```

API RDS

Vous pouvez supprimer une sauvegarde automatisée conservée à l'aide de la commande de l'opération d'API Amazon RDS DeleteDBInstanceAutomatedBackup.

Les paramètres suivants permettent de supprimer une sauvegarde automatisée conservée :

- `DbiResourceId` – Identifiant de la ressource de l'instance de base de données source.

  Vous pouvez rechercher l'identifiant ressource de l'instance de base de données source d'une sauvegarde automatisée conservée à l'aide de l'opération de l'API Amazon RDS DescribeDBInstanceAutomatedBackups.

Sauvegardes automatiques avec moteurs de stockage MySQL non pris en charge

Pour le moteur de base de données MySQL, les sauvegardes automatiques sont uniquement prises en charge pour le moteur de stockage InnoDB. L'utilisation de ces fonctions avec d'autres moteurs de stockage MySQL, dont MyISAM, peut entraîner un comportement peu fiable lors de la restauration à partir de sauvegardes. Plus précisément, dans la mesure où les moteurs de stockage comme MyISAM n'assurent pas une récupération sur incident fiable, vos tables risquent d'être corrompues en cas d'incident. Pour cette raison, nous vous invitons à utiliser le moteur de stockage InnoDB.

- Pour convertir des tables MyISAM existantes en tables InnoDB, vous pouvez utiliser la commande `ALTER TABLE` (par exemple, `ALTER TABLE table_name ENGINE=innodb, ALGORITHM=COPY;`).
- Si vous choisissez d'utiliser MyISAM, vous pouvez essayer de réparer manuellement les tables endommagées après un incident à l'aide de la commande `REPAIR`. Pour de plus amples informations, veuillez consulter la section Instruction REPAIR TABLE dans la documentation de MySQL. Cependant, comme indiqué dans la documentation MySQL, il y a de fortes chances que vous ne puissiez pas récupérer toutes vos données.
- Si vous souhaitez prendre un instantané de vos tables MyISAM avant la restauration, procédez comme suit :
  1. Arrêtez toutes les activités de vos tables MyISAM (autrement dit, fermez toutes les sessions).

Vous pouvez fermer toutes les sessions en appelant la commande mysql.rds_kill pour chaque processus retourné à partir de la commande `SHOW FULL PROCESSLIST`.

2. Verrouillez et videz chacune de vos tables MyISAM. Par exemple, les commandes suivantes verrouillent et vident deux tables nommées `myisam_table1` et `myisam_table2` :

```
mysql> FLUSH TABLES myisam_table, myisam_table2 WITH READ LOCK;
```

3. Créez un instantané de votre instance de base de données. Une fois l'instantané terminé, libérez les verrous et reprenez l'activité sur les tables MyISAM. Vous pouvez libérer les verrous sur vos tables à l'aide de la commande suivante :

```
mysql> UNLOCK TABLES;
```

Ces étapes obligent MyISAM à vider sur disque les données stockées en mémoire, ce qui garantit un démarrage propre lors d'une restauration à partir d'un instantané de bases de données. Pour plus d'informations sur la création d'un instantané de base de données, consultez Création d'un instantané de base de données (p. 327).

Sauvegardes automatiques avec moteurs de stockage MariaDB non pris en charge

Pour le moteur de base de données MariaDB, les sauvegardes automatiques sont uniquement prises en charge avec le moteur de stockage InnoDB (version 10.2 et suivante) et le moteur de stockage XtraDB (versions 10.0 et 10.1). L'utilisation de ces fonctions avec d'autres moteurs de stockage MariaDB, dont Aria, peut entraîner un comportement peu fiable lors de la restauration à partir de sauvegardes. Même si Aria est une solution de remplacement résistante aux incidents de myISAM, vos tables risquent toujours d'être endommagées en cas d'incident. Pour cette raison, nous vous invitons à utiliser le moteur de stockage XtraDB.

- Pour convertir les tables Aria existantes en tables InnoDB, vous pouvez utiliser la commande `ALTER TABLE`. Par exemple : `ALTER TABLE table_name ENGINE=innodb, ALGORITHM=COPY;`
- Pour convertir les tables Aria existantes en tables XtraDB, vous pouvez utiliser la commande `ALTER TABLE`. Par exemple : `ALTER TABLE table_name ENGINE=xtradb, ALGORITHM=COPY;`
- Si vous choisissez d'utiliser Aria, vous pouvez essayer de réparer manuellement les tables endommagées après un incident à l'aide de la commande `REPAIR TABLE`. Pour plus d'informations, consultez http://mariadb.com/kb/en/mariadb/repair-table/.
- Si vous souhaitez prendre un instantané de vos tables Aria avant la restauration, procédez comme suit :
  1. Arrêtez toutes les activités de vos tables Aria (autrement dit, fermez toutes les sessions).
  2. Verrouillez et videz chacune de vos tables Aria.
  3. Créez un instantané de votre instance de base de données. Une fois l'instantané terminé, libérez les verrous et reprenez l'activité sur les tables Aria. Ces étapes obligent Aria à vider sur disque les données stockées en mémoire et à garantir ainsi un démarrage propre lors d'une restauration à partir d'un instantané de base de données.

Création d'un instantané de base de données

Amazon RDS crée un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière et non pas seulement les bases de données. La création de

cet instantané de base de données sur une instance de base de données mono-AZ entraîne une brève interruption E/S qui peut durer de quelques secondes à quelques minutes, en fonction de la taille et de la classe de votre instance de base de données. Pour MariaDB, MySQL, Oracle et PostgreSQL, l'activité E/S n'est pas suspendue sur votre instance principale lors de la sauvegarde pour les déploiements multi-AZ, car la sauvegarde est prise à partir de l'instance de secours. Pour SQL Server, l'activité E/S est suspendue brièvement pendant la sauvegarde pour les déploiements multi-AZ.

Lorsque vous créez un snapshot DB, vous devez identifier quelle instance de base de données vous allez sauvegarder, puis nommer votre snapshot DB afin de pouvoir effectuer une restauration à partir de ce dernier ultérieurement. Le temps nécessaire à la création d'un instantané varie en fonction de la taille de vos bases de données. Étant donné que l'instantané inclut l'intégralité du volume de stockage, la taille des fichiers, comme les fichiers temporaires, a également une incidence sur le temps nécessaire à la création de l'instantané.

> Note
>
> Pour les instances de base de données PostgreSQL, les données des tables non journalisées peuvent ne pas être restaurées à partir d'instantanés. Pour plus d'informations, consultez Bonnes pratiques pour utiliser les moteurs de stockage PostgreSQL (p. 142).

Contrairement aux sauvegardes automatisées, les instantanés manuels ne sont pas soumis à la période de rétention des sauvegardes. Les instantanés n'expirent pas.

Pour les sauvegardes à très long terme des données MariaDB, MySQL et PostgreSQL, nous vous recommandons d'exporter les données d'instantané vers Amazon S3. Si la version majeure de votre moteur de base de données n'est plus prise en charge, vous ne pouvez pas restaurer cette version à partir d'un instantané. Pour de plus amples informations, veuillez consulter Exportation de données d'instantanés de bases de données vers Amazon S3 (p. 349).

Vous pouvez créer un instantané de base de données en utilisant la AWS Management Console, l'AWS CLI ou l'API RDS.

Console

Pour créer un instantané de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Dans la liste d'instances de base de données, choisissez l'instance de base de données pour laquelle vous souhaitez prendre un instantané.
4. Sous Actions, choisissez Prendre un instantané.

   La fenêtre Take DB Snapshot (Prendre un instantané de base de données) apparaît.
5. Dans la zone Nom de l'instantané, entrez le nom de l'instantané.

6. Choisissez Prendre un instantané.

AWS CLI

Lorsque vous créez un instantané de base de données à l'aide de l'AWS CLI, vous devez identifier quelle instance de base de données vous allez sauvegarder, puis nommer votre instantané de base de données afin de pouvoir effectuer une restauration à partir de ce dernier ultérieurement. Pour ce faire, vous pouvez utiliser la commande `create-db-snapshot` de l'AWS CLI, avec les paramètres suivants :

- `--db-instance-identifier`
- `--db-snapshot-identifier`

Dans cet exemple, vous créez un instantané de base de données appelé *`mydbsnapshot`* pour une instance de base de données appelée *`mydbinstance`*.

Example

Pour Linux, macOS ou Unix :

```
aws rds create-db-snapshot \
    --db-instance-identifier mydbinstance \
    --db-snapshot-identifier mydbsnapshot
```

Pour Windows :

```
aws rds create-db-snapshot ^
    --db-instance-identifier mydbinstance ^
    --db-snapshot-identifier mydbsnapshot
```

API RDS

Lorsque vous créez un instantané de base de données à l'aide de l'API Amazon RDS, vous devez identifier quelle instance de base de données vous allez sauvegarder, puis nommer votre instantané de base de données afin de pouvoir effectuer une restauration à partir de ce dernier ultérieurement. Pour ce faire, vous pouvez utiliser la commande `CreateDBSnapshot` de l'API Amazon RDS, avec les paramètres suivants :

- `DBInstanceIdentifier`
- `DBSnapshotIdentifier`

Restauration à partir d'un instantané de base de données

Amazon RDS crée un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière et non seulement les bases de données. Vous pouvez créer une instance de base de données en effectuant une restauration à partir de cet instantané de de base de données. Lorsque vous restaurez la/l'instance de base de données, vous indiquez le nom de l'instantané de de base de données à partir duquel la restauration est effectuée, puis un nom pour la nouvelle instance de base de données créée à partir de l'opération de restauration. Vous ne pouvez pas restaurer un instantané de base de données sur une instance de base de données qui existe déjà ; le système crée une nouvelle instance de base de données lors de la restauration.

Vous pouvez restaurer une instance de base de données et utiliser un type de stockage différent que l'instantané de base de données source Dans ce cas, le processus de restauration est plus lent, à cause du travail supplémentaire nécessaire pour migrer les données vers le nouveau type de stockage. Si vous effectuez une restauration vers ou à partir d'un stockage magnétique, le processus de migration est plus lent. Ceci est dû au fait que le stockage magnétique ne dispose pas de la capacité IOPS du stockage IOPS provisionnés ou Usage général (SSD).

Note

Vous ne pouvez pas restaurer une instance de base de données à partir d'un instantané de base de données qui est à la fois partagé et chiffré. Par contre, vous pouvez créer une copie de l'instantané de base de données et restaurer l'instance de base de données à partir de cette copie.

Considérations relatives au groupe de paramètres

Nous vous recommandons de conserver le groupe de paramètres de tout instantané de base de données que vous créez, de telle sorte que vous puissiez associer votre instance de base de données restaurée au groupe de paramètres approprié. Vous pouvez spécifier le groupe de paramètres lorsque vous restaurez l'instance de base de données.

Considérations relatives aux groupes de sécurité

Lorsque vous restaurez une instance ou un de base de données, le groupe de sécurité par défaut est associé à l'instance ou au restauré par défaut.

Note

- Si vous utilisez la console Amazon RDS, vous pouvez spécifier un groupe de sécurité personnalisé à associer à l'instance ou créer un nouveau groupe de sécurité VPC.
- Si vous utilisez AWS CLI, vous pouvez spécifier un groupe de sécurité personnalisé pour l'associer à l'instance ou au en incluant l'option `--vpc-security-group-ids` dans la commande `restore-db-instance-from-db-snapshot`.
- Si vous utilisez l'API Amazon RDS, vous pouvez inclure le paramètre `VpcSecurityGroupIds.VpcSecurityGroupId.N` dans l'action `RestoreDBInstanceFromDBSnapshot`.

Dès que la restauration est terminée et que votre nouvelle instance de base de données est disponible, vous pouvez associer n'importe quel groupe de sécurité personnalisé utilisé par l'instantané dont vous vous êtes servi pour la restauration. Vous devez appliquer ces modifications en modifiant l'instance de base de données à l'aide de la console RDS, de la commande de l'AWS CLI `modify-db-instance` ou de l'opération d'API Amazon RDS `ModifyDBInstance`. Pour de plus amples informations, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

Considérations relatives au groupe d'options

Lorsque vous restaurez une instance de base de données, le groupe d'options associé à l'instantané de base de données est associé à l'instance de base de données restaurée après sa création. Par exemple, si l'instantané de base de données à partir duquel vous effectuez la restauration utilise Oracle Transparent Data Encryption, l'instance de base de données restaurée utilise le même groupe d'options.

Lorsque vous affectez un groupe d'options à une instance de base de données, il est également lié à la plateforme prise en charge sur laquelle se trouve l'instance de base de données, VPC ou EC2-Classic (non VPC). Si une instance de base de données est dans un VPC, le groupe d'options associé à l'instance de base de données est lié à ce VPC. Cela signifie que vous ne pouvez pas utiliser le groupe d'options assigné à une instance de base de données si vous tentez de restaurer l'instance dans un VPC différent

ou sur une autre plateforme. Si vous restaurez une instance de base de données dans un autre VPC ou sur une autre plateforme, vous devez attribuer le groupe d'options par défaut à l'instance, assigner un groupe d'options lié à ce VPC ou à cette plateforme, ou créer un groupe d'options et l'affecter à l'instance de base de données. Pour les options permanentes ou persistantes, lorsque vous restaurez une instance de base de données dans un VPC différent, vous devez créer un nouveau groupe d'options incluant l'option persistante ou permanente.

Considérations relatives à Microsoft SQL Server

Lorsque vous restaurez un instantané de base de données Microsoft SQL Server sur une nouvelle instance, vous pouvez toujours effectuer une restauration sur la même édition que votre instantané. Dans certains cas, vous pouvez également modifier l'édition de l'instance de base de données. Vous trouverez ci-dessous les limitations qui s'appliquent lors de la modification des éditions :

- L'instantané de base de données doit disposer de suffisamment de stockage alloué à la nouvelle édition.
- Seules les modifications d'édition suivantes sont prises en charge :
  - De Standard Edition vers Enterprise Edition
  - De Web Edition vers Standard Edition ou Enterprise Edition
  - D'Express Edition vers Web Edition, Standard Edition ou Enterprise Edition

Si vous voulez passer d'une édition à une nouvelle édition qui n'est pas prise en charge en restaurant un instantané, vous pouvez essayer d'utiliser la fonction de sauvegarde et de restauration native. SQL Server vérifie si votre base de données est compatible ou non avec la nouvelle édition en fonction des fonctionnalités SQL Server que vous avez activées sur la base de données. Pour plus d'informations, consultez Importation et exportation de bases de données SQL Server (p. 634).

Considérations relatives à Oracle

Si vous utilisez Oracle GoldenGate, conservez toujours le groupe de paramètres avec le paramètre `compatible`. Lorsque vous restaurez une instance de base de données depuis un instantané de base de données, vous devez spécifier le groupe de paramètres associé à une valeur de paramètre `compatible` correspondante ou supérieure.

Vous pouvez mettre à niveau un instantané de base de données pendant qu'il est encore un instantané de base de données, avant de le restaurer. Pour plus d'informations, consultez Mise à niveau d'un instantané de base de données Oracle (p. 988).

Restaurer à partir d'un instantané

Vous pouvez restaurer une instance de base de données à partir d'un instantané de base de données à l'aide de la AWS Management Console, de l'AWS CLI ou de l'API RDS.

Console

Pour restaurer une instance de base de données à partir d'un instantané de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Snapshots (Instantanés).
3. Choisissez l'instantané de base de données à partir duquel vous voulez restaurer.
4. Pour Actions, choisissez Restore Snapshot (Restaurer l'instantané).
5. Sur la page Restaurer l'instance DB, pour Identifiant de l'instance DB, saisissez le nom de votre instance de base de données restaurée.

6. Choisissez Restore DB Instance.

AWS CLI

Pour restaurer une instance de base de données à partir d'un instantané de base de données, utilisez la commande restore-db-instance-from-db-snapshot de l'AWS CLI.

Dans cet exemple, vous effectuez la restauration à partir d'un instantané de base de données créé auparavant, qui est nommé mydbsnapshot. La restauration s'effectue sur une nouvelle instance de base de données appelée mynewdbinstance.

Example

Pour Linux, macOS ou Unix :

```
aws rds restore-db-instance-from-db-snapshot \
    --db-instance-identifier mynewdbinstance \
    --db-snapshot-identifier mydbsnapshot
```

Pour Windows :

```
aws rds restore-db-instance-from-db-snapshot ^
    --db-instance-identifier mynewdbinstance ^
    --db-snapshot-identifier mydbsnapshot
```

La sortie générée lors de l'exécution de cette commande est semblable à ce qui suit :

```
DBINSTANCE  mynewdbinstance  db.m3.large  MySQL     50       sa              creating  3  n
  5.6.40  general-public-license
```

API RDS

Pour restaurer une instance de base de données à partir d'un instantané de base de données, appelez la fonction d'API Amazon RDS RestoreDBInstanceFromDBSnapshot avec les paramètres suivants :

- `DBInstanceIdentifier`
- `DBSnapshotIdentifier`

Copie d'un instantané

Avec Amazon RDS, vous pouvez copier les instantanés de de bases de données automatisés ou manuels. Après avoir copié un instantané, la copie est un instantané manuel.

Vous pouvez copier un instantané dans la même région AWS ou entre plusieurs régions AWS, ainsi que copier des instantanés partagés.

Limites

Vous trouverez ci-dessous certaines limites qui s'appliquent lorsque vous copiez des instantanés :

- Vous ne pouvez pas copier un instantané vers ou depuis régions AWS suivantes : Chine (Pékin) ou Chine (Ningxia).

- Vous pouvez copier un instantané entre les régions AWS GovCloud (US-East) et AWS GovCloud (US-West), mais pas entre ces régions AWS GovCloud (US) et d'autres régions AWS.
- Si vous supprimez un instantané source avant que l'instantané cible soit disponible, la copie d'instantané peut échouer. Vérifiez que l'instantané cible a le statut `AVAILABLE` avant de supprimer un instantané source.
- Vous pouvez avoir jusqu'à cinq demandes de copie d'instantanés en cours vers une même région de destination par compte.
- Selon les régions impliquées et le volume de données à copier, la copie d'un instantané entre régions peut prendre plusieurs heures. Dans le cas d'un grand nombre de demandes de copie d'instantané entre régions à partir d'une région AWS source donnée, Amazon RDS peut mettre en file d'attente les nouvelles demandes de copie entre régions provenant de cette région AWS source en attendant que certaines copies en cours se terminent. Aucune information d'avancement n'est affichée sur les demandes de copie quand elles sont en file d'attente. Les informations d'avancement sont affichées lorsque la copie commence.

Conservation des instantanés

Amazon RDS supprime les instantanés de base de données automatisés à la fin de leur période de rétention, lorsque vous désactivez les instantanés de base de données automatisés pour un d'instance de base de données ou lorsque vous supprimez un d'instance de base de données. Si vous souhaitez conserver un instantané de base de données à plus long terme, copiez-le pour créer un instantané de base de données manuel, qui sera conservé jusqu'à ce que vous le supprimiez. Des coûts de stockage Amazon RDS peuvent s'appliquer aux instantanés manuels si ces derniers dépassent votre espace de stockage par défaut.

Pour de plus amples informations sur les coûts de stockage des sauvegardes, veuillez consulter Tarification Amazon RDS.

Copie d'instantanés partagés

Vous pouvez copier des instantanés que d'autres comptes AWS ont partagés avec vous. Si vous copiez un instantané chiffré qui a été partagé à partir d'un autre compte AWS, vous devez avoir accès à la clé principale client (CMK) AWS KMS qui a permis de chiffrer l'instantané.

Vous pouvez copier un instantané de bases de données partagé d'une région à une autre, sous réserve que l'instantané ne soit pas chiffré. Cependant, si l'instantané de base de données partagé est chiffré, vous ne pouvez le copier que dans la même région AWS.

> Note
>
> La copie des instantanés incrémentiels partagés dans la même région AWS est prise en charge lorsqu'ils ne sont pas chiffrés ou chiffrés à l'aide de la même clé KMS AWS que l'instantané complet initial. Si vous utilisez une clé KMS différente pour chiffrer les instantanés suivants lors de leur copie, ces instantanés partagés sont des instantanés complets.

Gestion du chiffrement

Vous pouvez copier un instantané chiffré à l'aide d'une clé principale client (CMK) AWS KMS. Si vous copiez un instantané chiffré, la copie de l'instantané doit également être chiffrée. Si vous copiez un instantané chiffré dans la même région AWS, vous pouvez chiffrer la copie à l'aide de la même clé CMK AWS KMS que l'instantané d'origine ; vous pouvez également spécifier une autre clé CMK AWS KMS. Si vous copiez un instantané chiffré entre différentes régions, vous ne pouvez pas utiliser la même clé CMK AWS KMS pour la copie que celle utilisée pour l'instantané source, car les clés CMK AWS KMS sont spécifiques à une région. Vous devez, à la place, indiquer une clé CMK AWS KMS valide dans la région AWS de destination.

L'instantané source reste chiffré pendant tout le processus de copie. Pour plus d'informations, consultez Limitations des instances de base de données chiffrées Amazon RDS (p. 1524).

Vous pouvez également chiffrer une copie d'un instantané non chiffré. De cette façon, vous pouvez ajouter rapidement un chiffrement à une instance de base de données non chiffrée au préalable. En d'autres termes, vous pouvez créer un instantané de votre instance de base de données lorsque vous êtes prêt à la chiffrer, puis créer une copie de cet instantané et spécifier une clé CMK AWS KMS pour chiffrer votre copie de l'instantané. Vous pouvez ensuite restaurer une instance de base de données chiffrée à partir de l'instantané chiffré.

Copie d'instantané incrémentielle

Un instantané incrémentiel contient uniquement les données qui ont été modifiées après l'instantané le plus récent de la même instance de base de données. La copie d'instantanés incrémentiels est plus rapide est entraîne des coûts de stockage plus faibles que la copie d'instantanés complets. La copie d'instantanés incrémentiels d'une région AWS à l'autre est prise en charge pour les instantanés chiffrés et non chiffrés.

> Note
>
> Lorsque vous copiez un instantané source qui est une copie d'instantané, la nouvelle copie n'est pas incrémentielle car la copie d'instantané source ne comprend pas les métadonnées requises pour les copies incrémentielles.

L'aspect incrémentiel d'une copie d'instantané est déterminé par la dernière copie d'instantané effectuée. Si la dernière copie d'instantané a été supprimée, la copie suivante est une copie complète, non une copie incrémentielle. Si une copie est toujours en attente lorsque vous démarrez une autre copie, la deuxième copie ne démarre qu'une fois la première copie terminée.

Copie d'instantanés dans des régions AWS

Selon les régions AWS impliquées et le volume de données à copier, la copie d'un instantané entre régions peut prendre plusieurs heures. Dans certains cas, il peut y avoir un grand nombre de demandes de copie d'instantanés d'une région à une autre à partir d'une région AWS source donnée. Dans ces cas, Amazon RDS peut mettre en file d'attente les nouvelles demandes de copie entre régions provenant de cette région AWS source en attendant que certaines copies en cours se terminent. Aucune information d'avancement n'est affichée sur les demandes de copie quand elles sont en file d'attente. Les informations d'avancement sont affichées lorsque la copie commence.

La copie d'instantanés entre régions n'est pas prise en charge dans les régions d'adhésion AWS suivantes :

- Afrique (Le Cap)
- Asie-Pacifique (Hong Kong)
- Europe (Milan)
- Moyen-Orient (Bahreïn)

Lorsque vous copiez un instantané dans une région AWS différente de la région AWS de l'instantané source, la première copie est une copie complète de l'instantané, même si vous copiez un instantané incrémentiel. Une copie complète d'un instantané conserve toutes les données et métadonnées requises pour restaurer l'instance de base de données. Après avoir copié le premier instantané, vous pouvez copier des instantanés incrémentiels de la même instance de base de donnée vers la même région de destination dans le même compte AWS. Pour de plus amples informations sur les instantanés incrémentiels, veuillez consulter Copie d'instantané incrémentielle (p. 334).

Lorsque vous copiez un instantané entre des régions ou des comptes, la copie est une copie incrémentielle si les conditions suivantes sont remplies :

- L'instantané a été préalablement copié dans la région ou le compte de destination.
- La dernière copie d'instantané existe toujours dans la région ou le compte de destination.
- Toutes les copies de l'instantané dans la région ou dans le compte de destination sont soit non chiffrées, soit chiffrées avec la même clé CMK.

> **Note**
>
> Pour les instantanés partagés, la copie d'instantanés incrémentiels parmi des régions AWS est prise en charge uniquement que lorsqu'ils ne sont pas chiffrés.

Considérations relatives au groupe d'options

Les groupes d'options sont spécifiques à la région AWS dans laquelle ils ont été créés et vous ne pouvez pas utiliser un groupe d'options d'une région AWS donnée dans une autre région AWS.

Lorsque vous copiez un instantané d'une région à une autre, vous pouvez spécifier un nouveau groupe d'options pour l'instantané. Nous vous recommandons de préparer le nouveau groupe d'options avant de copier l'instantané. Dans la région AWS de destination, créez un groupe d'options avec les mêmes paramètres que le d'instance de base de données d'origine. Si un groupe existe déjà dans la nouvelle région AWS, vous pouvez l'utiliser.

Si vous copiez un instantané et ne spécifiez pas un nouveau groupe d'options pour cet instantané, lorsque vous le restaurez, le d'instance de base de données obtient le groupe d'options par défaut. Pour fournir au nouveau d'instance de base de données les mêmes options que la version d'origine, vous devez procéder comme suit :

1. Dans la région AWS de destination, créez un groupe d'options avec les mêmes paramètres que le d'instance de base de données d'origine. Si un groupe existe déjà dans la nouvelle région AWS, vous pouvez l'utiliser.
2. Après avoir restauré l'instantané dans la région AWS de destination, modifiez le nouveau d'instance de base de données, et ajoutez le groupe d'options nouveau ou existant de l'étape précédente.

Considérations relatives au groupe de paramètres

Lorsque vous copiez un instantané d'une région à une autre, la copie n'inclut pas le groupe de paramètres utilisé par l'instance de base de données d'origine. Lorsque vous restaurez un instantané pour créer un d'instance de base de données, ce d'instance de base de données obtient le groupe de paramètres par défaut pour la région AWS dans laquelle l'objet est créé. Pour fournir au nouveau d'instance de base de données les mêmes paramètres que la version d'origine, vous devez procéder comme suit :

1. Dans la région AWS destinataire, créez un groupe de paramètres de de base de données avec les mêmes réglages que le d'instance de base de données d'origine. Si un groupe existe déjà dans la nouvelle région AWS, vous pouvez l'utiliser.
2. Après avoir restauré l'instantané dans la région AWS de destination, modifiez le nouveau d'instance de base de données, et ajoutez le groupe de paramètres nouveau ou existant de l'étape précédente.

Copie d'un instantané de base de données

Utilisez les procédures de cette rubrique pour copier un instantané de base de données. Pour accéder à une présentation de la copie d'un instantané, consultez Copie d'un instantané (p. 332).

Pour chaque compte AWS, vous pouvez copier jusqu'à cinq snapshots DB à la fois d'une région AWS vers une autre. Si vous copiez un instantané de base de données vers une autre région AWS, vous créez un

instantané de base de données manuel qui est conservé dans cette région AWS. La copie d'un instantané de base de données hors de la région AWS source entraîne des frais de transfert de données Amazon RDS.

Pour de plus amples informations sur la tarification du transfert des données, veuillez consulter la Tarification Amazon RDS.

Une fois que la copie de l'instantané de base de données a été créée dans la nouvelle région AWS, la copie de l'instantané de base de données se comporte de la même façon que tous les autres instantané de base de données dans cette région AWS.

Vous pouvez copier un instantané de base de données en utilisant la AWS Management Console, l'AWS CLI ou l'API RDS.

Console

Cette procédure permet de copier un instantané de bases de données chiffré ou non chiffré, dans une même région AWS ou d'une région à une autre, à l'aide d'AWS Management Console.

Pour copier un instantané de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Snapshots.
3. Sélectionnez l'instantané de base de données que vous voulez copier.
4. Sous Actions, choisissez Copier un instantané. La page Make Copy of DB Snapshot (Copier l'instantané de base de données) apparaît.

5. (Facultatif) Pour copier l'instantané de base de données dans une autre région AWS, choisissez la nouvelle région AWS dans Région de destination.

Note

La région AWS de destination doit avoir la même version de moteur de base de données disponible que la région AWS source.

6. Tapez le nom de la copie de l'instantané de base de données dans Nouvel identificateur d'instantané DB.
7. (Facultatif) Choisissez un nouveau groupe d'options dans Target Option Group (Groupe d'options cible).

   Spécifiez cette option si vous copiez un instantané à partir d'une région AWS vers une autre et que votre instance de base de données utilise un groupe d'options non défini par défaut.

   Si votre instance de base de données source utilise le chiffrement TDE (Transparent Data Encryption) pour Oracle ou Microsoft SQL Server, vous devez spécifier cette option lors d'une copie entre régions. Pour plus d'informations, consultez Considérations relatives au groupe d'options (p. 335).
8. (Facultatif) Pour copier les balises et les valeurs de l'instantané vers la copie de cet instantané, choisissez Copier les balises.
9. (Facultatif) Choisissez l'une des options suivantes pour Enable Encryption (Activer le chiffrement) :
   - Si l'instantané de base de données n'est pas chiffré et que vous ne souhaitez pas chiffrer la copie, choisissez Disable encryption (Désactiver le chiffrement).
   - Si l'instantané de base de données n'est pas chiffré mais que vous souhaitez chiffrer la copie, choisissez Enable encryption (Activer le chiffrement). Dans ce cas, dans Clé principale, spécifiez l'identifiant de clé AWS KMS à utiliser pour chiffrer la copie de l'instantané de base de données.
   - Si l'instantané de base de données est chiffré, choisissez Enable encryption (Activer le chiffrement). Dans ce cas, vous devez chiffrer la copie. Oui est donc déjà sélectionné. Dans Clé principale, spécifiez l'identifiant de clé AWS KMS à utiliser pour chiffrer la copie de l'instantané de base de données.
10. Choisissez Copier l'instantané.

AWS CLI

Vous pouvez copier un instantané de base de données en utilisant la commande d'AWS CLI copy-db-snapshot. Si vous copiez l'instantané vers une nouvelle région AWS, exécutez la commande dans cette nouvelle région AWS.

Les options suivantes sont utilisées pour copier un instantané de base de données. Toutes les options ne sont pas requises pour tous les scénarios. Utilisez les descriptions et les exemples qui suivent pour déterminer quelles options utiliser.

- `--source-db-snapshot-identifier` – L'identifiant de l'instantané de base de données source.
  - Si l'instantané source est dans la même région AWS que la copie, spécifiez un identifiant de l'instantané de base de données valide. Par exemple, `rds:mysql-instance1-snapshot-20130805`.
  - Si l'instantané source est dans une autre région AWS que la copie, spécifiez un ARN d'instantané de base de données valide. Par exemple, `arn:aws:rds:us-west-2:123456789012:snapshot:mysql-instance1-snapshot-20130805`.
  - Si vous effectuez la copie à partir d'un instantané de base de données manuel partagé, ce paramètre doit être l'Amazon Resource Name (ARN) de l'instantané de base de données partagé.
  - Si vous copiez un instantané chiffré, ce paramètre doit être au format ARN pour la région AWS source et doit correspondre à `SourceDBSnapshotIdentifier` dans le paramètre `PreSignedUrl`.
- `--target-db-snapshot-identifier` – L'identifiant de la nouvelle copie de l'instantané de base de données chiffré.

- `--copy-tags` – Inclut l'option de copie des balises pour copier les balises et les valeurs de l'instantané vers la copie de cet instantané.
- `--option-group-name` – Groupe d'options à associer à la copie de l'instantané.

  Spécifiez cette option si vous copiez un instantané à partir d'une région AWS vers une autre et que votre instance de base de données utilise un groupe d'options non défini par défaut.

  Si votre instance de base de données source utilise le chiffrement TDE (Transparent Data Encryption) pour Oracle ou Microsoft SQL Server, vous devez spécifier cette option lors d'une copie entre régions. Pour plus d'informations, consultez Considérations relatives au groupe d'options (p. 335).
- `--kms-key-id` – Identificateur de clé AWS KMS pour un instantané de base de données chiffré. L'identificateur de clé AWS KMS est l'ARN (Amazon Resource Name), l'identificateur de clé ou l'alias de clé pour la clé CMK AWS KMS.
  - Si vous copiez un instantané de base de données chiffré à partir de votre compte AWS, vous pouvez spécifier une valeur pour ce paramètre afin de chiffrer la copie avec une nouvelle clé CMK AWS KMS. Si vous ne spécifiez pas de valeur pour ce paramètre, la copie de l'instantané de base de données est chiffrée avec la même clé CMK AWS KMS que l'instantané de base de données source.
  - Si vous copiez un instantané de base de données chiffré qui est partagé à partir d'un autre compte AWS, vous devez spécifier une valeur pour ce paramètre.
  - Si vous spécifiez ce paramètre lorsque vous copiez un instantané non chiffré, la copie est chiffrée.
  - Si vous copiez un instantané chiffré vers une autre région AWS, vous devez spécifier une clé CMK AWS KMS pour la région AWS de destination. Les clés CMK AWS KMS sont spécifiques à la région AWS dans laquelle elles sont créées et vous ne pouvez pas utiliser de clés de chiffrement issues d'une région AWS donnée dans une autre région AWS.
- `--source-region` – ID de la région AWS de l'instantané de base de données source. Si vous copiez un instantané chiffré vers une autre région AWS, vous devez spécifier cette option.

Example Source non chiffrée, même région de destination

Le code ci-dessous permet de créer une copie d'un instantané, avec le nouveau nom `mydbsnapshotcopy`, dans la même région AWS que l'instantané source. Lorsque la copie est réalisée, toutes les balises de l'instantané d'origine sont copiées dans la copie de l'instantané.

Pour Linux, macOS ou Unix :

```
aws rds copy-db-snapshot \
    --source-db-snapshot-identifier mysql-instance1-snapshot-20130805 \
    --target-db-snapshot-identifier mydbsnapshotcopy \
    --copy-tags
```

Pour Windows :

```
aws rds copy-db-snapshot ^
    --source-db-snapshot-identifier mysql-instance1-snapshot-20130805 ^
    --target-db-snapshot-identifier mydbsnapshotcopy ^
    --copy-tags
```

Example Source non chiffrée, autre région de destination

Le code suivant permet de créer une copie d'un instantané, avec le nouveau nom `mydbsnapshotcopy`, dans la région AWS où la commande est exécutée.

Pour Linux, macOS ou 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
```

Pour 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 Source chiffrée, autre région de destination

L'exemple de code suivant permet de copier un instantané de bases de données chiffré à partir de la région us-west-2 vers la région us-east-1. Exécutez la commande dans la région us-east-1.

Pour Linux, macOS ou 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 \
 --source-region us-west-2 \
 --kms-key-id my-us-east-1-key \
    --option-group-name custom-option-group-name
```

Pour 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 ^
 --source-region us-west-2 ^
 --kms-key-id my-us-east-1-key ^
    --option-group-name custom-option-group-name
```

API RDS

Vous pouvez copier un instantané de base de données en utilisant l'opération d'API Amazon RDS CopyDBSnapshot. Si vous copiez l'instantané vers une nouvelle région AWS, exécutez l'action dans cette nouvelle région AWS.

Les paramètres suivants sont utilisés pour copier un instantané de base de données. Tous les paramètres ne sont pas requis pour tous les scénarios. Utilisez les descriptions et les exemples qui suivent pour déterminer quels paramètres utiliser.

- `SourceDBSnapshotIdentifier` – L'identifiant de l'instantané de base de données source.
  - Si l'instantané source est dans la même région AWS que la copie, spécifiez un identifiant de l'instantané de base de données valide. Par exemple, `rds:mysql-instance1-snapshot-20130805`.
  - Si l'instantané source est dans une autre région AWS que la copie, spécifiez un ARN d'instantané de base de données valide. Par exemple, `arn:aws:rds:us-west-2:123456789012:snapshot:mysql-instance1-snapshot-20130805`.
  - Si vous effectuez la copie à partir d'un instantané de base de données manuel partagé, ce paramètre doit être l'Amazon Resource Name (ARN) de l'instantané de base de données partagé.
  - Si vous copiez un instantané chiffré, ce paramètre doit être au format ARN pour la région AWS source et doit correspondre à `SourceDBSnapshotIdentifier` dans le paramètre `PreSignedUrl`.

- `TargetDBSnapshotIdentifier` – L'identifiant de la nouvelle copie de l'instantané de base de données chiffré.
- `CopyTags` – Affectez à ce paramètre la valeur `true` pour copier les balises et les valeurs de l'instantané vers la copie de cet instantané. La valeur par défaut est `false`.
- `OptionGroupName` – Groupe d'options à associer à la copie de l'instantané.

  Spécifiez ce paramètre si vous copiez un instantané à partir d'une région AWS vers une autre et que votre instance de base de données utilise un groupe d'options non défini par défaut.

  Si votre instance de base de données source utilise le chiffrement TDE (Transparent Data Encryption) pour Oracle ou Microsoft SQL Server, vous devez spécifier ce paramètre lors d'une copie entre régions. Pour plus d'informations, consultez Considérations relatives au groupe d'options (p. 335).
- `KmsKeyId` – Identificateur de clé AWS KMS pour un instantané de base de données chiffré. L'identificateur de clé AWS KMS est l'ARN (Amazon Resource Name), l'identificateur de clé ou l'alias de clé pour la clé CMK AWS KMS.
  - Si vous copiez un instantané de base de données chiffré à partir de votre compte AWS, vous pouvez spécifier une valeur pour ce paramètre afin de chiffrer la copie avec une nouvelle clé CMK AWS KMS. Si vous ne spécifiez pas de valeur pour ce paramètre, la copie de l'instantané de base de données est chiffrée avec la même clé CMK AWS KMS que l'instantané de base de données source.
  - Si vous copiez un instantané de base de données chiffré qui est partagé à partir d'un autre compte AWS, vous devez spécifier une valeur pour ce paramètre.
  - Si vous spécifiez ce paramètre lorsque vous copiez un instantané non chiffré, la copie est chiffrée.
  - Si vous copiez un instantané chiffré vers une autre région AWS, vous devez spécifier une clé CMK AWS KMS pour la région AWS de destination. Les clés CMK AWS KMS sont spécifiques à la région AWS dans laquelle elles sont créées et vous ne pouvez pas utiliser de clés de chiffrement issues d'une région AWS donnée dans une autre région AWS.
- `PreSignedUrl` – URL qui contient une demande signée via Signature Version 4 pour l'opération d'API `CopyDBSnapshot` dans la région AWS source qui contient l'instantané de base de données source à copier.

  Vous devez spécifier ce paramètre lorsque vous copiez un instantané de base de données chiffré à partir d'une autre région AWS en utilisant l'API Amazon RDS. Vous pouvez spécifier l'option de région source à la place de ce paramètre lorsque vous copiez un instantané de bases de données chiffré à partir d'une autre région AWS en utilisant l'interface de ligne de commande (CLI) AWS.

  L'URL pré-signée doit être une demande valide pour l'opération d'API `CopyDBSnapshot` qui peut être exécutée dans la région AWS source qui contient l'instantané de base de données chiffré à copier. La demande d'URL pré-signée doit contenir les valeurs de paramètres suivantes :
  - `DestinationRegion` - Région AWS vers laquelle l'instantané de base de données chiffré sera copié. Cette région AWS est la même que celle où l'action `CopyDBSnapshot`, qui contient cette URL pré-signée, est appelée.

    Par exemple, si vous copiez un instantané de bases de données chiffré de la région us-west-2 vers la région us-east-1, vous appelez l'action `CopyDBSnapshot` dans la région us-east-1 et fournissez une URL présignée contenant un appel à l'action `CopyDBSnapshot` dans la région us-west-2. Pour cet exemple, il convient d'affecter la région us-east-1 au paramètre `DestinationRegion` figurant dans l'URL présignée.
  - `KmsKeyId` - Identificateur de clé AWS KMS de la clé à utiliser pour chiffrer la copie de l'instantané de base de données dans la région AWS de destination. Il s'agit du même identifiant pour l'action `CopyDBSnapshot` qui est appelée dans la région AWS de destination et l'action contenue dans l'URL pré-signée.
  - `SourceDBSnapshotIdentifier` - Identifiant d'instantané de base de données pour l'instantané chiffré à copier. Cet identifiant doit être au format Amazon Resource Name (ARN) pour la région AWS source. Par exemple, si vous copiez un instantané de bases de données chiffré à partir de la

région us-west-2, le paramètre `SourceDBSnapshotIdentifier` ressemble à : `arn:aws:rds:us-west-2:123456789012:snapshot:mysql-instance1-snapshot-20161115`.

Pour plus d'informations sur les demandes signées par Signature Version 4, consultez les informations suivantes :

- Authentification des demandes : utilisation des paramètres de requête (AWS Signature Version 4) dans le Amazon Simple Storage Service API Reference
- Processus de signature version 4 dans le AWS General Reference

Example Source non chiffrée, même région de destination

Le code ci-dessous permet de créer une copie d'un instantané, avec le nouveau nom `mydbsnapshotcopy`, dans la même région AWS que l'instantané source. Lorsque la copie est réalisée, toutes les balises de l'instantané d'origine sont copiées dans la copie de l'instantané.

```
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 Source non chiffrée, autre région de destination

Le code suivant permet de créer une copie d'un instantané, avec le nouveau nom `mydbsnapshotcopy`, dans la région us-west-1.

```
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 Source chiffrée, autre région de destination

Le code suivant permet de créer une copie d'un instantané, avec le nouveau nom `mydbsnapshotcopy`, dans la région us-east-1.

```
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
```

Partage d'un instantané de de base de données

Amazon RDS vous permet de partager un instantané de de base de données manuel des façons suivantes :

- Le partage d'un instantané de de base de données manuel chiffré ou non chiffré permet aux comptes AWS autorisés de copier l'instantané.
- Le partage d'un instantané de base de données manuel non chiffré permet aux comptes AWS autorisés de restaurer directement une instance de base de données à partir de l'instantané, plutôt que d'effectuer une copie et de la restaurer. Toutefois, vous ne pouvez pas restaurer une instance de base de données à partir d'un instantané de base de données qui est à la fois partagé et chiffré. Par contre, vous pouvez créer une copie de l'instantané de base de données et restaurer l'instance de base de données à partir de cette copie.

> **Note**
>
> Pour partager un instantané de de base de données automatisé, créez un instantané de de base de données manuel en copiant l'instantané automatisé, puis partagez cette copie. Ce processus s'applique également aux ressources générées par AWS Backup.

Pour plus d'informations sur la copie d'un instantané, consultez Copie d'un instantané (p. 332). Pour plus d'informations sur la restauration d'une instance de base de données à partir d'un instantané de de base de données, consultez Restauration à partir d'un instantané de base de données (p. 329).

Vous pouvez partager un instantané manuel avec 20 autres comptes AWS maximum. Vous pouvez également partager un instantané manuel non chiffré marqué comme public ; il est ainsi accessible à tous les comptes AWS. Lors du partage d'un instantané marqué comme public, n'incluez aucune information privée dans vos instantanés publics.

Les limites suivantes s'appliquent lors du partage de snapshots manuels avec d'autres comptes AWS :

- Lorsque vous restaurez une instance ou un de base de données depuis un instantané partagé à l'aide de l'AWS Command Line Interface (AWS CLI) ou de l'API Amazon RDS, vous devez spécifier l'Amazon Resource Name (ARN) de l'instantané partagé en tant qu'identifiant de l'instantané.
- Vous ne pouvez pas partager un instantané de bases de données qui utilise un groupe d'options comportant des options permanentes ou persistantes, sauf pour les instances de base de données Oracle qui possèdent l'option `Timezone` et/ou `OLS`.

  Une option permanente ne peut pas être supprimée d'un groupe d'options. Les groupes d'options avec des options persistantes ne peuvent pas être supprimés d'une instance de base de données une fois que le groupe d'options a été assigné à l'instance de base de données.

  Le tableau suivant répertorie les options permanentes et persistantes ainsi que leurs moteurs de base de données associés.

Nom d'option	Persistante	Permanent	Moteur de base de données
TDE	Oui	Non	Configurer SQL Server Enterprise Edition
TDE	Oui	Oui	Oracle Enterprise Edition
Fuseau horaire	Oui	Oui	Oracle Enterprise Edition Oracle Standard Edition Oracle Standard Edition One Oracle Standard Edition Two

Pour les instances de base de données Oracle, vous pouvez copier les instantanés de bases de données partagés qui possèdent l'option `Timezone` et/ou `OLS`. Pour ce faire, spécifiez un groupe d'options cibles qui inclut ces options lorsque vous copiez l'instantané de bases de données. L'option OLS est permanente et persistante uniquement pour les instances de bases de données Oracle exécutant Oracle version 12.2 ou ultérieure. Pour de plus amples informations sur ces options, veuillez consulter Fuseau horaire Oracle (p. 1088) et Oracle Label Security (p. 1054).

Partage d'un instantané chiffré

Vous pouvez partager des instantanés de de base de données qui ont été chiffrés « au repos » en utilisant l'algorithme de chiffrement AES-256, comme décrit dans Chiffrement des ressources Amazon RDS (p. 1522). Pour ce faire, vous devez exécuter les étapes suivantes :

1. Partagez la clé principale client (CMK) AWS Key Management Service (AWS KMS) qui a été utilisée pour chiffrer l'instantané avec tous les comptes que vous souhaitez autoriser à accéder à l'instantané.

   Vous pouvez partager des clés CMK AWS KMS avec un autre compte AWS en ajoutant l'autre compte à la stratégie de clé AWS KMS. Pour plus de détails sur la mise à jour d'une stratégie de clé, voir Stratégies de clés dans le Guide du développeur AWS KMS. Pour obtenir un exemple de création d'une stratégie de clé, consultez Détermination de l'accès à une clé principale client (CMK) AWS KMS (p. 344) plus loin dans cette rubrique.
2. Utilisez l'API AWS Management Console, AWS CLI ou Amazon RDS pour partager l'instantané chiffré avec les autres comptes.

Ces restrictions s'appliquent au partage d'instantanés chiffrés :

- Vous ne pouvez pas partager des instantanés chiffrés marqués comme publics.

- Vous ne pouvez pas partager des instantanés Oracle ou Microsoft SQL Server qui sont chiffrés à l'aide de Transparent Data Encryption (TDE).
- Vous ne pouvez pas partager un instantané chiffré à l'aide de la clé CMK AWS KMS par défaut du compte AWS qui a partagé l'instantané.

Détermination de l'accès à une clé principale client (CMK) AWS KMS

Pour qu'un autre compte AWS copie un instantané de de base de données chiffré partagé depuis votre compte, le compte avec lequel vous partagez votre instantané doit avoir accès à la clé principale client (CMK) AWS KMS qui a chiffré l'instantané. Pour autoriser un autre compte AWS à accéder à une clé CMK AWS KMS, mettez à jour la stratégie de clé pour la clé CMK AWS KMS avec l'ARN du compte AWS auquel vous partagez en tant que `Principal` dans la stratégie de clé AWS KMS, puis autorisez l'action `kms:CreateGrant`.

Une fois que vous avez donné à un compte AWS l'accès à votre clé CMK AWS KMS, pour copier votre instantané chiffré, ce compte AWS doit créer un utilisateur AWS Identity and Access Management (IAM) s'il n'en possède pas déjà un. En outre, ce compte AWS doit également attacher une stratégie IAM pour cet utilisateur IAM qui permet à ce dernier de copier un instantané de de base de données chiffré à l'aide de votre clé CMK AWS KMS. Le compte doit être un utilisateur IAM et ne peut pas être une identité du compte AWS racine en raison des restrictions de sécurité AWS KMS.

Dans l'exemple de stratégie suivant, l'utilisateur `111122223333` est le propriétaire de la clé CMK AWS KMS, et l'utilisateur `444455556666` est le compte avec lequel la clé est partagée. Cette stratégie de clé mise à jour permet au compte AWS d'accéder à la clé CMK AWS KMS en incluant l'ARN pour l'identité du compte AWS racine pour l'utilisateur `444455556666` en tant que `Principal` pour la stratégie et en autorisant l'action `kms:CreateGrant`.

```
{
  "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: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}}
    }
  ]
}
```

Création d'une stratégie IAM pour permettre la copie d'un instantané chiffré

Une fois que le compte AWS externe peut accéder à votre clé principale client (CMK) AWS KMS, le propriétaire de ce compte AWS peut créer une stratégie qui autorise un utilisateur IAM créé pour ce compte à copier un instantané chiffré avec cette clé CMK AWS KMS.

L'exemple suivant montre une stratégie pouvant être attachée à un utilisateur IAM pour un compte AWS `444455556666` qui permet à l'utilisateur IAM de copier un instantané partagé depuis le compte AWS `111122223333` qui a été chiffré avec la clé CMK AWS KMS `c989c1dd-a3f2-4a5d-8d96-e793d082ab26` dans la région `us-west-2`.

```
{
    "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
                }
            }
        }
    ]
}
```

Pour plus de détails sur la mise à jour d'une stratégie de clé, voir Stratégies de clés dans le Guide du développeur AWS KMS.

Partage d'un instantané

Vous pouvez partager un instantané de de base de données à l'aide de la AWS Management Console, de l'AWS CLI ou de l'API RDS.

Console

En utilisant la console Amazon RDS, vous pouvez partager un instantané de de base de données manuel avec jusqu'à 20 comptes AWS. Vous pouvez également utiliser la console pour arrêter le partage d'un instantané manuel avec un ou plusieurs comptes.

Pour partager un instantané de de base de données manuel à l'aide de la console Amazon RDS

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Snapshots.
3. Sélectionnez l'instantané manuel que vous voulez partager.
4. Pour Actions, choisissez Partager l'instantané.
5. Choisissez l'une des options suivantes pour DB snapshot visibility (Visibilité d'instantané de base de données).
   - Si la source est non chiffrée, choisissez Public pour permettre à tous les comptes AWS de restaurer une instance ou un de base de données à partir d'un instantané de de base de données manuel, ou choisissez Privé pour autoriser uniquement les comptes AWS indiqués à restaurer une instance ou un de base de données à partir de votre instantané de base de données manuel.

     Warning

     Si vous configurez DB Snapshot Visibility (Visibilité de l'instantané de base de données) sur Public, tous les comptes AWS peuvent restaurer une instance ou un de base de données depuis votre instantané de de base de données manuel et accéder à vos données. Ne partagez aucun instantané de de base de données manuel contenant des informations privées en le marquant comme Public.
   - Si la source est chiffrée, la Visibilité d'instantané de base de données est définie sur Privé, car les instantanés chiffrés ne peuvent pas être partagés s'ils sont marqués comme étant publics.
6. Dans ID de compte AWS, saisissez l'identifiant du compte AWS que vous souhaitez autoriser à restaurer une instance ou un de base de données depuis votre instantané manuel, puis choisissez Ajouter. Faites de même pour inclure des identifiants de compte AWS supplémentaires, jusqu'à 20 comptes AWS.

   Si vous faites une erreur en ajoutant un identifiant de compte AWS à la liste des comptes autorisés, vous pouvez le supprimer de la liste en choisissant Delete à droite de l'identifiant de compte AWS incorrect.

7. Après avoir ajouté des identifiants pour tous les comptes AWS que vous souhaitez autoriser à restaurer l'instantané manuel, choisissez Save pour enregistrer vos changements.

Pour arrêter le partage d'un instantané de de base de données manuel avec un compte AWS

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Snapshots.
3. Sélectionnez l'instantané manuel que vous voulez cesser de partager.
4. Choisissez Actions, puis Share Snapshot (Partager instantané).
5. Pour supprimer une autorisation pour un compte AWS, choisissez Delete pour l'identifiant du compte AWS dans la liste des comptes autorisés.

6. Choisissez Save pour enregistrer les changements.

AWS CLI

Pour partager un instantané de de base de données, utilisez la commande `aws rds modify-db-snapshot-attribute` . Utilisez le paramètre `--values-to-add` pour ajouter une liste des ID de comptes AWS autorisés à restaurer l'instantané manuel.

L'exemple suivant active deux identifiants de compte AWS `111122223333` et `444455556666`, pour restaurer l'instantané de base de données appelé `manual-snapshot1`.

Example

Pour Linux, macOS ou Unix :

```
aws rds modify-db-snapshot-attribute \
--db-snapshot-identifier manual-snapshot1 \
--attribute-name restore \
--values-to-add {"111122223333","444455556666"}
```

Pour Windows :

```
aws rds modify-db-snapshot-attribute ^
--db-snapshot-identifier manual-snapshot1 ^
--attribute-name restore ^
--values-to-add "[\"111122223333\",\"444455556666\"]"
```

> **Note**
>
> Lorsque vous utilisez l'invite de commande Windows, vous devez utiliser des guillemets doubles (") d'échappement dans le code JSON en les préfixant d'une barre oblique inverse (\).

Pour supprimer de la liste un identifiant de compte AWS, utilisez le paramètre `--values-to-remove`. L'exemple suivant empêche l'ID 444455556666 de compte AWS de restaurer l'instantané.

Example

Pour Linux, macOS ou Unix :

```
aws rds modify-db-snapshot-attribute \
--db-snapshot-identifier manual-snapshot1 \
--attribute-name restore \
--values-to-remove {"444455556666"}
```

Pour Windows :

```
aws rds modify-db-snapshot-attribute ^
--db-snapshot-identifier manual-snapshot1 ^
--attribute-name restore ^
--values-to-remove "[\"444455556666\"]"
```

> **Note**
>
> Lorsque vous utilisez l'invite de commande Windows, vous devez utiliser des guillemets doubles (") d'échappement dans le code JSON en les préfixant d'une barre oblique inverse (\).

Pour répertorier les comptes AWS activés pour restaurer un instantané, utilisez la commande de l'AWS CLI `describe-db-snapshot-attributes`

API RDS

Vous pouvez également partager un instantané de de base de données manuel avec d'autres comptes AWS à l'aide de l'API Amazon RDS. Pour ce faire, appelez l'opération `ModifyDBSnapshotAttribute` . Indiquez `restore` pour `AttributeName`, et utilisez le paramètre `ValuesToAdd` pour ajouter une liste des ID de comptes AWS pour ceux autorisés à restaurer l'instantané manuel.

Pour qu'un instantané manuel soit défini comme étant public et qu'il puisse être restauré par tous les comptes AWS, utilisez la valeur `all`. Toutefois, n'ajoutez pas la valeur `all` pour tous les snapshots manuels contenant des informations privées que vous ne souhaitez pas mettre à la disposition de tous les comptes AWS. De même, ne spécifiez pas la valeur `all` pour les instantanés chiffrés, car il est impossible de rendre tous ces instantanés publics.

Pour supprimer l'autorisation de partage d'un compte AWS, utilisez l'opération `ModifyDBSnapshotAttribute` avec `AttributeName` configuré sur `restore` et le paramètre `ValuesToRemove`. Pour marquer un instantané manuel comme privé, supprimez la valeur `all` de la liste des valeurs pour l'attribut `restore`.

Pour répertorier tous les comptes AWS autorisés à restaurer un instantané, utilisez l'opération d'API `DescribeDBSnapshotAttributes` .

Exportation de données d'instantanés de bases de données vers Amazon S3

Vous pouvez exporter des données d'instantanés de bases de données vers un compartiment Amazon S3. Une fois les données exportées, vous pouvez les analyser directement via des outils tels que Amazon Athena ou Amazon Redshift Spectrum. Le processus d'exportation s'exécute en arrière-plan et n'affecte pas les performances de votre instance de base de données active.

Lorsque vous exportez un instantané de base de données, Amazon RDS extrait les données de l'instantané et les stocke dans un compartiment Amazon S3 de votre compte. Les données sont stockées dans un format Apache Parquet qui est compressé et cohérent.

Vous pouvez exporter tous les types d'instantanés et de clusters de bases de données, y compris les instantanés manuels, les instantanés système automatisés et les instantanés créés par le service AWS Backup. Par défaut, toutes les données de l'instantané sont exportées. Toutefois, vous pouvez choisir d'exporter des ensembles spécifiques de bases de données, de schémas ou de tables.

> **Note**
>
> L'exportation d'instantanés à partir d'instances de base de données qui utilisent le stockage magnétique n'est pas prise en charge.

Amazon RDS prend en charge l'exportation d'instantanés dans toutes les régions AWS, sauf :

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

Les tableaux suivants indiquent les versions du moteur prises en charge pour l'exportation de données d'instantanés vers Amazon S3.

MariaDB	MySQL	PostgreSQL
10.3	8.0.13 et plus	11.2 et plus

MariaDB	MySQL	PostgreSQL
10.2.12 et plus 10.1.26 et plus 10.0.32 et plus	5.7.24 et plus 5.6.40 et plus	10.7 et plus De 9.6.6 à 9.6.9, 9.6.12 et plus 9.5.16 et plus

Pour obtenir la liste complète des versions de moteur prises en charge par Amazon RDS, veuillez consulter les rubriques suivantes :

- Versions de MariaDB sur Amazon RDS (p. 544)
- Versions de MySQL sur Amazon RDS (p. 782)
- Versions de base de données PostgreSQL prises en charge (p. 1468)

Rubriques

- Présentation de l'exportation des données d'instantané (p. 350)
- Configuration de l'accès à un compartiment Amazon S3 (p. 351)
- Exportation d'un instantané vers un compartiment Amazon S3 (p. 353)
- Surveillance des exportations d'instantanés (p. 355)
- Annulation d'une tâche d'exportation d'instantané (p. 357)
- Dépannage des erreurs d'autorisations PostgreSQL (p. 358)
- Conversion des données lors de l'exportation vers un compartiment Amazon S3 (p. 358)

Présentation de l'exportation des données d'instantané

La procédure suivante fournit une présentation de l'exportation des données d'instantané de base de données vers un compartiment Amazon S3. Pour plus de détails, consultez les sections suivantes.

Pour exporter des données d'instantané de base de données vers Amazon S3

1. Identifiez l'instantané à exporter.

   Utilisez un instantané automatisé ou manuel existant ou créez un instantané manuel d'une instance de base de données.
2. Configurez l'accès au compartiment Amazon S3.

   Un compartiment est un conteneur d'objets ou de fichiers Amazon S3. Pour fournir les informations permettant d'accéder à un compartiment, procédez comme suit :

   a. Identifiez le compartiment S3 vers lequel l'instantané doit être exporté. Le compartiment S3 doit être situé dans la même région AWS que l'instantané. Pour plus d'informations, consultez Identification du compartiment Amazon S3 pour l'exportation (p. 351).

   b. Créez une clé principale client (CMK) AWS Key Management Service (AWS KMS) pour le chiffrement côté serveur. La clé principale client AWS KMS est utilisée par la tâche d'exportation de l'instantané pour configurer le chiffrement côté serveur AWS KMS lors de l'écriture des données d'exportation dans S3. Pour de plus amples informations, veuillez consulter Chiffrement des ressources Amazon RDS (p. 1522).

   c. Créez un rôle AWS Identity and Access Management (IAM) qui accorde à la tâche d'exportation de l'instantané l'accès au compartiment S3. Pour de plus amples informations, veuillez consulter Fournir l'accès à un compartiment Amazon S3 à l'aide d'un rôle IAM (p. 351).

3. Exportez l'instantané vers Amazon S3 à l'aide de la console ou de la commande d'interface de ligne de commande `start-export-task`. Pour de plus amples informations, veuillez consulter Exportation d'un instantané vers un compartiment Amazon S3 (p. 353).
4. Pour accéder aux données exportées dans le compartiment Amazon S3, veuillez consulter Chargement, téléchargement et gestion d'objets dans le Amazon Simple Storage Service Guide de l'utilisateur de la console.

Configuration de l'accès à un compartiment Amazon S3

Pour exporter des données d'instantané de base de données vers un fichier Amazon S3, vous accordez d'abord à l'instantané l'autorisation d'accéder au compartiment Amazon S3. Vous créez ensuite un rôle IAM pour autoriser le service Amazon RDS à écrire dans le compartiment Amazon S3.

Rubriques

- Identification du compartiment Amazon S3 pour l'exportation (p. 351)
- Fournir l'accès à un compartiment Amazon S3 à l'aide d'un rôle IAM (p. 351)

Identification du compartiment Amazon S3 pour l'exportation

Identifiez le compartiment Amazon S3 vers lequel exporter l'instantané de base de données. Utilisez un compartiment S3 existant ou créez un nouveau compartiment S3.

> **Note**
>
> Le compartiment S3 vers lequel effectuer l'exportation doit se trouver dans la même région AWS que l'instantané.

Pour de plus amples informations sur l'utilisation des Amazon S3 compartiments, veuillez consulter les points suivants dans le Amazon Simple Storage Service Guide de l'utilisateur de la console :

- Comment afficher les propriétés d'un compartiment S3 ?
- Comment activer le chiffrement par défaut pour un compartiment S3 ?
- Comment créer un compartiment S3 ?

Fournir l'accès à un compartiment Amazon S3 à l'aide d'un rôle IAM

Avant d'exporter les données d'instantané de base de données vers Amazon S3, vous devez accorder aux tâches d'exportation d'instantané une autorisation d'accès en écriture au compartiment Amazon S3.

Pour ce faire, créez une stratégie IAM qui donne accès au compartiment. Créez ensuite un rôle IAM et attachez la stratégie à ce rôle. Vous affectez ultérieurement le rôle IAM à votre tâche d'exportation d'instantané.

> **Important**
>
> Si vous prévoyez d'utiliser la AWS Management Console pour exporter votre instantané, vous pouvez choisir de créer automatiquement la stratégie et le rôle IAM lors de ladite exportation. Pour obtenir des instructions, consultez Exportation d'un instantané vers un compartiment Amazon S3 (p. 353).

Pour accorder aux tâches d'instantané de base de données l'accès à Amazon S3

1. Créez une stratégie IAM. Cette stratégie fournit les autorisations d'accès au compartiment et aux objets qui permettent à votre tâche d'exportation d'instantané d'accéder à Amazon S3.

   Incluez dans la stratégie les actions obligatoires suivantes pour permettre le transfert de fichiers depuis Amazon RDS vers un compartiment S3.

   - `s3:PutObject*`
   - `s3:GetObject*`
   - `s3:ListBucket`
   - `s3:DeleteObject*`
   - `s3:GetBucketLocation`

   Incluez dans la stratégie les ressources suivantes pour identifier le compartiment S3 et les objets qu'il contient. La liste de ressources suivante indique le format Amazon Resource Name (ARN) pour l'accès à Amazon S3.

   - `arn:aws:s3:::your-s3-bucket`
   - `arn:aws:s3:::your-s3-bucket/*`

   Pour de plus amples informations sur la création d'une stratégie IAM pour Amazon RDS, veuillez consulter Création et utilisation d'une stratégie IAM pour l'accès à une base de données IAM (p. 1558). Veuillez consulter également Didacticiel : Créer et attacher votre première stratégie gérée par le client dans le IAM Guide de l'utilisateur.

   La commande d'AWS CLI suivante crée une stratégie IAM nommée `ExportPolicy` avec ces options. Elle accorde un accès à un compartiment nommé `your-s3-bucket`.

   > **Note**
   >
   > Après avoir créé la stratégie, notez son ARN. Vous en aurez besoin par la suite pour attacher la stratégie à un rôle IAM.

```
aws iam create-policy  --policy-name ExportPolicy --policy-document '{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Effect": "Allow",
             "Action": [
                 "s3:ListBucket",
                 "s3:GetBucketLocation"
             ],
             "Resource": [
                 "arn:aws:s3:::*"
             ]
         },
         {
             "Effect": "Allow",
             "Action": [
                 "s3:PutObject*",
                 "s3:GetObject*",
                 "s3:DeleteObject*"
             ],
             "Resource": [
                 "arn:aws:s3:::your-s3-bucket",
                 "arn:aws:s3:::your-s3-bucket/*"
             ]
         }
```

```
    ]
}'
```

2. Créez un rôle IAM. L'objectif est ici de permettre à Amazon RDS d'endosser ce rôle IAM en votre nom pour accéder à vos compartiments Amazon S3. Pour de plus amples informations, veuillez consulter Création d'un rôle pour déléguer les autorisations à un utilisateur IAM dans le IAM Guide de l'utilisateur.

   L'exemple suivant montre comment utiliser la commande d'AWS CLI pour créer un rôle nommé `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. Attachez la stratégie IAM que vous avez créée au rôle IAM que vous venez de créer.

   La commande d'AWS CLI suivante attache la stratégie créée précédemment au rôle nommé `rds-s3-export-role`. Remplacez *`your-policy-arn`* par l'ARN de stratégie que vous avez noté lors d'une étape précédente.

```
aws iam attach-role-policy  --policy-arn your-policy-arn  --role-name rds-s3-export-
role
```

Exportation d'un instantané vers un compartiment Amazon S3

Vous pouvez avoir jusqu'à cinq tâches d'exportation d'instantané de base de données simultanées en cours par compte.

> **Note**
>
> L'exportation d'instantanés RDS peut prendre un certain temps en fonction du type et de la taille de votre base de données. La tâche d'exportation commence par restaurer et mettre à l'échelle l'ensemble de la base de données avant d'extraire les données vers Amazon S3. La progression de la tâche au cours de cette phase s'affiche sous l'intitulé Starting. Lorsque la tâche passe à l'exportation de données vers S3, la progression affiche l'intitulé En cours.
> La durée nécessaire à l'exportation dépend des données stockées dans la base de données. Par exemple, l'exportation des tables comportant des colonnes numériques d'index ou de clé primaire bien distribuées est la plus rapide. L'opération prendra plus de temps pour les tables qui ne contiennent pas de colonne adaptée au partitionnement et les tables avec un seul index sur une colonne basée sur une chaîne, car l'exportation utilise un processus à thread unique plus lent.

Vous pouvez exporter un instantané de base de données vers Amazon S3 à l'aide de l'AWS Management Console, de l'AWS CLI ou de l'API RDS.

Console

L'option de console Exporter vers Amazon S3 s'affiche uniquement pour les instantanés pouvant être exportés vers Amazon S3. Un instantané peut ne pas être disponible pour l'exportation pour les raisons suivantes :

- Le moteur de base de données n'est pas pris en charge pour l'exportation S3.
- La version de l'instance de base de données n'est pas prise en charge pour l'exportation S3.
- L'exportation S3 n'est pas prise en charge dans la région AWS où l'instantané a été créé.

Pour exporter un instantané de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Snapshots (Instantanés).
3. Dans les onglets, choisissez le type d'instantané que vous souhaitez exporter.
4. Dans la liste des instantanés, choisissez celui que vous souhaitez exporter.
5. Pour actions, choisissez Export to Amazon S3 (Exporter vers Amazon S3).

   La fenêtre Export to Amazon S3 (Exporter vers Amazon S3) apparaît.
6. Dans Export Identifier (Identifiant d'exportation), entrez un nom pour identifier la tâche d'exportation. Cette valeur est également utilisée pour le nom du fichier créé dans le compartiment S3.
7. Choisissez la quantité de données à exporter :
   - Choisissez All (Tout) pour exporter toutes les données de l'instantané.
   - Choisissez Partial (Partiel) pour exporter des parties spécifiques de l'instantané. Pour identifier les parties de l'instantané à exporter, entrez une ou plusieurs tables pour Identifiers (Identifiants).
8. Pour S3 bucket (Compartiment S3), choisissez le compartiment vers lequel exporter.

   Pour affecter les données exportées à un chemin d'accès de dossier dans le compartiment S3, entrez le chemin d'accès facultatif pour S3 prefix (Préfixe S3).
9. Pour Rôle IAM, choisissez un rôle qui vous accorde un accès en écriture au compartiment S3 choisi, ou créez un nouveau rôle.
   - Si vous avez créé un rôle en suivant les étapes décrites dans Fournir l'accès à un compartiment Amazon S3 à l'aide d'un rôle IAM (p. 351), choisissez ce rôle.
   - Si vous n'avez pas créé un rôle qui vous accorde un accès en écriture au compartiment S3 choisi, choisissez Créer un nouveau rôle pour créer le rôle automatiquement. Ensuite, saisissez un nom pour le rôle dans Nom du rôle IAM.
10. Pour Master key (Clé principale), entrez l'ARN de la clé à utiliser pour chiffrer les données exportées.
11. Choisissez Export to Amazon S3 (Exporter vers Amazon S3).

AWS CLI

Pour exporter un instantané de base de données vers Amazon S3 à l'aide de l'AWS CLI, utilisez la commande start-export-task avec les options requises suivantes :

- `--export-task-identifier`
- `--source-arn`
- `--s3-bucket-name`
- `--iam-role-arn`
- `--kms-key-id`

Dans les exemples suivants, la tâche d'exportation d'instantané est nommée *my_snapshot_export*. Elle exporte un instantané vers un compartiment S3 nommé *my_export_bucket*.

Example

Pour Linux, macOS ou 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 master_key
```

Pour 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 master_key
```

Vous trouverez ci-après un exemple de sortie.

```
{
    "Status": "STARTING",
    "IamRoleArn": "iam_role",
    "ExportTime": "2019-08-12T01:23:53.109Z",
    "S3Bucket": "my_export_bucket",
    "PercentProgress": 0,
    "KmsKeyId": "master_key",
    "ExportTaskIdentifier": "my_snapshot_export",
    "TotalExtractedDataInGB": 0,
    "TaskStartTime": "2019-11-13T19:46:00.173Z",
    "SourceArn": "arn:aws:rds:AWS_Region:123456789012:snapshot:snapshot_name"
}
```

Pour fournir un chemin de dossier dans le compartiment S3 pour l'exportation d'instantané, incluez l'option `--s3-prefix` dans la commande start-export-task .

API RDS

Pour exporter un instantané de base de données vers Amazon S3 à l'aide de l'API Amazon RDS, utilisez l'opération StartExportTask avec les paramètres requis suivants :

- `ExportTaskIdentifier`
- `SourceArn`
- `S3BucketName`
- `IamRoleArn`
- `KmsKeyId`

Surveillance des exportations d'instantanés

Vous pouvez surveiller les exportations d'instantanés de bases de données à l'aide de l'AWS Management Console, de l'AWS CLI ou de l'API RDS.

Console

Pour surveiller les exportations d'instantanés de bases de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Snapshots (Instantanés).
3. Pour afficher la liste des exportations d'instantanés, choisissez l'onglet Exportations dans Amazon S3.
4. Pour afficher des informations sur une exportation d'instantané spécifique, choisissez la tâche d'exportation.

AWS CLI

Pour surveiller les exportations d'instantanés de bases de données à l'aide de l'AWS CLI, utilisez la commande describe-export-tasks .

L'exemple suivant montre comment afficher les informations actuelles sur toutes vos exportations d'instantanés.

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"
        }
    ]
}
```

Pour afficher des informations sur une exportation d'instantané spécifique, incluez l'option `--export-task-identifier` avec la commande `describe-export-tasks`. Pour filtrer la sortie, incluez l'option `--Filters`. Pour plus d'options, veuillez consulter la commande describe-export-tasks .

API RDS

Pour afficher des informations sur les exportations d'instantanés de bases de données à l'aide de l'API Amazon RDS, utilisez l'opération DescribeExportTasks .

Pour suivre l'achèvement du workflow d'exportation ou pour déclencher un autre workflow, vous pouvez vous abonner à des rubriques Amazon Simple Notification Service. Pour plus d'informations sur Amazon SNS, consultez Utilisation de la notification d'événement Amazon RDS (p. 467).

Annulation d'une tâche d'exportation d'instantané

Vous pouvez annuler une tâche d'exportation d'instantané de base de données à l'aide de l'AWS Management Console, de l'AWS CLI ou de l'API RDS.

> **Note**
>
> L'annulation d'une tâche d'exportation d'instantané ne supprime aucune des données exportées vers Amazon S3. Pour de plus amples informations sur la suppression des données à l'aide de la console, veuillez consulter Comment supprimer des objets d'un compartiment S3 ?. Pour supprimer les données à l'aide de l'interface de ligne de commande, utilisez la commande delete-object.

Console

Pour annuler une tâche d'importation d'instantané

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Snapshots (Instantanés).
3. Choisissez l'onglet Exports in Amazon S3 (Exportations dans Amazon S3) .
4. Choisissez la tâche d'exportation d'instantané que vous souhaitez annuler.
5. Choisissez Cancel (Annuler).
6. Choisissez Cancel export task (Annuler la tâche d'exportation) sur la page de confirmation.

AWS CLI

Pour annuler une tâche d'exportation d'instantané à l'aide de l'AWS CLI, utilisez la commande cancel-export-task. La commande requiert l'option `--export-task-identifier`.

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"
}
```

API RDS

Pour annuler une tâche d'exportation d'instantané à l'aide de l'API Amazon RDS, utilisez l'opération CancelExportTask avec le paramètre `ExportTaskIdentifier`.

Dépannage des erreurs d'autorisations PostgreSQL

Lors de l'exportation de bases de données PostgreSQL vers Amazon S3, vous pouvez voir une erreur `PERMISSIONS_DO_NOT_EXIST` indiquant que certaines tables ont été ignorées. Cela est généralement dû au superutilisateur, que vous spécifiez lors de la création de l'instance de base de données, qui n'a pas les autorisations d'accéder à ces tables.

Pour corriger cette erreur, exécutez la commande suivante :

```
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA schema_name TO superuser_name
```

Pour de plus amples informations sur les privilèges des superutilisateurs, veuillez consulter Privilèges du compte utilisateur principal (p. 1605).

Conversion des données lors de l'exportation vers un compartiment Amazon S3

Lorsque vous exportez un instantané de base de données vers un compartiment Amazon S3, Amazon RDS convertit les données, les exporte et les stocke au format Parquet. Pour de plus amples informations sur Parquet, veuillez consulter le site web Apache Parquet.

Parquet stocke toutes les données sous l'un des types primitifs suivants :

- BOOLEAN
- INT32
- INT64
- INT96
- FLOAT
- DOUBLE

- BYTE_ARRAY – Tableau d'octets de longueur variable, également connu sous le nom de binaire
- FIXED_LEN_BYTE_ARRAY – Tableau d'octets de longueur fixe utilisé lorsque les valeurs ont une taille constante

Les types de données Parquet sont peu nombreux afin de la complexité de la lecture et de l'écriture du format. Parquet fournit des types logiques pour étendre les types primitifs. Un type logique est implémenté sous forme d'annotation avec les données dans un champ de métadonnées `LogicalType`. L'annotation de type logique explique comment interpréter le type primitif.

Lorsque le type logique `STRING` annote un type `BYTE_ARRAY`, il indique que le tableau d'octets doit être interprété comme une chaîne de caractères codée en UTF-8. Une fois la tâche d'exportation terminée, Amazon RDS vous avertit si une conversion de chaîne s'est produite. Les données sous-jacentes exportées sont toujours les mêmes que celles de la source. Cependant, en raison de la différence d'encodage en UTF-8, certains caractères peuvent apparaître différents de la source lorsqu'ils sont lus dans des outils tels que Athena.

Pour de plus amples informations, veuillez consulter Parquet Logical Type Definitions dans la documentation Parquet.

Note

- Certains caractères ne sont pas pris en charge dans les noms de colonnes des tables de base de données. Les tables dont les noms de colonnes contiennent les caractères suivants sont ignorées lors de l'exportation.

```
,;{}()\n\t=
```

- Si les données contiennent une valeur très élevée proche de 500 Mo ou supérieure à ce nombre, l'exportation échoue.
- Si le nom de la base de données, du schéma ou de la table contient des espaces, l'exportation partielle n'est pas prise en charge. Toutefois, vous pouvez exporter l'intégralité de l'instantané de base de données.

Rubriques

- Mappage de type de données MySQL et MariaDB vers Parquet (p. 359)
- Mappage de type de données PostgreSQL vers Parquet (p. 362)

Mappage de type de données MySQL et MariaDB vers Parquet

Le tableau suivant montre le mappage des types de données MySQL et MariaDB aux types de données Parquet lorsque les données sont converties et exportées vers Amazon S3.

Type de données source	Type primitif du format Parquet	Annotation de type logique	Notes de conversion
Types de données numériques			
BIGINT	INT64		
BIGINT UNSIGNED	FIXED_LEN_BYTE_ARRAY(9)	DECIMAL(20,0)	Parquet ne prend en charge que les types signés, de sorte que le mappage nécessite un octet supplémentaire (8 plus

Type de données source	Type primitif du format Parquet	Annotation de type logique	Notes de conversion
			1) pour stocker le type BIGINT_UNSIGNED.
BIT	BYTE_ARRAY		
DECIMAL	INT32	DECIMAL(p,s)	Si la valeur source est inférieure à 2^{31}, elle est stockée sous la forme INT32.
	INT64	DECIMAL(p,s)	Si la valeur source est supérieure ou égale à 2^{31} mais inférieure à 2^{63}, elle est stockée sous la forme INT64.
	FIXED_LEN_BYTE_ARRAY(N)	DECIMAL(p,s)	Si la valeur source est supérieure ou égale à 2^{63}, elle est stockée sous la forme FIXED_LEN_BYTE_ARRAY(N).
	BYTE_ARRAY	STRING	Parquet ne prend pas en charge une précision décimale supérieure à 38. La valeur décimale est convertie en une chaîne de type BYTE_ARRAY et encodée en UTF8.
DOUBLE	DOUBLE		
FLOAT	DOUBLE		
INT	INT32		
INT UNSIGNED	INT64		
MEDIUMINT	INT32		
MEDIUMINT UNSIGNED	INT64		
NUMERIC	INT32	DECIMAL(p,s)	Si la valeur source est inférieure à 2^{31}, elle est stockée sous la forme INT32.
	INT64	DECIMAL(p,s)	Si la valeur source est supérieure ou égale à 2^{31} mais inférieure à 2^{63}, elle est stockée sous la forme INT64.

Type de données source	Type primitif du format Parquet	Annotation de type logique	Notes de conversion
	FIXED_LEN_ARRAY(N)	DECIMAL(p,s)	Si la valeur source est supérieure ou égale à 2^{63}, elle est stockée sous la forme FIXED_LEN_BYTE_ARRAY(N).
	BYTE_ARRAY	STRING	Parquet ne prend pas en charge la précision numérique supérieure à 38. Cette valeur numérique est convertie en une chaîne de type BYTE_ARRAY et encodée en UTF8.
SMALLINT	INT32		
SMALLINT UNSIGNED	INT32		
TINYINT	INT32		
TINYINT UNSIGNED	INT32		
Types de données chaîne			
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	
Types de données de date et d'heure			

Type de données source	Type primitif du format Parquet	Annotation de type logique	Notes de conversion
DATE	BYTE_ARRAY	STRING	Une date est convertie en une chaîne de type BYTE_ARRAY et encodée en UTF8.
DATETIME	INT64	TIMESTAMP_MICROS	
TIME	BYTE_ARRAY	STRING	Un type TIME est converti en une chaîne BYTE_ARRAY et encodé en UTF8.
TIMESTAMP	INT64	TIMESTAMP_MICROS	
YEAR	INT32		
Types de données géométriques			
GEOMETRY	BYTE_ARRAY		
GEOMETRYCOLLECTION	BYTE_ARRAY		
MULTIPOINT	BYTE_ARRAY		
MULTIPOLYGON	BYTE_ARRAY		
POINT	BYTE_ARRAY		
POLYGON	BYTE_ARRAY		
Type de données JSON			
JSON	BYTE_ARRAY	STRING	

Mappage de type de données PostgreSQL vers Parquet

Le tableau suivant montre le mappage des types de données PostgreSQL aux types de données Parquet lorsque les données sont converties et exportées vers Amazon S3.

Type de données PostgreSQL	Type primitif du format Parquet	Annotation de type logique	Notes de mappage
Types de données numériques			
BIGINT	INT64		
BIGSERIAL	INT64		
DECIMAL	BYTE_ARRAY	STRING	Un type DECIMAL est converti en une chaîne de type BYTE_ARRAY et encodé en UTF8. Cette conversion vise à éviter les complications dues à la précision des

Type de données PostgreSQL	Type primitif du format Parquet	Annotation de type logique	Notes de mappage
			données et aux valeurs de données qui ne sont pas un nombre (NaN).
DOUBLE PRECISION	DOUBLE		
INTEGER	INT32		
MONEY	BYTE_ARRAY	STRING	
REAL	FLOAT		
SERIAL	INT32		
SMALLINT	INT32	INT_16	
SMALLSERIAL	INT32	INT_16	
Types de chaînes et de données associés			
ARRAY	BYTE_ARRAY	STRING	Un tableau est converti en chaîne et encodé en tant que BINARY (UTF8). Cette conversion vise à éviter les complications dues à la précision des données, aux valeurs de données qui ne sont pas un nombre (NaN) et aux valeurs de données horaires.
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	
Types de données de date et d'heure			
DATE	BYTE_ARRAY	STRING	

Type de données PostgreSQL	Type primitif du format Parquet	Annotation de type logique	Notes de mappage
INTERVAL	BYTE_ARRAY	STRING	
TIME	BYTE_ARRAY	STRING	
TIME WITH TIME ZONE	BYTE_ARRAY	STRING	
TIMESTAMP	BYTE_ARRAY	STRING	
TIMESTAMP WITH TIME ZONE	BYTE_ARRAY	STRING	
Types de données géométriques			
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	
Types de données JSON			
JSON	BYTE_ARRAY	STRING	
JSONB	BYTE_ARRAY	STRING	
Autres types de données			
BOOLEAN	BOOLEAN		
CIDR	BYTE_ARRAY	STRING	Type de données de réseau
COMPOSITE	BYTE_ARRAY	STRING	
DOMAIN	BYTE_ARRAY	STRING	
INET	BYTE_ARRAY	STRING	Type de données de réseau
MACADDR	BYTE_ARRAY	STRING	
OBJECT IDENTIFIER	S/O		
PG_LSN	BYTE_ARRAY	STRING	
RANGE	BYTE_ARRAY	STRING	
UUID	BYTE_ARRAY	STRING	

Restauration d'une instance de base de données à une date spécifiée

Vous pouvez restaurer une instance de base de données à un point donné dans le temps, et créer ainsi une instance de base de données. Lorsque vous restaurez une instance de base de données à un instant dans le passé, le groupe de sécurité de base de données par défaut s'applique à la nouvelle instance de base de données. Si vous avez besoin d'appliquer des groupes de sécurité de base de données personnalisés à votre instance de base de données, vous devez le faire explicitement à l'aide de la AWS Management Console, de la commande `modify-db-instance` de l'AWS CLI ou de l'opération `ModifyDBInstance` de l'API Amazon RDS une fois que l'instance de base de données est disponible.

RDS charge les journaux de transaction pour les instances de bases de données Amazon S3 toutes les 5 minutes. Pour déterminer l'heure de restauration la plus récente pour une instance de base de données, utilisez la commande describe-db-instances de l'AWS CLI et examinez la valeur retournée dans le champ `LatestRestorableTime` de l'instance de base de données. Pour afficher l'heure de restauration la plus récente pour chaque instance de base de données dans la console Amazon RDS, choisissez Automated backups (Sauvegardes automatisées).

Vous pouvez procéder à une restauration à n'importe quel moment dans le passé au cours de la période de rétention des sauvegardes. Pour afficher l'heure de restauration la plus ancienne pour chaque instance de base de données, choisissez Automated backups (Sauvegardes automatisées) dans la console Amazon RDS.

> **Note**
>
> Nous vous recommandons de restaurer la même taille d'instance de base de données—et les mêmes E/S par seconde ou similaires si vous utilisez le stockage IOPS provisionnés—comme instance DB source. Vous pouvez obtenir une erreur si, par exemple, vous choisissez une taille d'instance de base de données avec une valeur d'IOPS incompatible.

Plusieurs des moteurs de base de données utilisés par Amazon RDS obéissent à des considérations particulières lors de la restauration à partir d'un instant dans le passé. Lorsque vous restaurez une instance de base de données Oracle à un instant dans le passé, vous pouvez spécifier que la nouvelle instance de base de données utilise un autre moteur de base de données Oracle, modèle de licence et DBName (SID). Lorsque vous restaurez une instance de base de données SQL à un instant dans le passé, chaque base de données au sein de cette instance est restaurée à un point dans le temps situé au sein d'1 seconde de chaque autre base de données de l'instance. Les transactions qui couvrent plusieurs bases de données au sein de l'instance peuvent ne pas être restaurées de manière cohérente. De plus, pour une instance de base de données SQL Server, les modes `OFFLINE`, `EMERGENCY` et `SINGLE_USER` ne sont pas pris en charge actuellement. La définition d'une base de données avec l'un de ces modes entraîne l'arrêt de la date de restauration possible la plus récente pour la totalité de l'instance.

Certaines actions, comme la modification du modèle de récupération d'une base de données SQL Server, peuvent rompre la séquence des journaux utilisés pour une restauration à un instant dans le passé. Dans certains cas, Amazon RDS peut détecter ce problème et l'heure de restauration la plus récente ne peut plus avancer. Dans d'autres cas, comme lorsqu'une base de données SQL Server utilise le modèle de récupération `BULK_LOGGED`, la rupture de la séquence de journalisation n'est pas détectée. Il se peut qu'il ne soit pas possible de restaurer une instance de base de données SQL Server à un instant dans le passé s'il existe une rupture dans la séquence de journalisation. Pour ces raisons, Amazon RDS ne prend pas en charge le modèle de récupération des bases de données SQL Server.

Vous pouvez restaurer une instance de base de données à un instant dans le passé à l'aide de la AWS Management Console, l'AWS CLI, ou l'API RDS.

Console

Pour restaurer une instance de base de données à une date spécifiée

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Automated backups (Sauvegardes automatisées).
3. Choisissez l'instance de base de données que vous souhaitez restaurer.
4. Sous Actions, sélectionnez Restaurer à un moment donné.

   La fenêtre Restaurer à un instant dans le passé s'affiche.
5. Choisissez Dernière heure de restauration possible pour restaurer à la dernière heure possible, ou choisissez Personnalisé pour choisir une heure.

   Si vous choisissez Personnalisé, saisissez la date et l'heure de restauration souhaitée de l'instance.

   > **Note**
   >
   > Les heures sont exprimées dans votre fuseau horaire local, qui est indiqué par son décalage par rapport à l'heure UTC. Par exemple, UTC-5 est l'heure normale de l'Est/heure avancée du Centre.
6. Pour Identifiant d'instance de base de données, entrez le nom de l'instance de base de données restaurée.
7. Choisissez d'autres options si nécessaire.
8. Choisissez Restaurer à un instant dans le passé.

AWS CLI

Pour restaurer une instance de base de données à une date spécifiée, utilisez la commande `restore-db-instance-to-point-in-time` de l'interface de ligne de commande AWS pour créer une nouvelle instance de base de données.

Example

Pour Linux, macOS ou 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
```

Pour 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
```

API RDS

Pour restaurer une instance de base de données à une date spécifiée, appelez l'opération d'API Amazon RDS `RestoreDBInstanceToPointInTime` avec les paramètres suivants :

- `SourceDBInstanceIdentifier`

- `TargetDBInstanceIdentifier`
- `RestoreTime`

Suppression d'un instantané

Vous pouvez supprimer des instantanés de base de données gérés par Amazon RDS lorsque vous n'en avez plus besoin.

> Note
>
> Pour supprimer des sauvegardes gérées par AWS Backup, utilisez la console AWS Backup. Pour de plus amples informations sur AWS Backup, veuillez consulter le Manuel du développeur AWS Backup.

Suppression d'un instantané de base de données

Vous pouvez supprimer un instantané de base de données manuel, partagé ou public à l'aide de l'AWS Management Console, de l'AWS CLI ou de l'API RDS.

Pour supprimer un instantané partagé ou public, vous devez vous connecter au compte AWS propriétaire de l'instantané.

Si vous souhaitez supprimer des instantanés de base de données automatiques sans supprimer l'instance de base de données, définissez la période de conservation des sauvegardes de l'instance de base de données sur 0. Les instantanés automatiques sont supprimés lorsque la modification est appliquée. Vous pouvez appliquer la modification immédiatement si vous ne souhaitez pas attendre la prochaine période de maintenance. Une fois la modification terminée, vous pouvez réactiver les sauvegardes automatiques en définissant la période de conservation des sauvegardes sur un nombre supérieur à 0. Pour plus d'informations sur la modification d'une instance de base de données , consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Si vous avez supprimé une instance de base de données, vous pouvez supprimer ses instantanés de base de données automatiques en supprimant les sauvegardes automatiques de l'instance de base de données. Pour plus d'informations sur les sauvegardes automatiques, consultez Utilisation des sauvegardes (p. 317).

Console

Pour supprimer un instantané de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Instantanés.
3. Choisissez l'instantané de base de données à supprimer.
4. Pour Actions, choisissez Supprimer la pile.
5. Dans la page de confirmation, sélectionnez Supprimer.

AWS CLI

Vous pouvez supprimer un instantané de base de données en utilisant la commande delete-db-snapshot de l'AWS CLI.

Les options suivantes sont utilisées pour supprimer un instantané de base de données.

- `--db-snapshot-identifier` – Identifiant de l'instantané de base de données.

Example

Le code suivant supprime l'instantané de base de données `mydbsnapshot`.

Pour Linux, macOS ou Unix :

```
aws rds delete-db-snapshot \
    --db-snapshot-identifier mydbsnapshot
```

Pour Windows :

```
aws rds delete-db-snapshot ^
    --db-snapshot-identifier mydbsnapshot
```

API RDS

Vous pouvez supprimer un instantané de base de données en utilisant l'opération d'API Amazon RDS DeleteDBSnapshot.

Les paramètres suivants sont utilisés pour supprimer un instantané de base de données.

- `DBSnapshotIdentifier` – Identifiant de l'instantané de base de données.

Didacticiel : restaurer une instance de base de données à partir d'un instantané de base de données

Un scénario fréquent lors de l'utilisation d'Amazon RDS consiste à avoir une instance de base de données que vous utilisez occasionnellement, mais dont vous n'avez pas besoin en permanence. Par exemple, vous pouvez avoir une enquête client trimestrielle qui utilise une instance Amazon Elastic Compute Cloud (Amazon EC2) pour héberger un site web d'enquête et une instance de base de données pour stocker les résultats de l'enquête. Une solution pour économiser de l'argent sur un tel scénario consiste à prendre un instantané de base de données de l'instance de base de données une fois l'enquête terminée, à supprimer l'instance de base de données et à restaurer cette dernière quand vous avez besoin de reconduire l'enquête.

Dans l'illustration suivante, vous pouvez voir le scénario où une instance EC2 hébergeant un site web d'enquête client se trouve dans le même Amazon Virtual Private Cloud (Amazon VPC) qu'une instance de base de données conservant les données de l'enquête client. Notez que chaque instance possède son propre groupe de sécurité ; le groupe de sécurité de l'instance EC2 autorise l'accès depuis Internet, tandis que le groupe de sécurité de l'instance de base de données autorise uniquement l'accès depuis ou vers l'instance EC2. Lorsque l'enquête est terminée, l'instance EC2 peut être arrêtée et l'instance de base de données peut être supprimée après la création d'un instantané de base de données final. Si vous devez mener une nouvelle enquête client, vous pouvez redémarrer l'instance EC2 et restaurer l'instance de base de données à partir de l'instantané de base de données.

Pour plus d'informations sur la configuration des groupes de sécurité VPC nécessaires pour ce scénario qui permet à l'instance EC2 de se connecter à l'instance de base de données, consultez Une instance de base de données d'un VPC accédée par une instance EC2 du même VPC (p. 1613).

Vous devez créer un instantané de base de données avant de pouvoir restaurer une instance de base de données à partir de celui-ci. Lorsque vous restaurez l'instance de base de données, vous indiquez le nom de l'instantané de base de données à partir duquel la restauration est effectuée, puis un nom pour la nouvelle instance de base de données créée à partir de l'opération de restauration. Vous ne pouvez pas restaurer un instantané de base de données sur une instance de base de données existante ; une nouvelle instance de base de données est créée lors de la restauration.

Conditions requises pour la restauration d'une instance de base de données à partir d'un instantané de base de données

Certains paramètres de l'instance de base de données restaurée étant réinitialisés quand l'instance est restaurée, vous devez conserver les ressources originales pour pouvoir restaurer l'instance de base de données à ses paramètres précédents. Par exemple, si vous restaurez une instance de base de données à partir d'un instantané de base de données, le paramètre DB par défaut et un groupe de sécurité par défaut sont associés à l'instance restaurée. Cette association signifie que le groupe de sécurité par défaut n'autorise pas l'accès à l'instance de base de données, et aucune valeur de paramètre personnalisée n'est disponible dans le groupe de paramètres par défaut. Vous devez conserver le groupe de paramètres de base de données et le groupe de sécurité associé à l'instance de base de données utilisée pour créer l'instantané de base de données.

Les conditions suivantes sont requises pour que vous puissiez restaurer une instance de base de données à partir d'un instantané de base de données :

- Vous devez avoir créé un instantané de base de données d'une instance de base de données avant de pouvoir restaurer une instance de base de données à partir de cet instantané de base de données. Pour plus d'informations sur la création d'un instantané de base de données, consultez Création d'un instantané de base de données (p. 327).
- Vous devez conserver le groupe de paramètres et le groupe de sécurité associé à l'instance de base de données à partir de laquelle vous avez créé l'instantané de base de données.

- Vous devez déterminer le groupe d'options correct pour l'instance de base de données restaurée :
  - Le groupe d'options associé à l'instantané de base de données à partir duquel vous avez procédé à la restauration est associé à l'instance de base de données restaurée une fois la création effectuée. Par exemple, si l'instantané de base de données à partir duquel vous effectuez la restauration utilise Oracle Transparent Data Encryption (TDE), l'instance de base de données restaurée utilise le même groupe d'options, lequel incluait l'option TDE.
  - Vous ne pouvez pas utiliser le groupe d'options associé à l'instance de base de données originale si vous tentez de restaurer cette instance dans un autre VPC ou sur une plateforme différente. Cette restriction intervient parce que, quand un groupe d'options est affecté à une instance de base de données, il est également lié à la plateforme sur laquelle se trouve l'instance de base de données, à savoir VPC ou EC2-Classic (non-VPC). Si une instance de base de données est dans un VPC, le groupe d'options associé à l'instance est lié à ce VPC.
  - Si vous restaurez une instance de base de données dans un autre VPC ou sur une autre plateforme, vous devez attribuer le groupe d'options par défaut à l'instance, assigner un groupe d'options lié à ce VPC ou à cette plateforme, ou créer un groupe d'options et l'affecter à l'instance de base de données. Notez qu'avec les options permanentes ou persistantes, telles qu'Oracle TDE, vous devez créer un nouveau groupe d'options incluant l'option persistante ou permanente lorsque vous restaurez une instance de base de données dans un VPC différent. Pour plus d'informations sur l'utilisation de groupes d'options, consultez Utilisation de groupes d'options (p. 209).

Restauration d'une instance de base de données à partir d'un instantané de base de données

Vous pouvez utiliser la procédure suivante pour restaurer à partir d'un instantané dans AWS Management Console.

Pour restaurer une instance de base de données à partir d'un instantané de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Snapshots (Instantanés).
3. Choisissez l'instantané de base de données à partir duquel vous voulez restaurer.
4. Pour Actions, choisissez Restaurer l'instantané.

   La page Restaurer l'instantané s'affiche.
5. Pour Identifiant d'instance DB, sous Paramètres, tapez le nom unique que vous voulez utiliser pour l'instance de base de données restaurée.

   Si vous restaurez à partir d'une instance de base de données que vous avez supprimée après avoir effectué l'instantané de base de données, vous pouvez utiliser le nom de cette instance de base de données.
6. Choisissez des paramètres supplémentaires selon vos besoins.
7. Choisissez Restore DB Instance.

Modification d'une instance de base de données restaurée

Dès que la restauration est terminée, vous devez associer le groupe de sécurité personnalisé utilisé par l'instance à partir de laquelle vous avez restauré à tout groupe de paramètres DB personnalisé applicable que vous pourriez avoir. Seul le paramètre DB par défaut et les groupes de sécurité sont associés à l'instance restaurée. Pour restaurer la fonctionnalité de l'instance de base de données à celle de l'instance de base de données à partir de laquelle l'instantané a été créé, vous devez modifier l'instance de base de données afin d'utiliser le groupe de sécurité et le groupe de paramètres utilisés par l'instance de base de données précédente.

Vous devez appliquer les modifications explicitement à l'aide de la commande Modifier de la console RDS, de l'API `ModifyDBInstance` ou de l'outil de ligne de commande `aws rds modify-db-instance`, lorsque l'instance de base de données est disponible. Nous vous recommandons de conserver les groupes de paramètres de tout instantané de base de données en votre possession, de telle sorte que vous puissiez associer une instance restaurée au fichier de paramètres approprié.

Vous pouvez modifier les autres paramètres sur l'instance de base de données restaurée. Par exemple, vous pouvez utiliser un autre type de stockage que l'instantané de base de données source. Dans ce cas, le processus de restauration est plus lent, à cause du travail supplémentaire nécessaire pour migrer les données vers le nouveau type de stockage. En cas de restauration depuis ou vers un stockage Magnétique (Standard), le processus de migration est plus lent, car le stockage Magnétique ne dispose pas des mêmes capacités IOPS des IOPS provisionnées ou du stockage à usage général (SSD).

Les étapes suivantes assument que votre instance de base de données se trouve dans un VPC. Si votre instance de base de données ne se trouve pas dans un VPC, utilisez AWS Management Console pour trouver le Security Group DB dont vous avez besoin pour l'instance de base de données.

Pour modifier une instance de base de données restaurée afin qu'elle ait les paramètres de l'instance de base de données originale

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez le nom de l'instance de base de données créée lorsque vous avez effectué la restauration à partir de l'instantané de base de données pour en afficher les détails. Choisissez l'onglet Connectivity (Connectivité). Le groupe de sécurité attribué à l'instance de base de données peut ne pas autoriser l'accès. S'il n'existe aucune règle entrante, aucune autorisation n'autorise l'accès entrant.

4. Sélectionnez Modify.
5. Dans la section Network & Security (Réseau et sécurité), sélectionnez le groupe de sécurité que vous voulez utiliser pour votre instance de base de données. Si vous devez ajouter des règles pour créer un groupe de sécurité à utiliser avec une instance EC2, consultez Une instance de base de données d'un VPC accédée par une instance EC2 du même VPC (p. 1613) pour plus d'informations.

   Vous pouvez également supprimer un groupe de sécurité en choisissant le signe X qui lui est associé.

6. Choisissez Continuer, puis Appliquer immédiatement.
7. Choisissez Modifier l'instance de base de données.

   Une fois le statut de l'instance disponible, choisissez le nom de l'instance de base de données pour en afficher les détails. Choisissez l'onglet Connectivity (Connectivité), puis confirmez que le nouveau groupe de sécurité a été appliqué, ce qui autorise l'accès de l'instance de base de données.

Surveillance d'une instance de base de données Amazon RDS

Cette section vous explique comment surveiller Amazon RDS.

Rubriques

- Présentation de la surveillance de Amazon RDS. (p. 373)
- Statut d'instance de bases de données (p. 386)
- Utilisation des recommandations Amazon RDS (p. 389)
- Surveillance améliorée (p. 394)
- Utilisation d'Amazon RDS Performance Insights (p. 410)
- Utilisation de la notification d'événement Amazon RDS (p. 467)
- Affichage d'événements Amazon RDS (p. 486)
- Obtention d'événements CloudWatch Events et Amazon EventBridge pour Amazon RDS (p. 487)
- Amazon RDS Fichiers journaux de base de données (p. 490)
- Utilisation de AWS CloudTrail et Amazon RDS (p. 526)

Présentation de la surveillance de Amazon RDS.

La surveillance est un enjeu important pour assurer la fiabilité, la disponibilité et les performances de Amazon RDS et de vos solutions AWS. Pour déboguer plus facilement une éventuelle défaillance à plusieurs points, nous vous recommandons de collecter les données de surveillance de toutes les parties de votre solution AWS.

Plan de surveillance

Avant de commencer la surveillance Amazon RDS, nous vous recommandons de créer un plan de surveillance. Ce plan doit répondre aux questions suivantes :

- Quels sont les objectifs de la surveillance ?
- Quelles sont les ressources à surveiller ?
- A quelle fréquence les ressources doivent-elles être surveillées ?
- Quels outils de surveillance utiliser ?
- Qui exécute les tâches de surveillance ?
- Qui doit être informé en cas de problème ?

Référence des performances

Pour atteindre vos objectifs de surveillance, vous devez établir une référence. Pour ce faire, mesurez les performances dans différentes conditions de charge et à différents moments dans votre environnement Amazon RDS. Vous pouvez surveiller les métriques suivantes :

- Débit réseau
- Connexions client
- E/S pour les opérations de lecture, d'écriture ou de métadonnées

- Soldes de crédit en rafales pour vos instances de base de données

Nous vous recommandons de stocker les données de performances historiques pour Amazon RDS. À l'aide des données stockées, vous pouvez comparer les performances actuelles aux tendances passées. Vous pouvez également faire la distinction entre les modèles normaux de performances et les anomalies, puis concevoir des méthodes pour résoudre les problèmes.

Instructions sur les performances

En général, les valeurs acceptables pour les métriques de performances dépendent de l'activité de votre application par rapport à votre référence. Enquêtez sur les écarts cohérents ou tendanciels de vos données de référence. Les métriques suivantes sont souvent à l'origine des problèmes de performances :

- Forte utilisation de l'UC et de la RAM – Des valeurs importantes de l'utilisation de l'UC et de la RAM peuvent être appropriées, si elles sont conformes aux objectifs pour votre application (comme le débit ou la simultanéité).
- Utilisation de l'espace disque – Enquêtez sur l'utilisation de l'espace disque si l'espace utilisé est constamment égal ou supérieur à 85 pour cent de l'espace disque total. Voyez s'il est possible de supprimer des données de l'instance ou d'archiver des données sur un système différent pour libérer de l'espace.
- Trafic réseau – Pour le trafic réseau, discutez avec votre administrateur pour connaître le débit attendu pour votre domaine réseau et votre connexion Internet. Enquêtez sur le trafic réseau si le débit est constamment inférieur à vos attentes.
- Connexions de la base de données – Envisagez de limiter les connexions de la base de données si vous constatez un nombre important de connexions utilisateur en même temps qu'une baisse des performances de l'instance et des temps de réponse. Le bon nombre de connexions utilisateur pour votre instance de base de données dépend de votre classe d'instance et de la complexité des opérations exécutées. Pour déterminer le nombre de connexions de la base de données, associez votre instance de base de données à un groupe de paramètres dans lequel le paramètre `User Connections` est configuré sur une autre valeur que 0 (illimité). Vous pouvez utiliser un groupe de paramètres existant ou en créer un nouveau. Pour plus d'informations, consultez Utilisation de groupes de paramètres de base de données (p. 225).
- Métriques IOPS – Les valeurs attendues pour les métriques d'IOPS par seconde dépendent de la spécification du disque et de la configuration du serveur, donc utilisez vos données de référence pour connaître les caractéristiques typiques. Enquêtez si les valeurs sont constamment différentes de vos données de référence. Pour de meilleures performances d'E/S par seconde, veillez à ce que votre ensemble de travail typique puisse être chargé en mémoire pour minimiser les opérations de lecture et écriture.

Lorsque les performances se situent en dehors de votre de base établie, vous devrez peut-être apporter des modifications pour optimiser la disponibilité de votre base de données pour votre charge de travail. Par exemple, vous devrez peut-être modifier la classe d'instance de votre instance de base de données. Ou encore, modifier le nombre d'instances de base de données et de réplicas en lecture disponibles pour les clients.

Outils de surveillance

AWS fournit différents outils que vous pouvez utiliser pour surveiller Amazon RDS. Vous pouvez configurer certains de ces outils pour qu'ils effectuent la surveillance automatiquement, tandis que d'autres nécessitent une intervention manuelle.

Outils de surveillance automatique

Nous vous recommandons d'automatiser le plus possible les tâches de surveillance.

Outils de création de rapports Amazon RDS

Vous pouvez utiliser les outils automatiques suivants pour surveiller Amazon RDS et signaler un problème éventuel :

- Événements Amazon RDS – Abonnez-vous aux événements Amazon RDS pour être informé des modifications qui se produisent au niveau d'une instance de base de données, d'un , d'un instantané de base de données, d'un , d'un groupe de paramètres de base de données ou d'un groupe de sécurité de base de données. Pour plus d'informations, consultez Utilisation de la notification d'événement Amazon RDS (p. 467).
- Database log files (Fichiers de journaux de base de données) – Affichez, téléchargez ou consultez les fichiers journaux de base de données à l'aide de la console Amazon RDS ou des opérations d'API Amazon RDS. Vous pouvez également interroger certains fichiers journaux de base de données qui sont chargés dans des tables de base de données. Pour plus d'informations, consultez Amazon RDS Fichiers journaux de base de données (p. 490).
- Surveillance améliorée Amazon RDS — Consultez les métriques en temps réel pour le système d'exploitation. Pour plus d'informations, consultez Surveillance améliorée (p. 394).
- Performance Insights Amazon RDS — Pour évaluer rapidement la charge sur votre base de données et déterminer où et quand prendre des mesures. Pour de plus amples informations, veuillez consulter Utilisation d'Amazon RDS Performance Insights (p. 410).
- Recommandations Amazon RDS — Consultez les recommandations automatisées pour les ressources de base de données, telles que les instances de base de données, les les réplicas en lecture, et les groupes de paramètres de de base de données. Pour plus d'informations, consultez Utilisation des recommandations Amazon RDS (p. 389).

Outils de surveillance intégrés

Amazon RDS s'intègre à Amazon CloudWatch, Amazon EventBridge et AWS CloudTrail pour offrir des fonctions de surveillance supplémentaires :

- Amazon CloudWatch – Ce service surveille vos ressources AWS et les applications que vous exécutez sur AWS en temps réel. Vous pouvez utiliser les fonctions Amazon CloudWatch suivantes avec Amazon RDS :
  - Métriques Amazon CloudWatch – Amazon RDS envoie automatiquement des métriques à CloudWatch toutes les minutes pour chaque base de données active. Vous n'aurez pas de frais supplémentaires à régler pour les métriques Amazon RDS dans CloudWatch. Pour plus d'informations, consultez the section called "Affichage des métriques d'instances de base de données" (p. 384).
  - Alarmes Amazon CloudWatch – Vous pouvez regarder une seule métrique Amazon RDS sur une période donnée. Vous pouvez ensuite effectuer une ou plusieurs actions en fonction de la valeur de la métrique selon le seuil que vous définissez. Pour plus d'informations, consultez Surveillance avec Amazon CloudWatch (p. 376).
- Amazon CloudWatch Logs – La plupart des moteurs de base de données vous permettent de surveiller, de stocker et d'accéder aux fichiers journaux dans CloudWatch Logs. Pour de plus amples informations, veuillez consulter Amazon CloudWatch Logs User Guide.
- Amazon EventBridge – est un service de bus d'événements sans serveur qui facilite la connexion de vos applications aux données provenant de diverses sources. EventBridge fournit un flux de données en temps réel à partir de vos propres applications, applications Software-as-a-Service (SaaS) et services AWS, et achemine ces données vers des cibles telles que Lambda. Cela vous permet de surveiller les événements qui se produisent dans les services et de créer des architectures basées sur les événements. Pour de plus amples informations, veuillez consulter Obtention d'événements CloudWatch Events et Amazon EventBridge pour Amazon RDS (p. 487).
- AWS CloudTrail – Vous pouvez voir un enregistrement d'actions qu'un utilisateur, un rôle ou un service AWS entreprend dans Amazon RDS. CloudTrail capture comme des événements tous les appels d'API pour Amazon RDS. Ces captures incluent les appels de la console Amazon RDS et les appels de

code vers les opérations d'API Amazon RDS. Si vous créez un journal de suivi, vous pouvez activer la livraison continue des événements CloudTrail dans un compartiment Amazon S3, y compris des événements pour Amazon RDS. Si vous ne configurez pas de journal de suivi, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Event history (Historique des événements). Pour de plus amples informations, veuillez consulter Utilisation de AWS CloudTrail et Amazon RDS (p. 526).

Outils de surveillance manuelle

Vous devez surveiller manuellement les éléments que les CloudWatch alarmes ne couvrent pas. Les tableaux de bord des consoles Amazon RDS, CloudWatch, AWS Trusted Advisor et d'autres consoles AWS fournissent un aperçu de l'état de votre environnement AWS. Nous recommandons de consulter également les fichiers journaux sur votre instance de base de données.

- À partir de la console Amazon RDS, vous pouvez surveiller les éléments suivants pour vos ressources :
  - Nombre de connexions à une instance de base de données
  - Quantité d'opérations de lecture et d'écriture à une instance de base de données
  - Volume de stockage en cours d'utilisation par une instance de base de données
  - Quantité de mémoire et d'UC utilisée pour une instance de base de données
  - Quantité de trafic réseau en direction et à partir d'une instance de base de données
- A partir du tableau de bord Trusted Advisor, vous pouvez vérifier les amélioration dans les domaines de l'optimisation des coûts, de la sécurité, de la tolérance aux pannes et des performances :
  - Instances de base de données Amazon RDS inactives
  - Risque lié à l'accès aux groupes de sécurité Amazon RDS
  - Sauvegardes Amazon RDS
  - Multi-AZ Amazon RDS

  Pour plus d'informations sur ces vérifications, consultez Bonnes pratiques Trusted Advisor (Checks).
- La page d'accueil CloudWatch présente :
  - Alarmes et statuts en cours
  - Graphiques des alarmes et des ressources
  - Statut d'intégrité du service

  De plus, vous pouvez utiliser CloudWatch pour effectuer les tâches suivantes :
  - Créer des tableaux de bord personnalisés pour surveiller les services qui vous intéressent.
  - Données de métriques de graphiques pour résoudre les problèmes et découvrir les tendances.
  - Rechercher et parcourir toutes les métriques des ressources AWS.
  - Créer et modifier des alarmes pour être informé des problèmes.

Surveillance avec Amazon CloudWatch

Vous pouvez surveiller vos instances de base de données avec Amazon CloudWatch, qui recueille et traite les données brutes de Amazon RDS en métriques lisibles et disponibles en quasi temps réel. Par défaut, les données des métriques Amazon RDS sont automatiquement envoyées à CloudWatch toutes les minutes. Pour de plus amples informations sur CloudWatch, veuillez consulter Qu'est-ce que Amazon CloudWatch ? dans le Guide de l'utilisateur Amazon CloudWatch.

Les points de données d'une durée de 60 secondes (1 minute) sont disponibles pendant 15 jours Cela signifie que pouvez accéder aux informations historiques et acquérir un meilleur point de vue de la façon dont votre service ou application web s'exécute. Pour de plus amples informations sur la conservation

des métriques CloudWatch, veuillez consulter Conservation des métriques dans le Guide de l'utilisateur Amazon CloudWatch.

> **Note**
>
> Si vous utilisez Amazon RDS Performance Insights, des métriques supplémentaires sont disponibles. Pour plus d'informations, consultez Métriques Performance Insights publiées dans Amazon CloudWatch (p. 464).

Métriques et dimensions d'Amazon RDS

Lorsque vous utilisez les ressources Amazon RDS, Amazon RDS envoie les métriques et les dimensions à Amazon CloudWatch toutes les minutes. Vous pouvez utiliser les procédures suivantes pour afficher les métriques d'Amazon RDS.

Pour afficher des métriques à l'aide de la console Amazon CloudWatch

Les métriques sont d'abord regroupées par espace de noms de service, puis par les différentes combinaisons de dimension au sein de chaque espace de noms.

1. Ouvrez la console CloudWatch à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Si nécessaire, changez la région AWS. Dans la barre de navigation, choisissez la région AWS où se trouvent vos données AWS. Pour de plus amples informations, veuillez consulter Régions et points de terminaison.
3. Dans le volet de navigation, choisissez Metrics. Choisissez l'espace de nom de métrique RDS.

4. Sélectionnez une dimension de métrique, par exemple By Database Class (Par classe de base de données).
5. Pour trier les métriques, utilisez l'en-tête de colonne. Pour représenter graphiquement une métrique, cochez la case en regard de la métrique. Pour filtrer par ressource, sélectionnez l'ID de ressource, puis

Add to search (Ajouter à la recherche). Pour filtrer par métrique, choisissez le nom de la métrique, puis Add to search (Ajouter à la recherche).

Pour afficher les métriques à l'aide de AWS CLI

- A partir d'une invite de commande, utilisez la commande suivante.

```
aws cloudwatch list-metrics --namespace AWS/RDS
```

Métriques Amazon RDS

L'espace de noms `AWS/RDS` inclut les métriques suivantes.

> **Note**
>
> La console Amazon RDS peut afficher des métriques dans des unités différentes des unités envoyées à Amazon CloudWatch. Par exemple, la console Amazon RDS peut afficher une métrique en mégaoctets (Mo), alors qu'elle est envoyée à Amazon CloudWatch en octets.

Métrique	Nom de la console	Description
`BinLogDiskUsage`	Utilisation du disque par les journaux binaires (Mo)	Quantité d'espace disque occupée par les journaux binaires sur le principal. Concerne les réplicas en lecture MySQL. Unités : octets
`BurstBalance`	Solde de la rafale (Pourcentage)	Pourcentage de crédits d'E/S disponibles dans le compartiment en rafales pour les SSD à usage général (gp2). Unités : pourcentage

Métrique	Nom de la console	Description
`CPUUtilization`	Utilisation du processeur (pourcentage)	Pourcentage d'utilisation de la CPU. Unités : pourcentage
`CPUCreditUsage`	Utilisation du crédit de l'UC (nombre)	(Instances T2) Nombre de crédits UC dépensés par l'instance pour l'utilisation de l'UC. Un crédit UC équivaut à un vCPU fonctionnant à 100 % d'utilisation pendant une minute ou une combinaison équivalente de vCPU, d'utilisation et de temps. Par exemple, vous pouvez avoir un vCPU fonctionnant à 50 % d'utilisation pendant deux minutes ou deux vCPU fonctionnant à 25 % d'utilisation pendant deux minutes. Les métriques de crédits UC sont disponibles uniquement toutes les 5 minutes. Si vous spécifiez une période supérieure à cinq minutes, utilisez la statistique `Sum` au lieu de la statistique `Average`. Unités : crédits (minutes vCPU)
`CPUCreditBalance`	Solde de crédit UC (nombre)	(Instances T2) Nombre de crédits UC gagnés qu'une instance a accumulés depuis son lancement ou son démarrage. Pour les instances T2 Standard, le `CPUCreditBalance` inclut également le nombre de crédits de lancement qui ont été accumulés. Les crédits sont accumulés dans le solde de crédits quand ils sont gagnés et supprimés du solde de crédits lorsqu'ils sont dépensés. Le solde de crédits présente une limite maximum qui est déterminée par la taille de l'instance. Une fois que la limite est atteinte, tous les nouveaux crédits gagnés sont rejetés. Pour les instances T2 Standard, les crédits de lancement ne sont pas comptés dans la limite. L'instance peut dépenser les crédits figurant dans le `CPUCreditBalance` pour dépasser le niveau de base de l'utilisation de l'UC. Les crédits figurant dans le `CPUCreditBalance` d'une instance en cours d'exécution n'expirent pas. Lorsque l'instance s'arrête, le `CPUCreditBalance` ne persiste pas, et tous les crédits accumulés sont perdus. Les métriques de crédits UC sont disponibles uniquement toutes les 5 minutes. Unités : crédits (minutes vCPU)

Métrique	Nom de la console	Description
`DatabaseConnections`	Connexions de base de données (nombre)	Nombre de connexions de base de données en cours d'utilisation. La valeur de métrique peut ne pas inclure les connexions de base de données interrompues qui n'ont pas encore été nettoyées par votre base de données. Ainsi, le nombre de connexions de base de données enregistrées par votre base de données peut être supérieur à la valeur de métrique. Unités : nombre
`DiskQueueDepth`	Profondeur de la file d'attente (nombre)	Nombre de demandes d'E/S (lecture et écriture) en attente d'accès au disque. Unités : nombre
`FailedSQLServerAgentJobsCount`	Nombre de tâches de SQL Server Agent ayant échoué (nombre/minute)	Nombre de tâches Microsoft SQL Server Agent ayant échoué au cours de la dernière minute. Unité : nombre/minute
`FreeableMemory`	Mémoire libérable (Mo)	Quantité de mémoire vive disponible. Pour les instances de bases de données MariaDB, MySQL, Oracle et PostgreSQL, cette métrique rapporte la valeur du champ `MemAvailable` de `/proc/meminfo`. Unités : octets
`FreeStorageSpace`	Espace de stockage disponible (Mo)	Quantité d'espace de stockage disponible. Unités : octets
`MaximumUsedTransactionIDs`	Nombre maximal d'ID de transaction utilisés (nombre)	Le nombre d'ID de transaction maximum qui ont été utilisés. S'applique à PostgreSQL. . Unités : nombre
`NetworkReceiveThroughput`	Débit de réception réseau (Mo/seconde)	Trafic de réseau entrant (réception) sur l'instance DB, notamment le trafic de base de données client et le trafic Amazon RDS, utilisé pour la supervision et la réplication. Unités : octets/seconde
`NetworkTransmitThroughput`	Débit de transmission réseau (Mo/seconde)	Trafic de réseau sortant (transmission) sur l'instance DB, comprenant le trafic de base de données client et le trafic Amazon RDS, utilisé pour la supervision et la réplication. Unités : octets/seconde
`OldestReplicationSlotLag`	Retard emplacement de réplication le plus ancien (Mo)	Taille du retard du réplica le plus en retard en termes de données WAL reçues. S'applique à PostgreSQL. Unités : mégaoctets

Métrique	Nom de la console	Description
`ReadIOPS`	E/S par seconde en lecture (nombre/seconde)	Nombre moyen d'opérations d'E/S de lecture de disque par seconde. Unités : nombre/seconde
`ReadLatency`	Latence en lecture (millisecondes)	Temps moyen nécessaire pour les opérations d'E/S par disque. Unités : secondes
`ReadThroughput`	Débit de lecture (Mo/seconde)	Nombre moyen d'octets lus sur le disque par seconde. Unités : octets/seconde
`ReplicaLag`	Retarde du réplica (millisecondes)	Durée pendant laquelle une instance de base de données de réplica en lecture retarde l'instance de base de données source. S'applique aux réplicas en lecture MySQL, MariaDB, Oracle, PostgreSQL et SQL Server. Unités : secondes
`ReplicationSlotDiskUsage`	Utilisation du disque par emplacement de réplica (Mo)	Espace disque utilisé par les fichiers d'emplacement de réplication. S'applique à PostgreSQL. Unités : mégaoctets
`SwapUsage`	Utilisation d'espace d'échange (Mo)	Quantité d'espace d'échange utilisé sur l'instance DB. Cette métrique n'est pas disponible pour SQL Server. Unités : octets
`TransactionLogsDiskUsage`	Utilisation du disque par les journaux de transactions (Mo)	Espace disque utilisé par les journaux de transactions. S'applique à PostgreSQL. Unités : mégaoctets
`TransactionLogsGeneration`	Génération des journaux de transactions (Mo/seconde)	Taille de journaux de transactions générés par seconde. S'applique à PostgreSQL. Unités : octets/seconde
`WriteIOPS`	E/S par seconde en écriture (nombre/seconde)	Nombre moyen d'opérations d'E/S d'écriture de disque par seconde. Unités : nombre/seconde
`WriteLatency`	Latence d'écriture (millisecondes)	Temps moyen nécessaire pour les opérations d'E/S par disque. Unités : secondes
`WriteThroughput`	Débit d'écriture (Mo/seconde)	Nombre moyen d'octets écrits sur le disque par seconde. Unités : octets/seconde

Dimensions Amazon RDS

Les données des métriques de Amazon RDS peuvent être filtrées à l'aide des dimensions du tableau suivant :

Dimension	Description
`DBInstanceIdentifier`	Cette dimension filtre les données que vous demandez en fonction d'une instance de base de données spécifique.
`DBClusterIdentifier`	Cette dimension filtre les données que vous demandez pour un cluster de base de données Amazon Aurora spécifique.
`DBClusterIdentifier, Role`	Cette dimension filtre les données que vous demandez pour un cluster de base de données Aurora spécifique, en regroupant les métriques par rôle d'instance (WRITER/READER). Par exemple, vous pouvez regrouper des métriques pour toutes les instances READER qui appartiennent à un cluster.
`DatabaseClass`	Cette dimension filtre les données que vous demandez pour toutes les instances dans une classe de base de données. Par exemple, vous pouvez regrouper des métriques pour toutes les instances qui appartiennent à la classe de base de données `db.r5.large`.
`EngineName`	Cette dimension filtre les données que vous demandez en fonction du nom du moteur identifié uniquement. Par exemple, vous pouvez regrouper des métriques pour toutes les instances ayant le nom de moteur `mysql`.
`SourceRegion`	Cette dimension filtre les données que vous demandez pour la région spécifiée uniquement. Par exemple, vous pouvez regrouper des métriques pour toutes les instances de la région `us-east-1`.

Création d'alarmes CloudWatch pour surveiller Amazon RDS

Vous pouvez créer une alarme CloudWatch qui envoie un message Amazon SNS lorsque l'alarme change d'état. Une alarme surveille une seule métrique pendant la période que vous spécifiez. Elle peut également réaliser une ou plusieurs actions en fonction de la valeur de la métrique par rapport à un seuil donné sur un certain nombre de périodes. Cette action est une notification envoyée vers une rubrique Amazon SNS ou une stratégie Amazon EC2 Auto Scaling.

Les alarmes appellent les actions pour les modifications d'état soutenues uniquement. Les alarmes CloudWatch n'appellent pas une action uniquement parce qu'elles se trouvent dans un état particulier. L'état doit avoir changé et avoir été maintenu pendant un nombre de périodes spécifié. Les procédures suivantes montrent comment créer des alarmes pour Amazon RDS.

Pour définir des alarmes à l'aide de la console CloudWatch

1. Connectez-vous à la AWS Management Console et ouvrez la console CloudWatch à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Choisissez Alarmes , puis Créer une alarme. Cela fait démarrer l'Assistant de création d'alarme.
3. Choisissez Métriques RDS et faites défiler les métriques Amazon RDS pour localiser la métrique sur laquelle vous voulez placer une alarme. Pour afficher uniquement des métriques Amazon RDS, recherchez l'identifiant de votre ressource. Sélectionnez la métrique sur laquelle créer une alarme, puis Suivant.
4. Saisissez les valeurs Nom, Description et Lorsque de la métrique.

5. Si vous souhaitez que CloudWatch vous envoie un e-mail lorsque l'état d'alarme est atteint, choisissez L'état est ALARME dans le champ Chaque fois que cette alarme. Pour Envoyer une notification à, sélectionnez une rubrique SNS existante. Si vous choisissez Créer une rubrique, vous pouvez définir le nom d'une nouvelle liste d'abonnement par e-mail et les adresses e-mail pour cette liste. La liste est enregistrée et s'affiche dans le champ des alarmes futures.

   Note

   Si vous utilisez Créer la rubrique pour créer une nouvelle rubrique Amazon SNS, les adresses e-mail doivent être vérifiées avant de pouvoir recevoir des notifications. Les e-mails sont envoyés uniquement lorsque l'alarme passe à un état défini. Si ce changement d'état de l'alarme se produit avant la vérification des adresses e-mail, ces dernières ne reçoivent pas de notification.

6. Prévisualisez l'alarme que vous êtes sur le point de créer dans la zone Aperçu de l'alarme, puis choisissez Créer une alarme.

Pour définir une alarme à l'aide de l'AWS CLI

- Appelez `put-metric-alarm`. Pour plus d'informations, consultez AWS CLI Command Reference.

Pour définir une alarme à l'aide de l'API CloudWatch

- Appelez `PutMetricAlarm`. Pour plus d'informations, consultez Amazon CloudWatch API Reference.

Publication des journaux du moteur de base de données dans Amazon CloudWatch Logs

Vous pouvez configurer votre moteur de base de données Amazon RDS de sorte à publier des données de journaux dans un groupe de journaux dans Amazon CloudWatch Logs. CloudWatch Logs vous permet d'effectuer une analyse en temps réel des données de journaux et d'utiliser CloudWatch pour créer des alarmes et afficher des métriques. Vous pouvez utiliser CloudWatch Logs pour stocker les enregistrements de vos journaux dans un stockage hautement durable, que vous pouvez gérer grâce à l'agent CloudWatch Logs. Par exemple, vous pouvez déterminer quand faire subir une rotation aux enregistrements de journaux d'un hôte vers le service de journal, de sorte à pouvoir accéder aux journaux bruts lorsque vous en avez besoin.

Pour accéder aux informations spécifiques à chaque moteur de base de données, consultez les rubriques suivantes :

- the section called “Publication des journaux MariaDB dans Amazon CloudWatch Logs” (p. 496)
- the section called “Publication des journaux MySQL dans CloudWatch Logs” (p. 509)
- the section called “Publication des journaux Oracle dans Amazon CloudWatch Logs” (p. 518)
- the section called “Publication de journaux PostgreSQL dans CloudWatch Logs” (p. 523)
- the section called “Publication de journaux SQL Server dans Amazon CloudWatch Logs” (p. 504)

Note

Avant d'activer la publication des données de journaux, assurez-vous que vous détenez un rôle lié au service dans AWS Identity and Access Management (IAM). Pour plus d'informations sur les rôles liés à un service, consultez Utilisation des rôles liés à un service pour Amazon RDS (p. 1606).

Configuration de l'intégration de journaux CloudWatch

Pour publier vos fichiers journaux de base de données dans CloudWatch Logs, choisissez les journaux à publier. Vous pouvez effectuer ce choix dans la section Paramètres avancés lorsque vous créez une instance de base de données. Vous pouvez également modifier une instance de base de données existante pour commencer la publication.

Une fois que vous avez activé la publication, Amazon RDS diffuse en continu tous les enregistrements de journaux d'instances de base de données dans un groupe de journaux. Par exemple, vous possédez un groupe de journaux `/aws/rds/instance/log type` pour chaque type de journaux que vous publiez. Ce groupe de journaux se trouve dans la même région AWS que l'instance de base de données qui génère le journal.

Après avoir publié les enregistrements de journaux, vous pouvez utiliser CloudWatch Logs pour rechercher et filtrer les enregistrements. Pour de plus amples informations sur la recherche et le filtrage des journaux, veuillez consulter Recherche et filtrage des données de journaux.

Affichage des métriques d'instances de base de données

Amazon RDS fournit des métriques permettant de vérifier l'état de vos instances de base de données. Vous pouvez contrôler les métriques des instances de base de données et les métriques du système d'exploitation.

Vous trouverez ci-dessous des détails sur l'affichage des métriques pour votre instance de base de données à l'aide de la console RDS et CloudWatch. Pour plus d'informations sur la surveillance des métriques du système d'exploitation de votre instance de base de données en temps réel à l'aide de CloudWatch Logs, consultez Surveillance améliorée (p. 394).

Affichage des métriques via la console

Pour afficher les métriques DB et du système d'exploitation d'une instance de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Activez le nom de l'instance de base de données pour laquelle vous souhaitez obtenir des informations afin d'afficher les détails.

4. Sélectionnez l'onglet Surveillance.
5. Pour Surveillance, choisissez l'option d'affichage des métriques parmi les options suivantes :
   - CloudWatch – Affiche un résumé des métriques de l'instance de base de données disponibles à partir de Amazon CloudWatch. Chaque métrique inclut un graphique affichant la métrique supervisée sur une période donnée.
   - Enhanced monitoring (Surveillance améliorée) – Affiche un résumé des métriques du système d'exploitation disponible pour une instance de base de données lorsque l'option de surveillance améliorée est activée. Chaque métrique inclut un graphique affichant la métrique supervisée sur une période donnée.
   - Liste de processus de SE – Affiche les détails de chaque processus s'exécutant dans l'instance sélectionnée.
   - Performance Insights – Ouvre la console Amazon RDS Performance Insights pour votre instance de base de données.

> **Tip**
>
> Pour choisir la plage de temps des métriques représentées par les graphiques, vous pouvez utiliser la liste de plages de temps.
> Vous pouvez choisir n'importe lequel des graphiques pour afficher une vue plus détaillée.
> Vous pouvez aussi appliquer aux données des filtres propres aux métriques.

Affichage des métriques d'instances de base de données avec l'API ou l'interface de ligne de commande

Amazon RDS s'intègre avec les métriques CloudWatch pour fournir un grand nombre de métriques d'instances de base de données. Vous pouvez afficher les métriques CloudWatch à l'aide de la console RDS, de l'AWS CLI ou de l'API.

Pour obtenir une liste complète des métriques Amazon RDS, accédez à Dimensions et métriques Amazon RDS dans le manuel Guide de l'utilisateur Amazon CloudWatch.

Affichage des métriques de base de données via l'interface ligne de commande CloudWatch

> **Note**
>
> L'exemple d'interface de ligne de commande nécessite les outils de ligne de commande CloudWatch. Pour plus d'informations sur CloudWatch et pour télécharger les outils de développement, consultez Amazon CloudWatch sur le site web AWS. Les valeurs `StartTime` et `EndTime` fournies dans cet exemple sont uniquement fournies à titre d'exemple. Remplacez-les par les valeurs adaptées à votre instance de base de données.

Pour afficher les statistiques d'utilisation et de performance pour une instance de base de données

- Utilisez la commande CloudWatch `mon-get-stats` avec les paramètres suivants.

```
PROMPT>mon-get-stats FreeStorageSpace --dimensions="DBInstanceIdentifier=mydbinstance"
 --statistics= Average
  --namespace="AWS/RDS" --start-time 2009-10-16T00:00:00 --end-time 2009-10-16T00:02:00
```

Affichage des métriques DB via l'API CloudWatch

Les valeurs `StartTime` et `EndTime` fournies dans cet exemple sont uniquement fournies à titre d'exemple. Remplacez-les par les valeurs adaptées à votre instance de base de données.

Pour afficher les statistiques d'utilisation et de performance pour une instance de base de données

- Appelez l'API CloudWatch `GetMetricStatistics` avec les paramètres suivants :
  - `Statistics.member.1` = `Average`
  - `Namespace` = `AWS/RDS`
  - `StartTime` = `2009-10-16T00:00:00`
  - `EndTime` = `2009-10-16T00:02:00`
  - `Period` = `60`
  - `MeasureName` = `FreeStorageSpace`

Statut d'instance de bases de données

Le statut d'une instance de base de données indique son état de santé. Vous pouvez afficher le statut d'une instance de base de données à l'aide de la console Amazon RDS, de la commande AWS CLI describe-db-instances ou de l'opération d'API DescribeDBInstances.

> **Note**
>
> Amazon RDS utilise également un autre statut appelé état de la maintenance, qui est affiché dans la colonne Maintenance de la console Amazon RDS. Cette valeur indique l'état de tout correctif de maintenance qui doit être appliqué à une instance de base de données. L'état de la maintenance est indépendant du statut de l'instance de base de données. Pour plus d'informations sur l'état de la maintenance, consultez Application des mises à jour pour une instance de base de données (p. 262).

Le tableau suivant répertorie les valeurs de statut possibles pour les instances de base de données. Il décrit également le mode de facturation correspondant à chaque statut. Il indique si vous serez facturé pour l'instance de base de données et son stockage, uniquement pour le stockage, ou si vous ne serez pas facturé. Pour tous les statuts d'instance de base de données, vous êtres toujours facturé pour l'utilisation de la sauvegarde.

Statut d'instance de bases	Facturé	Description
available	Facturé	L'instance de base de données est saine et disponible.
backing-up	Facturé	L'instance de base de données est en cours de sauvegarde.
backtracking	Facturé	Un retour sur trace est en cours pour l'instance de base de données. Ce statut s'applique uniquement à Aurora MySQL.
configuring-enhanced-monitoring	Facturé	La surveillance améliorée est en cours d'activation ou de désactivation pour cette instance de base de données.

Statut d'instance de bases	Facturé	Description
configuring-iam-database-auth	Facturé	L'authentification de base de données AWS Identity and Access Management (IAM) est en cours d'activation ou de désactivation pour cette instance de base de données.
configuring-log-exports	Facturé	La publication des fichiers journaux dans Amazon CloudWatch Logs est en cours d'activation ou de désactivation pour cette instance de base de données.
converting-to-vpc	Facturé	L'instance de base de données est en cours de conversion depuis une instance qui ne se trouve pas dans un Amazon Virtual Private Cloud (Amazon VPC) vers une instance qui est dans un Amazon VPC.
creating	Non facturé	L'instance de base de données est en cours de création. L'instance de base de données n'est pas accessible pendant sa création.
deleting	Non facturé	L'instance de base de données est en cours de suppression.
failed	Non facturé	L'instance de base de données a échoué et Amazon RDS ne peut pas la récupérer. Effectuez une restauration à un moment déterminé dans le temps jusqu'à l'heure de restauration la plus récente de l'instance de base de données pour récupérer les données.
inaccessible-encryption-credentials	Non facturé	Impossible d'accéder à la clé principale client (CMK) AWS KMS utilisée pour chiffrer ou déchiffrer l’instance de base de données.
incompatible-network	Non facturé	Amazon RDS tente d'effectuer une action de récupération sur une instance de base de données, mais n'y parvient pas, car l'état du VPC empêche l'exécution de l'action. Cette situation peut se produire si, par exemple, toutes les adresses IP disponibles d'un sous-réseau sont en cours d'utilisation et qu'Amazon RDS ne peut pas obtenir d'adresse IP pour l'instance de base de données.
incompatible-option-group	Facturé	Amazon RDS a tenté d'appliquer une modification du groupe d'options, mais n'y parvient pas, et Amazon RDS ne peut pas rétablir l'état antérieur du groupe options. Pour plus d'informations, consultez la liste Événements récents de l'instance de base de données. Cette situation peut se produire si, par exemple, le groupe d'options contient une option telle que TDE et que l'instance de base de données ne comporte pas d'informations chiffrées.
incompatible-parameters	Facturé	Amazon RDS ne peut pas démarrer l'instance de base de données, car les paramètres spécifiés dans le groupe de paramètres de base de données de l'instance ne sont pas compatibles avec l'instance. Annulez les modifications des paramètres ou rendez-les compatibles avec l'instance de base de données pour rétablir l'accès à votre instance. Pour en savoir plus sur les paramètres incompatibles, consultez la liste Événements récents correspondant à l'instance de base de données.
incompatible-restore	Non facturé	Amazon RDS ne peut pas effectuer de restauration à un instant donné. Parmi les causes courantes de cet état figurent l'utilisation des tables temporaires, des tables MyISAM avec MySQL ou des tables Aria avec MariaDB.

Statut d'instance de bases	Facturé	Description
maintenance	Facturé	Amazon RDS applique une mise à jour de maintenance à l'instance base de données. Cet état est utilisé pour la maintenance de niveau d'instance que RDS planifie suffisamment à l'avance.
modifying	Facturé	L'instance de base de données est en cours de modification en raison d'une demande du client de modification de l'instance.
moving-to-vpc	Facturé	L'instance de base de données est en cours de transfert vers un nouveau Amazon Virtual Private Cloud (Amazon VPC).
rebooting	Facturé	L'instance de base de données est en cours de redémarrage en raison d'une demande du client ou d'un processus Amazon RDS nécessitant le redémarrage de l'instance.
renaming	Facturé	L'instance de base de données est en cours de changement de nom en raison d'une demande du client pour la renommer.
resetting-master-credentials	Facturé	Les informations d'identification principales de l'instance de base de données sont en cours de réinitialisation en raison d'une demande du client pour les réinitialiser.
restore-error	Facturé	L'instance de base de données a rencontré une erreur lors de la restauration à un instant donné dans le passé ou à partir d'un instantané.
starting	Facturé pour stockage	L'instance de base de données démarre.
stopped	Facturé pour stockage	L'instance de base de données est arrêtée.
stopping	Facturé pour stockage	L'instance de base de données est en cours d'arrêt.
storage-full	Facturé	L'instance de base de données a atteint sa capacité de stockage allouée. Son statut est critique et nous vous recommandons de corriger ce problème immédiatement. Pour cela, mettez votre stockage à l'échelle en modifiant l'instance de base de données. Pour éviter cette situation, définissez les alarmes Amazon CloudWatch de manière à ce qu'elles vous préviennent lorsque l'espace de stockage devient faible.
optimisation du stockage	Facturé	Votre instance de base de données est modifiée afin de changer la taille ou le type de stockage. L'instance de base de données est entièrement opérationnelle. Toutefois, tant que l’état de votre instance de base de données est storage-optimization, vous ne pouvez pas demander de modification au niveau de son stockage. Le processus d'optimisation du stockage est généralement court mais peut parfois prendre jusqu'à 24 heures ou même davantage.
upgrading	Facturé	La version du moteur de base de données est en cours de mise à niveau.

Utilisation des recommandations Amazon RDS

Amazon RDS fournit des recommandations automatisées pour les ressources de base de données, telles que les instances de base de données, les les réplicas en lecture et les groupes de paramètres de de base de données. Ces recommandations fournissent des conseils quand aux bonnes pratiques en analysant la la configuration de l'instance de base de données, son utilisation et les données de performances.

Vous trouverez des exemples de ces recommandations dans le tableau suivant.

Type	Description	Recommandation	Informations supplémentaires
Version de moteur obsolète	Votre instance de base de données n'exécute pas la dernière version de moteur mineure.	Nous vous recommandons de mettre à niveau vers la dernière version, car celle-ci contient les correctifs de sécurité les plus récents et d'autres améliorations.	Mise à niveau d'une version du moteur d'une instance de base de données (p. 267)
Maintenance en attente disponible	Une maintenance en attente est disponible sur votre instance de base de données.	Nous vous recommandons d'effectuer la maintenance en attente disponible sur votre instance de base de données. Les mises à jour du système d'exploitation se produisent le plus souvent pour des raisons de sécurité et doivent être réalisées dès que possible.	Entretien d'une instance de base de données (p. 260)
Sauvegardes automatiques désactivées	Les sauvegardes automatisées sont désactivées sur votre instance de bases de données.	Nous recommandons d'activer les sauvegardes automatisées sur votre instance de base de données. Les sauvegardes automatiques garantissent une restauration à un instant dans le passé de votre instance de bases de données. Vous bénéficiez d'un stockage de sauvegarde pouvant aller jusqu'à la taille de stockage de votre instance de base de données sans frais supplémentaires.	Utilisation des sauvegardes (p. 317)
Volumes magnétiques utilisés	Votre instance de base de données utilise le stockage magnétique.	Le stockage magnétique n'est pas recommandé pour la plupart des instances de base de données. Nous vous recommandons de passer au stockage à usage général (SSD) ou au stockage IOPS provisionnés.	Stockage d'instance de base de données Amazon RDS (p. 30)
Plateforme EC2 Classic utilisée	Votre instance de base de données utilise la plateforme EC2-Classic héritée.	Nous vous recommandons de déplacer votre instance de base de données vers la plateforme EC2-VPC pour un meilleur contrôle d'accès réseau. Amazon VPC fournit un réseau virtuel qui est isolé de manière logique des autres réseaux virtuels du cloud AWS.	Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611)

Type	Description	Recommandation	Informations supplémentaires
Surveillance améliorée désactivée	Votre instance de base de données n'a pas la surveillance améliorée activée.	Nous recommandons d'activer la surveillance améliorée. La surveillance améliorée fournit des métriques de système d'exploitation en temps réel pour la surveillance et le dépannage.	Surveillance améliorée (p. 394)
Chiffrement désactivé	Votre instance de base de données n'a pas le chiffrement activé.	Nous vous recommandons d'activer le chiffrement. Vous pouvez chiffrer vos instances de base de données Amazon RDS existantes en effectuant la restauration à partir d'un instantané chiffré.	Chiffrement des ressources Amazon RDS (p. 1522)
Classe d'instance de base de données de la génération précédente utilisée	Votre instance de base de données s'exécute sur une classe d'instance de base de données d'une génération précédente.	Les classes d'instance de base de données d'une génération précédente ont été remplacées par des classes d'instances de base de données avec de meilleurs prix, de meilleures performances, ou les deux. Nous recommandons d'exécuter votre instance de base de données sur une classe d'instance de base de données de la génération suivante.	Classes d'instances de base de données (p. 6)
Non-utilisation des grandes pages pour une instance de base de données Oracle	Le paramètre `use_large_pages` n'est pas défini sur `ONLY` dans le groupe de paramètres de base de données utilisé par votre instance de base de données.	Pour une meilleure évolutivité des bases de données, nous vous recommandons d'affecter à `use_large_pages` la valeur `ONLY` dans le groupe de paramètres de base de données utilisé par votre instance de base de données.	Utilisation de HugePages avec une instance de base de données Oracle (p. 954)
Paramètres de mémoire personnalisés différents des paramètres par défaut	Votre groupe de paramètres de base de données définit des paramètres de mémoire qui divergent trop par rapport aux valeurs par défaut.	Les paramètres qui divergent trop par rapport aux valeurs par défaut peuvent entraîner des erreurs et des performances médiocres. Nous vous recommandons d'affecter aux paramètres de mémoire personnalisés leurs valeurs par défaut dans le groupe de paramètres de base de données utilisé par l'instance de base de données.	Utilisation de groupes de paramètres de base de données (p. 225)

Type	Description	Recommandation	Informations supplémentaires
Mise en mémoire tampon des modifications activée pour une instance de base de données MySQL	La mise en mémoire tampon des modifications de votre groupe de paramètres de base de données est activée.	La mise en mémoire tampon des modifications permet à une distance de base de données de reporter certaines opérations d'écriture nécessaires pour gérer les index secondaires. Cette configuration peut améliorer légèrement les performances, mais elle peut créer un retard important dans le cadre de la récupération sur incident. Au cours de la récupération sur incident, l'index secondaire doit être mis à jour. Ainsi, les avantages de la mise en mémoire tampon des modifications sont contrebalancés par les événements de récupération sur incident potentiellement très longs. Nous vous recommandons de désactiver la mise en mémoire tampon des modifications.	Best practices for configuring parameters for Amazon RDS for MySQL, part 1: Parameters related to performance dans AWS Database Blog
Cache de requête activé pour une instance de base de données MySQL	Le paramètre de cache de requête est activé pour votre groupe de paramètres de base de données.	En raison du cache de requête, l'instance de base de données peut sembler s'interrompre lorsque les modifications nécessitent la purge du cache. La plupart des charges de travail ne bénéficient pas d'un cache de requête. Le cache de requête a été supprimé de MySQL version 8.0. Nous vous recommandons de désactiver le paramètre de cache de requête.	Best practices for configuring parameters for Amazon RDS for MySQL, part 1: Parameters related to performance dans AWS Database Blog
Journalisation vers la table	Votre groupe de paramètres de base de données définit la sortie de journalisation vers `TABLE`.	La définition de la sortie le journalisation sur `TABLE` utilise plus de stockage que la définition de ce paramètre sur `FILE`. Pour éviter d'atteindre la limite de stockage, nous vous recommandons de définir le paramètre de sortie de journalisation sur `FILE`.	Fichiers journaux de base de données MySQL (p. 506)

Amazon RDS génère des recommandations pour une ressource lorsque cette ressource est crée ou modifiée. Amazon RDS analyse également périodiquement vos ressources et génère des recommandations.

Réponse aux recommandations Amazon RDS

Vous trouverez des recommandations dans la AWS Management Console. Vous pouvez réaliser l'action recommandée immédiatement, la programmer pour la fenêtre de maintenance suivante ou l'ignorer.

Pour répondre aux recommandations Amazon RDS

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.

2. Dans le volet de navigation, choisissez Recommandations.

La page Recommandations s'affiche.

3. Sur la page Recommandations, choisissez l'une des options suivantes :

   - Active – Affiche les recommandations en cours que vous pouvez appliquer, ignorer ou programmer.
   - Ignorée – Affiche les recommandations que vous avez ignorées. Si vous choisissez Ignorée, vous pouvez appliquer ces recommandations ignorées.
   - Planifiée – Affiche les recommandations que vous avez planifiées, mais pas encore appliquées. Ces recommandations seront appliquées au cours de la prochaine fenêtre de maintenance planifiée.
   - Appliquée – Affiche les recommandations que vous avez appliquées.

Dans toute liste de recommandations, vous pouvez ouvrir une section pour afficher les recommandations y figurant.

Pour configurer les préférences d'affichage des recommandations dans chaque section, choisissez l'icône Préférences.

Dans la fenêtre Préférences qui s'affiche, vous pouvez définir les options d'affichage. Ces options comprennent les colonnes visibles et le nombre de recommandations à afficher sur la page.

4. Gérer vos recommandations actives :

   a. Choisissez Active et ouvrez une ou plusieurs sections pour consulter les recommandations y figurant.

   b. Choisissez une ou plusieurs recommandations, puis choisissez Appliquer maintenant (pour les appliquer immédiatement), Programme (pour les appliquer dans la fenêtre de maintenance suivante) ou Ignorer.

      Si le bouton Appliquer maintenant apparaît pour une recommandation sans être disponible (grisé), c'est que l'instance de base de données n'est pas disponible. Vous pouvez appliquer les recommandations immédiatement uniquement si le statut de l'instance de base de données est disponible. Par exemple, vous ne pouvez pas appliquer les recommandations immédiatement à l'instance de base de données si son statut est modification. Dans ce cas, attendez que l'instance de base de données soit disponible, puis appliquez la recommandation.

Si le bouton Appliquer maintenant n'apparaît pas pour une recommandation, vous ne pouvez pas appliquer la recommandation en utilisant la page Recommandations. Vous pouvez modifier l'instance de base de données pour appliquer la recommandation manuellement.

Pour de plus amples informations sur la modification d'une instance de base de données, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

> **Note**
>
> Lorsque vous choisissez Appliquer maintenant, une brève interruption de l'instance de base de données peut s'ensuivre.

Surveillance améliorée

Amazon RDS fournit des métriques en temps réel pour le système d'exploitation sur lequel votre instance de base de données s'exécute. Vous pouvez afficher les métriques de votre instance de base de données à l'aide de la console. En outre, vous pouvez utiliser la sortie JSON de Monitoring Enhanced Amazon CloudWatch Logs dans un système de surveillance de votre choix.

Par défaut, les métriques de surveillance améliorée sont stockées pendant 30 jours dans le CloudWatch Logs ; elles sont différentes des métriques CloudWatch classiques. Pour modifier la durée de stockage des métriques dans CloudWatch Logs, modifiez la période de rétention pour le groupe de journaux `RDSOSMetrics` dans la console CloudWatch. Pour plus d'informations, consultez la section Modification de la rétention des données de journaux dans CloudWatch Logs du Amazon CloudWatch Logs User Guide.

Étant donné que les métriques de surveillance améliorée sont stockées dans les journaux CloudWatch au lieu de celles de Cloudwatch, le coût de la surveillance améliorée dépend de plusieurs facteurs :

- Vous ne payez que pour l'utilisation de la surveillance améliorée au-delà de l'offre gratuite fournie par Amazon CloudWatch Logs.

  Pour de plus amples informations sur la tarification, veuillez consulter Tarification Amazon CloudWatch.
- Plus l'intervalle de surveillance est court, plus la fréquence des rapports sur les métriques du système d'exploitation est élevée, ce qui augmente les coûts de surveillance.
- Les coûts d'utilisation de la surveillance améliorée sont appliqués pour chaque instance de base de données pour laquelle l'option est activée. Surveiller un grand nombre d'instances de bases de données est plus onéreux que de n'en surveiller que quelques unes.
- Les instances de bases de données qui prennent en charge une charge de travail nécessitant des calculs intensifs doivent signaler une activité de traitement du système d'exploitation plus intense et des coûts plus élevés pour la surveillance améliorée.

Disponibilité de la surveillance améliorée

La surveillance améliorée est disponible pour les moteurs de base de données suivants :

- MariaDB
- Microsoft SQL Server
- MySQL version 5.5 ou version ultérieure
- Oracle
- PostgreSQL

La surveillance améliorée est disponible pour toutes les classes d'instance de base de données, à l'exception de la classe d'instance db.m1.small.

Différences entre les métriques CloudWatch et de surveillance améliorée

CloudWatch recueille les métriques relatives à l'utilisation de l'UC à partir de l'hyperviseur pour une instance de base de données, et la surveillance améliorée recueille les métriques à partir d'un agent sur l'instance. Par conséquent, des différences de mesures peuvent apparaître, car une petite quantité de travail est effectuée par la couche de l'hyperviseur. Les différences peuvent être plus importantes si vos instances de bases de données utilisent des classes d'instance plus petites, car dans ce cas un plus grand nombre de machines virtuelles sont gérées par la couche de l'hyperviseur sur une même instance physique. Les métriques de la surveillance améliorée sont utiles pour évaluer l'utilisation de l'UC par différents processus ou threads sur une instance de base de données.

Configuration et activation de la surveillance améliorée

Pour utiliser la surveillance améliorée, vous devez créer un rôle IAM, puis activer la surveillance améliorée.

Avant de commencer

La surveillance améliorée nécessite votre autorisation afin d'agir en votre nom et envoyer des informations relatives aux métriques du système d'exploitation à CloudWatch Logs. Vous octroyez les autorisations requises sont octroyées à l'aide d'un rôle AWS Identity and Access Management (IAM).

La première fois que vous activez la surveillance améliorée dans la console, vous pouvez sélectionner l'option Par défaut pour la propriété Monitoring Role (Rôle de surveillance) afin que RDS crée le rôle IAM requis. RDS crée ensuite automatiquement en votre nom un rôle nommé `rds-monitoring-role` et l'utilise pour l'instance de base de données spécifiée ou le réplica en lecture.

Vous pouvez également créer le rôle requis avant d'activer la surveillance améliorée, puis spécifier le nom de votre nouveau rôle lorsque vous activez la surveillance améliorée. Vous devez créer ce rôle requis si vous activez la surveillance améliorée à l'aide de l'AWS CLI ou de l'API RDS.

Pour créer le rôle IAM approprié et permettre à Amazon RDS de communiquer avec le service Amazon CloudWatch Logs en votre nom, procédez comme suit.

L'utilisateur qui active la surveillance améliorée doit se voir accorder l'autorisation `PassRole`. Pour plus d'informations, consultez l'exemple 2 de la section Octroi d'autorisations à un utilisateur pour transférer un rôle à un service AWS dans le Guide de l'utilisateur IAM.

Pour créer un rôle IAM pour la surveillance améliorée Amazon RDS

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com.
2. Dans le panneau de navigation, choisissez Rôles.
3. Choisissez Créer un rôle.
4. Choisissez l'onglet Service AWS, puis choisissez RDS dans la liste de services.
5. Choisissez RDS - Surveillance améliorée, puis Suivant : Autorisations.
6. Vérifiez que la page Stratégie d'autorisations attachée indique AmazonRDSEnhancedMonitoringRole, puis choisissez Suivant : Balises.
7. Sur la page Add tags (Ajouter des balises), choisissez Next: Review (Suivant : Révision).
8. Dans le champ Nom du rôle, entrez un nom pour votre rôle, par exemple **`emaccess`**, puis choisissez Créer un rôle.

Activation et désactivation de la surveillance améliorée

Vous pouvez activer et désactiver la surveillance améliorée à l'aide d'AWS Management Console, de l'AWS CLI ou de l'API RDS.

Console

Vous pouvez activer la surveillance améliorée lorsque vous créez une instance de base de données ou un réplica en lecture, ou lorsque vous modifiez une instance de base de données. Si vous modifiez une instance de base de données afin d'activer la surveillance améliorée, vous n'avez pas besoin de redémarrer votre instance de base de données afin que la modification prenne effet.

Vous pouvez activer la surveillance améliorée dans la console RDS lorsque vous effectuez l'une des opérations suivantes :

- Créer une instances de base de données – Vous pouvez activer la surveillance améliorée dans la section Surveillance sous Additional configuration (Configuration supplémentaire).
- Créer un réplica en lecture – Vous pouvez activer la surveillance améliorée dans la section Surveillance.
- Modify a DB Instance (Modifier une instance de base de données) – Vous pouvez activer la surveillance améliorée dans la section Surveillance.

Pour activer la surveillance améliorée à l'aide de la console RDS, faites défiler jusqu'à la section Surveillance et procédez comme suit :

1. Choisissez Activer la surveillance améliorée pour votre instance de base de données ou le réplica en lecture.
2. Définissez la propriété Monitoring Role (Rôle de surveillance) sur le rôle IAM que vous avez créé pour autoriser Amazon RDS à communiquer avec Amazon CloudWatch Logs en votre nom ou choisissez Par défaut pour que RDS créé en votre nom un rôle nommé `rds-monitoring-role`.
3. Définissez la propriété Granularité sur l'intervalle, en secondes, entre les points lorsque les métriques sont collectées pour votre instance de base de données ou réplica en lecture. La propriété Granularité peut être définie sur l'une des valeurs suivantes : `1`, `5`, `10`, `15`, `30` ou `60`.

Pour désactiver la surveillance améliorée, choisissez Désactiver la surveillance améliorée.

L'activation de la surveillance améliorée ne nécessite pas le redémarrage de votre instance de base de données.

> **Note**
>
> La console RDS est actualisée toutes les 5 secondes. Si la granularité est définie sur 1 seconde dans la console RDS, les métriques mises à jour s'affichent toutes les 5 secondes uniquement. Vous pouvez récupérer les mises à jour des métriques toutes les secondes à l'aide de CloudWatch Logs.

AWS CLI

Pour activer la surveillance améliorée à l'aide de l'AWS CLI, dans les commandes suivantes, définissez l'option `--monitoring-interval` sur une valeur autre que `0` et définissez l'option `--monitoring-role-arn` sur le rôle que vous avez créé dans Avant de commencer (p. 395).

- create-db-instance
- create-db-instance-read-replica
- modify-db-instance

L'option `--monitoring-interval` spécifie l'intervalle, en secondes, entre les points lorsque des métriques de surveillance améliorée sont collectées. Les valeurs valides pour l'option sont `0`, `1`, `5`, `10`, `15`, `30` et `60`.

Pour désactiver la surveillance améliorée à l'aide de l'AWS CLI, définissez l'option `--monitoring-interval` sur `0` dans ces commandes.

Example

L'exemple suivant active la surveillance améliorée pour une instance de base de données :

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --monitoring-interval 30 \
    --monitoring-role-arn arn:aws:iam::123456789012:role/emaccess
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --monitoring-interval 30 ^
    --monitoring-role-arn arn:aws:iam::123456789012:role/emaccess
```

API RDS

Pour activer la surveillance améliorée à l'aide de l'API RDS, dans les opérations suivantes, définissez le paramètre `MonitoringInterval` sur une valeur autre que `0` et définissez le paramètre `MonitoringRoleArn` sur le rôle que vous avez créé dans Avant de commencer (p. 395).

- CreateDBInstance
- CreateDBInstanceReadReplica
- ModifyDBInstance

Le paramètre `MonitoringInterval` spécifie l'intervalle, en secondes, entre les points lorsque des métriques de surveillance améliorée sont collectées. Les valeurs valides pour le paramètre sont `0`, `1`, `5`, `10`, `15`, `30` et `60`.

Pour désactiver la surveillance améliorée à l'aide de l'API RDS, définissez le paramètre `MonitoringInterval` sur `0` dans ces opérations.

Affichage de la surveillance améliorée

Vous pouvez afficher les métriques du système d'exploitation relevées par la surveillance améliorée dans la console RDS en choisissant Enhanced monitoring (Surveillance améliorée) pour Monitoring (Surveillance).

La page Enhanced Monitoring (Surveillance améliorée) est illustrée ci-après.

Certaines instances de base de données utilisent plusieurs disques pour le volume de stockage des données de l'instance de base de données. Sur ces instances de base de données, les graphiques Physical Devices (Appareils physiques) montrent les métriques de chacun des disques. Par exemple, le graphique suivant montre les métriques pour quatre disques.

Note

Actuellement, les graphiques Physical Devices (Appareils physiques) ne sont pas disponibles pour les instances de base de données Microsoft SQL Server.

Lorsque vous consultez les graphiques agrégés E/S de disque et Système de fichiers, l'appareil rdsdev se rapporte au système de fichiers `/rdsdbdata`, dans lequel tous les journaux et les fichiers de base de données sont stockés. L'appareil filesystem se rapporte au système de fichiers `/` (également appelé système de fichiers racine), dans lequel les fichiers associés au système d'exploitation sont stockés.

Si l'instance de base de données est un déploiement multi-AZ, vous pouvez afficher les métriques de système d'exploitation pour l'instance de base de données principale et son réplica de secours multi-AZ. Dans la vue Enhanced monitoring (Surveillance améliorée), choisissez primary (principal) pour afficher les métriques de système d'exploitation pour l'instance de base de données principale, ou choisissez secondary (secondaire) pour afficher les métriques de système d'exploitation pour le réplica de secours.

Pour plus d'informations sur les déploiements multi-AZ, consultez Haute disponibilité (multi-AZ) pour Amazon RDS (p. 43).

> **Note**
>
> Actuellement, l'affichage des métriques de systèmes d'exploitation pour un réplica de secours multi-AZ n'est pas pris en charge pour les instances de base de données MariaDB ou Microsoft SQL Server.

Si vous voulez afficher des détails sur les processus qui s'exécutent sur votre instance de base de données, choisissez Liste de processus de système d'exploitation pour Surveillance.

La vue Liste des processus est affichée ci-dessous.

Les métriques de surveillance améliorée affichées dans la vue Liste des processus sont organisées de la manière suivante :

- RDS child processes (Processus enfants RDS) – Affiche un résumé des processus RDS prenant en charge l'instance de base de données, par exemple `mysqld` pour les instances de base de données MySQL. Les threads du processus sont imbriqués sous le processus parent. Les threads du processus affichent uniquement l'utilisation de l'UC, car les autres métriques sont identiques pour tous les threads du processus. La console affiche 100 processus et threads maximum. Les résultats représentent une combinaison des principaux processus et threads de la consommation de l'UC et de la mémoire. S'il existe plus de 50 processus et 50 threads, la console affiche les 50 premiers éléments de chaque catégorie. Cette présentation vous aide à identifier les processus ayant le plus d'impact sur les performances.
- RDS processes (Processus RDS) – Affiche un récapitulatif des ressources utilisées par l'agent de gestion RDS, les processus de surveillance des diagnostics, et d'autres processus AWS nécessaires pour prendre en charge les instances de base de données RDS.
- OS processes (Processus SE) – Affiche un récapitulatif des processus du noyau et du système, qui ont généralement un faible impact sur les performances.

Les éléments répertoriés pour chaque processus sont les suivants :

- VIRT – Affiche la taille virtuelle du processus.
- RES – Affiche la mémoire physique réelle en cours d'utilisation par le processus.
- UC% – Affiche le pourcentage de la bande passante totale de l'UC utilisé par le processus.
- MEM% – Affiche le pourcentage de mémoire totale utilisé par le processus.

Les données de surveillance affichées dans la console RDS sont extraites d'Amazon CloudWatch Logs. Vous pouvez également extraire les métriques pour une instance de base de données sous forme de flux de journal à partir de CloudWatch Logs. Pour plus d'informations, consultez Affichage de la surveillance améliorée à l'aide de CloudWatch Logs (p. 401).

Les métriques de surveillance améliorée ne sont pas renvoyées dans les situations suivantes :

- Basculement de l'instance de base de données.
- Modification de la classe d'instance de l'instance de base de données (dimensionnement du calcul).

Les métriques de surveillance améliorée sont renvoyées pendant le redémarrage d'une instance de base de données car seul le moteur de base de données est redémarré. Les métriques concernant le système d'exploitation continuent d'être relevées.

Affichage de la surveillance améliorée à l'aide de CloudWatch Logs

Après avoir activé la surveillance améliorée pour votre instance de base de données, vous pouvez afficher les métriques pour votre instance de base de données à l'aide de CloudWatch Logs, chaque flux de journal représentant une seule instance de base de données surveillée. L'identifiant du flux de journal est l'identifiant de la ressource (`DbiResourceId`) de l'instance de base de données

Pour afficher les données du journal de la surveillance améliorée

1. Ouvrez la console CloudWatch à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Si besoin, choisissez la région dans laquelle se situe votre instance de base de données. Pour en savoir plus, consultez la section relative aux régions et points de terminaison du document Référence générale Amazon Web Services.
3. Choisissez Logs (Journaux) dans le volet de navigation.
4. Choisissez RDSOSMetrics dans la liste de groupes de journaux.

   Dans un déploiement multi-AZ, les fichiers journaux avec `-secondary` ajouté au nom correspondent au réplica de secours multi-AZ.

5. Choisissez le flux de journal à afficher dans la liste des flux de journaux.

Métriques du système d'exploitation disponibles

Les tableaux suivants répertorient les métriques du système d'exploitation disponibles à l'aide d'Amazon CloudWatch Logs.

Métriques pour les instances de bases de données MariaDB, MySQL, Oracle et PostgreSQL

Groupe	Métrique	Nom de la console	Description
`General`	`engine`	Non applicable	Moteur de base de données de l'instance de base de données.

Groupe	Métrique	Nom de la console	Description
	`instanceID`	Non applicable	Identifiant de l'instance de base de données.
	`instanceResourceID`	Non applicable	Identificateur immuable pour l'instance de base de données propre à une région AWS, également utilisé en tant qu'identifiant du flux de journal.
	`numVCPUs`	Non applicable	Nombre d'UC virtuelles de l'instance de base de données.
	`timestamp`	Non applicable	Heure à laquelle la métrique a été évaluée.
	`uptime`	Non applicable	Temps d'activité de l'instance de base de données.
	`version`	Non applicable	Version du format JSON du flux des métriques du système d'exploitation.
`cpuUtilization`	`guest`	Invité UC	Pourcentage de l'UC en cours d'utilisation par les programmes invités.
	`idle`	Inactivité de l'UC	Pourcentage de l'UC inactive.
	`irq`	IRQ UC	Pourcentage de l'UC en cours d'utilisation par les interruptions logicielles.
	`nice`	UC Nice	Pourcentage de l'UC en cours d'utilisation par des programmes s'exécutant avec la priorité la plus faible.
	`steal`	UC Steal	Pourcentage de l'UC en cours d'utilisation par d'autres machines virtuelles.
	`system`	Système UC	Pourcentage de l'UC en cours d'utilisation par le noyau.
	`total`	Total UC	Pourcentage total de l'UC en cours d'utilisation. Cette valeur inclut la valeur `nice`.
	`user`	Utilisateur UC	Pourcentage de l'UC en cours d'utilisation par des programmes utilisateurs.
	`wait`	Attente du processeur	Pourcentage de l'UC non utilisée pendant l'attente pour accéder aux E/S.
`diskIO`	`avgQueueLen`	Taille moyenne de la file d'attente	Nombre de requêtes en attente dans la file d'attente du périphérique d'E/S.
	`avgReqSz`	Taille moyenne de la demande	Taille moyenne de requête, en kilo-octets.
	`await`	E/S disque en attente	Nombre de millisecondes requises pour répondre aux requêtes, y compris le temps d'attente et le temps de service.

Groupe	Métrique	Nom de la console	Description
	`device`	Non applicable	Identifiant du périphérique de disque en cours d'utilisation.
	`diskQueueDepth`	Profondeur de la file d'attente de disque	Nombre de demandes d'entrée et de sortie (E/S) en attente pour accéder au disque.
	`readIOsPS`	E/S lecture	Nombre d'opérations de lecture par seconde.
	`readKb`	Total lecture	Nombre total de kilo-octets lus.
	`readKbPS`	Ko/s lecture	Nombre de kilo-octets lus par seconde.
	`readLatency`	Latence de lecture	Temps écoulé entre l'envoi d'une requête d'E/S de lecture et sa fin, en millisecondes. Cette métrique est uniquement disponible pour Amazon Aurora.
	`readThroughput`	Débit de lecture	Quantité de débit réseau utilisée par les demandes adressées au cluster DB, en octets par seconde. Cette métrique est uniquement disponible pour Amazon Aurora.
	`rrqmPS`	Rrqms	Nombre de requêtes de lecture fusionnées mises en file d'attente par seconde.
	`tps`	TPS	Nombre de transactions d'E/S par seconde.
	`util`	Util E/S disque	Pourcentage de temps UC pendant lequel les requêtes ont été émises.
	`writeIOsPS`	E/S écriture	Nombre d'opérations d'écriture par seconde.
	`writeKb`	Total écriture	Nombre total de kilo-octets écrits.
	`writeKbPS`	Ko/s écriture	Nombre de kilo-octets écrits par seconde.
	`writeLatency`	Latence en écriture	Temps moyen écoulé entre l'envoi d'une requête d'E/S d'écriture et sa fin, en millisecondes. Cette métrique est uniquement disponible pour Amazon Aurora.
	`writeThroughput`	Débit d'écriture	Quantité de débit réseau utilisée par les réponses du cluster DB, en octets par seconde. Cette métrique est uniquement disponible pour Amazon Aurora.
	`wrqmPS`	Wrqms	Nombre de requêtes d'écriture fusionnées mises en file d'attente par seconde.

Groupe	Métrique	Nom de la console	Description
`physicalDevices`	`avgQueueLen`	Taille moyenne de la file d'attente pour les périphériques physiques	Nombre de requêtes en attente dans la file d'attente du périphérique d'E/S.
	`avgReqSz`	Taille moyenne de la demande pour les périphériques physiques	Taille moyenne de requête, en kilo-octets.
	`await`	E/S disque en attente pour les périphériques physiques	Nombre de millisecondes requises pour répondre aux requêtes, y compris le temps d'attente et le temps de service.
	`device`	Non applicable	Identifiant du périphérique de disque en cours d'utilisation.
	`readIOsPS`	E/S lecture pour périphériques physiques	Nombre d'opérations de lecture par seconde.
	`readKb`	Nombre total de lecture pour les périphériques physiques	Nombre total de kilo-octets lus.
	`readKbPS`	Lecture ko/s pour les périphériques physiques	Nombre de kilo-octets lus par seconde.
	`rrqmPS`	Rrqms pour les périphériques physiques	Nombre de requêtes de lecture fusionnées mises en file d'attente par seconde.
	`tps`	TPS pour les périphériques physiques	Nombre de transactions d'E/S par seconde.
	`util`	Util. d'E/S de disque pour les périphériques physiques	Pourcentage de temps UC pendant lequel les requêtes ont été émises.

Groupe	Métrique	Nom de la console	Description
	`writeIOsPS`	Périphériques physiques en écriture IO/s	Nombre d'opérations d'écriture par seconde.
	`writeKb`	Nombre total d'écritures pour les périphériques physiques	Nombre total de kilo-octets écrits.
	`writeKbPS`	Écriture ko/s pour les périphériques physiques	Nombre de kilo-octets écrits par seconde.
	`wrqmPS`	Wrqms pour les périphériques physiques	Nombre de requêtes d'écriture fusionnées mises en file d'attente par seconde.
`fileSys`	`maxFiles`	Nombre maximum d'inodes	Nombre maximum de fichiers pouvant être créés pour le système de fichiers.
	`mountPoint`	Non applicable	Chemin vers le système de fichiers.
	`name`	Non applicable	Nom du système de fichiers.
	`total`	Total système de fichiers	Quantité totale d'espace disque disponible pour le système de fichiers, en kilo-octets.
	`used`	Système de fichiers utilisé	Quantité d'espace disque utilisé par des fichiers du système de fichiers, en kilo-octets.
	`usedFilePercent`	% utilisé	Pourcentage de fichiers disponibles en cours d'utilisation.
	`usedFiles`	Inodes utilisés	Nombre de fichiers dans le système de fichiers.
	`usedPercent`	% d'inodes utilisés	Pourcentage d'espace de disque du système de fichiers en cours d'utilisation.
`loadAverageMinute`	`fifteen`	Charge moyenne 15 min	Nombre de processus demandant du temps UC au cours des 15 dernières minutes.
	`five`	Charge moyenne 5 min	Nombre de processus demandant du temps UC au cours des 5 dernières minutes.

Groupe	Métrique	Nom de la console	Description
	`one`	Charge moyenne 1 min	Nombre de processus demandant du temps UC au cours de la dernière minute.
`memory`	`active`	Mémoire active	Quantité de mémoire attribuée, en kilo-octets.
	`buffers`	Mémoire mise en tampon	Quantité de mémoire utilisée pour la mise en mémoire tampon des demandes E/S avant écriture dans le périphérique de stockage, en kilo-octets.
	`cached`	Mémoire mise en cache	Quantité de mémoire utilisée pour la mise en cache d'E/S basés sur le système de fichiers.
	`dirty`	Mémoire corrompue	Quantité de pages mémoire de la RAM ayant été modifiées mais non écrites dans le bloc de données associé dans le stockage, en kilo-octets.
	`free`	Mémoire libre	Quantité de mémoire non attribuée, en kilo-octets.
	`hugePagesFree`	Grandes pages gratuites	Nombre de grandes pages gratuites. Les grandes pages sont une fonction du noyau Linux.
	`hugePagesRsvd`	Grandes pages Rsvd	Nombre de grandes pages dédiées.
	`hugePagesSize`	Taille des grandes pages	Taille de chaque unité de grandes pages, en kilo-octets.
	`hugePagesSurp`	Grandes pages excéd	Nombre de grandes pages excédentaires disponibles par rapport au nombre total.
	`hugePagesTotal`	Total de grandes pages	Le nombre total de grandes pages.
	`inactive`	Mémoire inactive	Quantité de pages mémoire moins fréquemment utilisées, en kilo-octets.
	`mapped`	Mémoire mappée	Quantité totale de contenu du système de fichiers mappé en mémoire dans un espace d'adressage de processus, en kilo-octets.
	`pageTables`	Tables de pages	Quantité de mémoire utilisée par les tables de page, en kilo-octets.
	`slab`	Mémoire de section	Quantité de structures de données noyau réutilisables, en kilo-octets.
	`total`	Mémoire totale	Quantité totale de mémoire, en kilo-octets.

Groupe	Métrique	Nom de la console	Description
	`writeback`	Mémoire en écriture différée	Quantité de pages de modification dans la RAM encore écrites dans le stockage de sauvegarde, en kilo-octets.
`network`	`interface`	Non applicable	Identifiant pour l'interface réseau utilisée pour l'instance de base de données.
	`rx`	RX	Nombre d'octets reçus par seconde.
	`tx`	TX	Nombre d'octets téléchargés par seconde.
`processList`	`cpuUsedPc`	% UC	Pourcentage de l'UC utilisé par le processus.
	`id`	Non applicable	Identifiant du processus.
	`memoryUsedPc`	% MEM	Quantité de mémoire utilisée par le processus, en kilo-octets.
	`name`	Non applicable	Nom du processus.
	`parentID`	Non applicable	Identifiant de processus pour le processus parent du processus.
	`rss`	RES	Quantité de RAM allouée au processus, en kilo-octets.
	`tgid`	Non applicable	Identifiant du groupe de threads. Numéro représentant l'ID du processus auquel appartient le thread. Cet identifiant permet de regrouper les threads d'un même processus.
	`VIRT`	VIRT	Quantité de mémoire virtuelle allouée au processus, en kilo-octets.
`swap`	`swap`	Swap	Quantité de mémoire d'échange disponible, en kilo-octets.
	`swap in`	Swaps dans	Quantité de mémoire, en kilo-octets, échangée depuis le disque.
	`swap out`	Swaps vers	Quantité de mémoire, en kilo-octets, échangée vers le disque.
	`free`	Swap libre	Quantité de mémoire d'échange libre, en kilo-octets.
	`committed`	Swap validé	Quantité de mémoire d'échange, en kilo-octets, utilisée en tant que mémoire cache.
`tasks`	`blocked`	Tâches bloquées	Nombre de tâches bloquées.
	`running`	Tâches en cours d'exécution	Nombre de tâches en cours d'exécution.
	`sleeping`	Tâches en veille	Nombre de tâches en veille.

Groupe	Métrique	Nom de la console	Description
	`stopped`	Tâches arrêtées	Nombre de tâches arrêtées.
	`total`	Total de tâches	Nombre total de tâches.
	`zombie`	Tâches zombies	Nombre de tâches enfant inactives avec une tâche parent active.

Métriques pour les instances de bases de données Microsoft SQL Server

Groupe	Métrique	Nom de la console	Description
`General`	`engine`	Non applicable	Moteur de base de données de l'instance de base de données.
	`instanceID`	Non applicable	Identifiant de l'instance de base de données.
	`instanceResourceID`	Non applicable	Identificateur immuable pour l'instance de base de données propre à une région AWS, également utilisé en tant qu'identifiant du flux de journal.
	`numVCPUs`	Non applicable	Nombre d'UC virtuelles de l'instance de base de données.
	`timestamp`	Non applicable	Heure à laquelle la métrique a été évaluée.
	`uptime`	Non applicable	Temps d'activité de l'instance de base de données.
	`version`	Non applicable	Version du format JSON du flux des métriques du système d'exploitation.
`cpuUtilization`	`idle`	Inactivité de l'UC	Pourcentage de l'UC inactive.
	`kern`	Noyau UC	Pourcentage de l'UC en cours d'utilisation par le noyau.
	`user`	Utilisateur UC	Pourcentage de l'UC en cours d'utilisation par des programmes utilisateurs.
`disks`	`name`	Non applicable	Identifiant du disque.
	`totalKb`	Espace disque total	Espace total du disque, en kilo-octets.
	`usedKb`	Espace disque utilisé	Quantité d'espace utilisé sur le disque, en kilo-octets.
	`usedPc`	% d'espace disque utilisé	Pourcentage d'espace utilisé sur le disque.
	`availKb`	Espace disque disponible	Espace disponible sur le disque, en kilo-octets.

Groupe	Métrique	Nom de la console	Description
	`availPc`	% d'espace disque disponible	Pourcentage d'espace disponible sur le disque.
	`rdCountPS`	Lectures/s	Nombre d'opérations de lecture par seconde.
	`rdBytesPS`	Ko/s lecture	Nombre d'octets lus par seconde.
	`wrCountPS`	E/S écriture	Nombre d'opérations d'écriture par seconde.
	`wrBytesPS`	Ko/s écriture	Nombre d'octets écrits par seconde.
`memory`	`commitTotKb`	Total de validation	Quantité d'espace d'adressage virtuel en cours d'utilisation basé sur le fichier d'échange, c'est-à-dire la charge d'écriture actuelle. Cette valeur est composée de la mémoire principale (RAM) et du disque (fichiers d'échange).
	`commitLimitKb`	Validation maximale	Valeur maximum acceptée pour la métrique `commitTotKb`. Cette valeur est la somme de la taille du fichier d'échange actuel et de la mémoire physique disponible pour le contenu paginable, à l'exclusion de la RAM affectée aux zones non paginables.
	`commitPeakKb`	Pic de validation	Plus grande valeur de la métrique `commitTotKb` depuis le dernier démarrage du système d'exploitation.
	`kernTotKb`	Mémoire totale du noyau	Quantité de mémoire dans les groupes de noyaux paginés et non paginés, en kilo-octets.
	`kernPagedKb`	Mémoire du noyau paginée	Quantité de mémoire dans le groupe de noyaux paginés, en kilo-octets.
	`kernNonpagedKb`	Mémoire du noyau non paginée	Quantité de mémoire dans le groupe de noyaux non paginés, en kilo-octets.
	`pageSize`	Taille de page	Taille d'une page, en octets.
	`physTotKb`	Mémoire totale	Quantité de mémoire physique, en kilo-octets.
	`physAvailKb`	Mémoire disponible	Quantité de mémoire physique disponible, en kilo-octets.
	`sqlServerTotKb`	Mémoire totale SQL Server	Quantité de mémoire dédiée à SQL Server, en kilo-octets.
	`sysCacheKb`	Cache système	Quantité de mémoire cache du système, en kilo-octets.
`network`	`interface`	Non applicable	Identifiant pour l'interface réseau utilisée pour l'instance de base de données.
	`rdBytesPS`	Lecture réseau Ko/s	Nombre d'octets reçus par seconde.

Groupe	Métrique	Nom de la console	Description
	`wrBytesPS`	Écriture réseau Ko/s	Nombre d'octets envoyés par seconde.
`processList`	`cpuUsedPc`	% utilisé	Pourcentage de l'UC utilisé par le processus.
	`memUsedPc`	% MEM	Pourcentage de mémoire totale utilisé par le processus.
	`name`	Non applicable	Nom du processus.
	`pid`	Non applicable	Identifiant du processus. Cette valeur n'est pas présente pour les processus appartenant à Amazon RDS.
	`ppid`	Non applicable	Identifiant de processus pour le parent de ce processus. Cette valeur est uniquement présente pour les processus enfant.
	`tid`	Non applicable	Identifiant du thread. Cette valeur est uniquement présente pour les threads. Le processus propriétaire peut être identifié à l'aide de la valeur `pid`.
	`workingSetKb`	Non applicable	Quantité de mémoire dans l'ensemble de travail privé, plus la quantité de mémoire en cours d'utilisation par le processus et pouvant être partagée avec d'autres processus, en kilo-octets.
	`workingSetPrivKb`	Non applicable	Quantité de mémoire en cours d'utilisation par un processus, mais ne pouvant pas être partagée avec d'autres processus, en kilo-octets.
	`workingSetShareableKb`	Non applicable	Quantité de mémoire en cours d'utilisation par un processus et pouvant être partagée avec d'autres processus, en kilo-octets.
	`virtKb`	Non applicable	Quantité d'espace d'adressage virtuel utilisé par le processus, in kilobytes. L'utilisation d'un espace d'adressage virtuel n'implique pas forcément l'utilisation correspondante de disque ou de pages de mémoire principale.
`system`	`handles`	Poignées	Nombre de handles utilisés par le système.
	`processes`	Processus	Nombre de processus s'exécutant sur le système.
	`threads`	Threads	Nombre de threads s'exécutant sur le système.

Utilisation d'Amazon RDS Performance Insights

Performance Insights complète les fonctions de surveillance existantes d'Amazon RDS. Ce service illustre les performances de votre base de données et facilite votre analyse des problèmes qui les impactent. Grâce au tableau de bord de Performance Insights, vous pouvez visualiser la charge de la base de données et la filtrer par attentes, instructions SQL, hôtes ou utilisateurs.

Rubriques

- Présentation de Performance Insights (p. 411)
- Activation et désactivation de Performance Insights (p. 413)
- Accès à Performance Insights (p. 418)
- Surveillance avec le tableau de bord de Performance Insights (p. 419)
- Personnalisation du tableau de bord de Performance Insights (p. 440)
- Récupération de données avec l'API Performance Insights (p. 451)
- Métriques Performance Insights publiées dans Amazon CloudWatch (p. 464)
- Journalisation des appels d'Analyse des performances à l'aide d'AWS CloudTrail (p. 465)

Présentation de Performance Insights

Par défaut, Performance Insights est activé dans l'assistant de création de console pour les moteurs Amazon RDS. Si vous disposez de plusieurs bases de données sur une instance de base de données, Performance Insights regroupe les données de performance.

Rubriques

- Charge de la base de données (p. 411)
- Utilisation maximale de l'UC (p. 412)
- Moteurs de base de données pris en charge pour Performance Insights (p. 412)

Charge de la base de données

La métrique centrale de Performance Insights est `DB Load`. La charge de la base de données représente le nombre moyen de sessions actives (AAS) pour le moteur de base de données. Une session active est une connexion qui a transmis du travail au moteur de base de données et qui attend une réponse. Par exemple, si vous envoyez une requête SQL au moteur de base de données, la session de base de données est active pendant que le moteur traite cette requête. La métrique `DB Load` est collectée toutes les secondes.

La métrique `DB Load` comporte des sous-composants appelés dimensions. Vous pouvez considérer les dimensions comme des catégories pour les différentes caractéristiques de la métrique `DB Load`. Lorsque vous diagnostiquez des problèmes de performances, les dimensions les plus utiles sont les événements d'attente et les principaux éléments SQL.

Événements d'attente

Un événement d'attente fait qu'une instruction SQL attend qu'un événement spécifique se produise avant de pouvoir continuer à s'exécuter. Par exemple, une exécution d'instruction SQL peut attendre jusqu'à ce qu'une ressource verrouillée soit déverrouillée. En combinant `DB Load` avec des événements d'attente, vous pouvez obtenir une image complète de l'état de la session. Les événements d'attente varient en fonction du moteur de base de données :

- Pour de plus amples informations sur tous les événements d'attente MariaDB et MySQL, veuillez consulter Wait Event Summary Tables dans la documentation MySQL.
- Pour plus d'informations sur tous les événements d'attente PostgreSQL, consultez les Tableaux des événements d'attente PostgreSQL dans la documentation PostgreSQL.
- Pour de plus amples informations sur tous les événements d'attente Oracle, veuillez consulter Descriptions of Wait Events dans la documentation Oracle.
- Pour de plus amples informations sur tous les événements d'attente SQL Server, veuillez consulter Types of Waits dans la documentation SQL Server.

Note

Pour Oracle, les processus en arrière-plan s'exécutent parfois sans instruction SQL associée. Dans ce cas, Performance Insights communique le type de processus en arrière-plan concaténé avec le signe deux-points, et la classe d'attente associée à ce processus en arrière-plan. Les types de processus en arrière-plan incluent LGWR, ARC0, PMON, etc.
Par exemple, lorsque le programme d'archivage effectue des opérations d'E/S, le rapport Performance Insights correspondant est similaire à `ARC1:System I/O`. Parfois, le type du processus en arrière-plan est également omis et Performance Insights communique uniquement la classe d'attente, par exemple `:System I/O`.

Principaux éléments SQL

Alors que les événements d'attente présentent des goulots d'étranglement, le principaux éléments SQL indiquent quelles requêtes contribuent le plus à la charge de la base de données. Par exemple, de nombreuses requêtes peuvent être en cours d'exécution sur la base de données, mais une seule d'entre elles peut consommer 99 % de la charge de la base de données. Dans ce cas, la charge élevée peut indiquer un problème avec la requête.

Par défaut, la console Performance Insights affiche les principales requêtes SQL qui contribuent à la charge de la base de données. La console affiche également des statistiques pertinentes pour chaque instruction. Pour diagnostiquer les problèmes de performances d'une instruction spécifique, vous pouvez examiner son plan d'exécution.

Utilisation maximale de l'UC

Dans le tableau de bord, le graphique Database load (Charge de base de données) collecte, regroupe et affiche les informations de session. Pour voir si les sessions actives dépassent l'utilisation maximale de l'UC, examinez leur relation sur la ligne Max vCPU (UC virtuelle max). La valeur de Max vCPU (UC virtuelle max) est déterminée par le nombre de cœurs de vCPU (UC virtuelle) pour votre instance de base de données.

Si la charge est souvent au-dessus de la ligne Max vCPU (UC virtuelle max) et que l'état d'attente principal est CPU, cela signifie que l'UC système est surchargée. Dans ce cas, vous pouvez décider de limiter les connexions à l'instance, d'ajuster les requêtes SQL avec une charge d'UC élevée, ou envisager l'utilisation d'une classe d'instance plus grande. Quel que soit leur état d'attente, les instances élevées et régulières indiquent que des problèmes de goulots d'étranglement ou de conflits de ressources devront peut-être être résolus. Cela peut être le cas même si la charge ne dépasse pas la ligne Max vCPU (UC virtuelle max).

La vidéo suivante présente Performance Insights.

Utilisation de Performance Insights pour analyser les performances de Amazon Aurora PostgreSQL

Moteurs de base de données pris en charge pour Performance Insights

Vous trouverez ci-après les moteurs de base de données qui prennent en charge Performance Insights.

Moteur de base de données	Versions de moteur de base de données prises en charge
Amazon Aurora avec compatibilité MySQL	Versions 2.04.2 et 2.x ultérieures (compatibles avec MySQL 5.7), et versions 1.17.3 et 1.x ultérieures (compatibles avec MySQL 5.6). Non pris en charge sur les classes d'instance de base de données db.t2 ou db.t3. Pour les clusters de base de données activés pour la requête parallèle, les versions minimales d'Aurora MySQL sont 2.09.0 et 1.23.0.

Moteur de base de données	Versions de moteur de base de données prises en charge
Amazon Aurora avec compatibilité PostgreSQL	Toutes les versions.
Amazon RDS for MariaDB	Versions 10.4.8 et 10.4 ultérieures, versions 10.3.13 et 10.3 ultérieures et versions 10.2.21 et 10.2 ultérieures. Non pris en charge pour MariaDB version 10.0 ou 10.1. Non pris en charge pour les instances de base de données MariaDB version 10.3.13 dans les régions AWS Europe (Francfort) et Europe (Stockholm). Non pris en charge sur les classes d'instance de base de données suivantes : db.t2.micro, db.t2.small, db.t3.micro, et db.t3.small.
Amazon RDS pour MySQL	Versions 8.0.17 et 8.0 ultérieures, versions 5.7.22 et 5.7 ultérieures, et versions 5.6.41 et 5.6 ultérieures. Non pris en charge pour la version 5.5. Non pris en charge sur les classes d'instance de base de données suivantes : db.t2.micro, db.t2.small, db.t3.micro, et db.t3.small.
Amazon RDS pour Microsoft SQL Server	Toutes les versions à l'exception de SQL Server 2008.
Amazon RDS pour PostgreSQL	Versions 10, 11 et 12.
Amazon RDS pour Oracle	Toutes les versions.

Note

L'Analyse des performances Amazon RDS n'est pas prise en charge dans la région Moyen-Orient (Bahreïn) ni dans les régions AWS GovCloud (US).

Important

Ce guide décrit l'utilisation de Amazon RDS Performance Insights avec des moteurs de bases de données non Aurora. Pour de plus amples informations sur l'utilisation d'Amazon RDS Performance Insights avec Amazon Aurora, veuillez consulter Utilisation d'Amazon RDS Performance Insights dans le Guide de l'utilisateur pour Amazon Aurora.

Activation et désactivation de Performance Insights

Pour utiliser Performance Insights, vous devez l'activer sur votre instance de base de données. Si nécessaire, vous pouvez le désactiver plus tard. L'activation et la désactivation de Performance Insights ne provoquent pas de temps d'arrêt, de redémarrage ou de basculement.

L'agent Performance Insights consomme une quantité limitée d'UC et de mémoire sur l'hôte de base de données. Lorsque la charge de base de données est élevée, l'agent limite l'impact sur les performances en collectant des données moins fréquemment.

Console

Dans la console, vous pouvez activer ou désactiver Performance Insights lorsque vous créez ou modifiez une nouvelle instance de base de données.

Activation ou désactivation de Performance Insights lors de la création d'une instance

Lorsque vous créez une nouvelle instance de base de données, activez Performance Insights en choisissant Activer Performance Insights dans la section Performance Insights. Vous pouvez aussi choisir Désactiver Performance Insights

Pour créer une instance de base de données, suivez les instructions relatives à votre moteur de base de données dans Création d'une instance de base de données Amazon RDS (p. 146).

L'image suivante représente la section Performance Insights (Analyse des performances).

Vous disposez des options suivantes lorsque vous choisissez Activer Performance Insights :

- Conservation – Durée de conservation des données de Performance Insights. Choisissez 7 jours (valeur par défaut) ou 2 ans.
- Clé principale : spécifiez votre clé principale client (CMK) AWS Key Management Service (AWS KMS). Performance Insights chiffre toutes les données potentiellement sensibles à l'aide votre clé CMK AWS KMS. Les données sont chiffrées en transit et au repos. Pour plus d'informations, consultez Chiffrement des ressources Amazon RDS (p. 1522).

Activation ou désactivation de Performance Insights lors de la modification d'une instance

Dans la console, vous pouvez modifier une instance de base de données pour activer ou désactiver Performance Insights.

Pour activer ou désactiver Performance Insights pour une instance de base de données à l'aide de la console

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Choisissez Bases de données.
3. Choisissez une instance de base de données, puis Modifiez.
4. Dans la section Performance Insights choisissez Activer Performance Insights ou Désactiver Performance Insights.

Vous disposez des options suivantes lorsque vous choisissez Activer Performance Insights :

- Conservation – Durée de conservation des données de Performance Insights. Choisissez 7 jours (valeur par défaut) ou 2 ans.
- Clé principale : spécifiez votre clé principale client (CMK) AWS Key Management Service (AWS KMS). Performance Insights chiffre toutes les données potentiellement sensibles à l'aide votre clé CMK AWS KMS. Les données sont chiffrées en transit et au repos. Pour plus d'informations, consultez Chiffrement des ressources Amazon RDS (p. 1522).

5. Choisissez Continue.
6. Pour Scheduling of Modifications (Planification des modifications), choisissez une des options suivantes :
   - Apply during the next scheduled maintenance window (Appliquer lors de la prochaine fenêtre de maintenance planifiée) – Attendre la prochaine fenêtre de maintenance pour appliquer la modification de Performance Insights.
   - Apply immediately (Appliquer immédiatement) – Appliquer la modification de Performance Insights dès que possible.
7. Choisissez Modify instance (Modifier l'instance).

AWS CLI

Lorsque vous utilisez la commande de l'AWS CLI create-db-instance, activez Performance Insights en spécifiant `--enable-performance-insights`. Ou désactivez Performance Insights en spécifiant `--no-enable-performance-insights`.

Vous pouvez également spécifier ces valeurs à l'aide des commandes d'AWS CLI suivantes :

- create-db-instance-read-replica
- modify-db-instance
- restore-db-instance-from-s3

La procédure suivante explique comment activer ou désactiver Performance Insights pour une instance de base de données à l'aide de l'AWS CLI.

Pour activer ou désactiver Performance Insights pour une instance de base de données à l'aide de l'AWS CLI

- Appelez la commande modify-db-instance d'AWS CLI et fournissez les valeurs suivantes :
  - `--db-instance-identifier` – Nom de l'instance de base de données.
  - `--enable-performance-insights` pour activer ou `--no-enable-performance-insights` pour désactiver

  L'exemple suivant active Performance Insights pour `sample-db-instance`.

  Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier sample-db-instance \
    --enable-performance-insights
```

  Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier sample-db-instance ^
    --enable-performance-insights
```

Lorsque vous activez Performance Insights, vous pouvez éventuellement spécifier la durée, en jours, de conservation des données de Performance Insights avec l'option `--performance-insights-retention-period`. Les valeurs valides sont 7 (valeur par défaut) ou 731 (2 ans).

L'exemple suivant active Performance Insights pour `sample-db-instance` et spécifie que les données de Performance Insights sont conservées pendant deux ans.

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier sample-db-instance \
    --enable-performance-insights \
    --performance-insights-retention-period 731
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier sample-db-instance ^
    --enable-performance-insights ^
    --performance-insights-retention-period 731
```

API RDS

Lorsque vous créez une nouvelle instance de base de données à l'aide de l'opération CreateDBInstance de l'API Amazon RDS, activez Performance Insights en définissant `EnablePerformanceInsights` sur `True`. Pour désactiver Performance Insights, définissez `EnablePerformanceInsights` sur `False`.

Vous pouvez également spécifier la valeur `EnablePerformanceInsights` à l'aide des opérations d'API suivantes :

- ModifyDBInstance
- CreateDBInstanceReadReplica
- RestoreDBInstanceFromS3

Lorsque vous activez Performance Insights, vous pouvez éventuellement spécifier la durée, en jours, de conservation des données de Performance Insights avec le paramètre `PerformanceInsightsRetentionPeriod`. Les valeurs valides sont 7 (valeur par défaut) ou 731 (2 ans).

Activation du schéma de performance pour Performance Insights sur Amazon RDS for MariaDB ou MySQL

Lorsque la fonction de schéma de performance est activée pour Amazon RDS for MariaDB ou MySQL, Performance Insights fournit des informations plus détaillées. Par exemple, Performance Insights affiche la charge de la base de données classée par événements d'attente détaillés. Si le schéma de performance n'est pas activé, Performance Insights affiche la charge de la base de données classée selon l'état de la liste du processus MySQL.

Le schéma de performance est activé automatiquement lorsque vous créez une instance de base de données Amazon RDS pour MariaDB ou MySQL avec Performance Insights activé. Dans ce cas, Performance Insights gère automatiquement les paramètres dans le tableau suivant.

Nom du paramètre	Valeur de paramètre
`performance_schema`	`1` (le paramètre `source` est défini sur `engine-default`)
`performance-schema-consumer-events-waits-current`	`ON`
`performance-schema-instrument`	`wait/%=ON`
`performance-schema-consumer-global-instrumentation`	`ON`
`performance-schema-consumer-thread-instrumentation`	`ON`

> **Important**
>
> Lorsque le schéma de performance est activé automatiquement, Performance Insights modifie les paramètres liés à ce dernier sur l'instance de base de données. Ces modifications ne sont pas visibles dans le groupe de paramètres associé à l'instance de base de données.

Pour de plus amples informations, veuillez consulter Performance Schema Command Options et Performance Schema Option and Variable Reference dans la documentation MySQL.

Activation manuelle du schéma de performance

Le schéma de performance n'est pas activé lorsque les deux conditions suivantes sont remplies :

- Le paramètre `performance_schema` est défini sur `0` ou `1`.
- Le paramètre `performance_schema source` est défini sur `user`.

Pour activer manuellement le schéma de performance

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Choisissez Groupes de paramètres.
3. Sélectionnez le groupe de paramètres pour votre instance de base de données.
4. Sélectionnez le paramètre `performance_schema`.
5. Sélectionnez Modifier les paramètres.
6. Sélectionnez Réinitialiser.
7. Sélectionnez Réinitialiser les paramètres.
8. Redémarrez l'instance de base de données.

Pour plus d'informations sur la modification des paramètres d'instance de base de données, consultez Modification de paramètres dans un groupe de paramètres de bases de données (p. 229). Pour de plus amples informations sur le tableau de bord, veuillez consulter Surveillance avec le tableau de bord de Performance Insights (p. 419). Pour plus d'informations sur le schéma de performances MySQL, consultez Manuel de référence MySQL 8.0.

Accès à Performance Insights

Pour accéder à Performance Insights, vous devez disposer des autorisations appropriées de AWS Identity and Access Management (IAM). Deux options sont disponibles pour l'octroi d'accès :

1. Attacher la stratégie gérée `AmazonRDSFullAccess` à un utilisateur ou rôle IAM.
2. Créer une stratégie personnalisée IAM et l'attacher à un utilisateur ou rôle IAM.

Stratégie gérée AmazonRDSFullAccess

`AmazonRDSFullAccess` est une stratégie gérée AWS qui accorde l'accès à toutes les opérations d'API Amazon RDS. La stratégie accorde aussi l'accès aux services connexes qui sont utilisés par la console Amazon RDS, par exemple, les notifications d'événement à l'aide de Amazon SNS.

En outre, `AmazonRDSFullAccess` contient toutes les autorisations nécessaires pour utiliser Performance Insights. Si vous attachez cette stratégie à un utilisateur ou un rôle IAM, le destinataire peut utiliser Performance Insights avec d'autres fonctionnalités de la console.

Utilisation d'une stratégie IAM personnalisée

Pour les utilisateurs qui ne bénéficient pas d'un accès total avec la stratégie `AmazonRDSFullAccess`, vous pouvez accorder l'accès à Performance Insights en créant ou modifiant une stratégie IAM gérée par l'utilisateur. Quand vous attachez la stratégie à un utilisateur ou rôle IAM, le destinataire peut se servir de Performance Insights.

Pour créer une stratégie personnalisée

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, choisissez Policies.
3. Choisissez Créer une stratégie.
4. Sur la page Créer une stratégie, choisissez l'onglet JSON.
5. Copiez et collez ce qui suit.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "pi:*",
            "Resource": "arn:aws:pi:*:*:metrics/rds/*"
        }
    ]
}
```

6. Choisissez Examiner une stratégie.
7. Indiquez un nom pour la stratégie et éventuellement une description, puis choisissez Créer une stratégie.

Vous pouvez maintenant attacher la stratégie à un utilisateur ou rôle IAM. La procédure suivante suppose que vous disposez déjà d'un utilisateur IAM à cette fin.

Pour attacher la stratégie à un utilisateur IAM

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.

2. Dans le volet de navigation, sélectionnez Users.
3. Choisissez un utilisateur existant dans la liste.

   Important

   Pour utiliser Performance Insights, assurez-vous que vous avez accès à Amazon RDS en plus de l'accès à la stratégie personnalisée. Par exemple, la stratégie prédéfinie `AmazonRDSReadOnlyAccess` fournit un accès en lecture seule à Amazon RDS. Pour de plus amples informations, veuillez consulter Gestion de l'accès à l'aide de stratégies (p. 1539).
4. Sur la page Récapitulatif, choisissez Ajouter des autorisations.
5. Choisissez Attacher directement les stratégies existantes. Pour Recherche, tapez les premiers caractères du nom de votre stratégie, comme illustré ci-après.

6. Choisissez votre stratégie, puis sélectionnez Suivant : Vérification.
7. Choisissez Add permissions.

Surveillance avec le tableau de bord de Performance Insights

Le tableau de bord de Performance Insights contient des informations sur les performances des bases de données qui vous aideront à analyser et à résoudre les problèmes de performances. Sur la page de tableau de bord principale, vous pouvez afficher des informations concernant la charge de la base de données. Vous pouvez également obtenir des informations détaillée concernant un état d'attente, une requête SQL, un hôte ou un utilisateur en particulier.

Ouverture du tableau de bord de Performance Insights

Pour afficher le tableau de bord de Performance Insights, procédez comme suit.

Pour afficher le tableau de bord Performance Insights dans AWS Management Console

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Performance Insights.
3. Choisissez une instance de base de données. Le tableau de bord de Performance Insights s'affiche pour cette instance de base de données.

   Pour les instances de base de données avec activation de Performance Insights, vous pouvez également accéder au tableau de bord en choisissant l'élément Sessions dans la liste des instances de base de données. Sous Activité actuelle, l'élément Sessions affiche la charge de base de données dans les sessions actives moyennes lors des cinq dernières minutes. La barre affiche visuellement le chargement. Votre instance de base de données est à l'arrêt lorsque la barre est vide. La barre se remplit de bleu à mesure que le chargement augmente. Une fois que le chargement dépasse le nombre d'UC virtuels (vUC) dans la classe d'instance de base de données, la barre vire au rouge, ce qui indique un engorgement potentiel.

   L'image suivante montre le tableau de bord pour une instance de base de données. Par défaut, le tableau de bord de Performance Insights affiche les données pour l'heure précédente.

4. (Facultatif) Choisissez un intervalle de temps différent en sélectionnant un bouton dans le coin supérieur droit. Par exemple, pour modifier l'intervalle à 5 heures, sélectionnez 5h.

Dans la capture d'écran suivante, l'intervalle de charge de base de données est de 5 heures.

5. (Facultatif) Pour actualiser automatiquement vos données, activez Auto refresh (Actualisation automatique).

Le tableau de bord Performance Insight s'actualise automatiquement avec de nouvelles données. Le taux de rafraîchissement dépend de la quantité de données affichées :

- Si vous choisissez 5 minutes, les données seront actualisées toutes les 5 secondes.
- 1 heure se réactualise toutes les minutes.
- 5 heures se réactualise toutes les minutes.
- 24 heures se réactualise toutes les 5 minutes.
- 1 semaine se réactualise toutes les heures.

Composants du tableau de bord de Performance Insights

Le tableau de bord est divisé en trois parties :

1. Counter Metrics (Métriques de compteur) – Affiche les données relatives à certaines métriques du compteur de performances.
2. DB Load Chart (Graphique de charge de base de données) – Affiche la comparaison entre la charge de base de données et la capacité de l'instance de base de données telle que représentée par la ligne Max vCPU (UC virtuelle max).
3. Principaux éléments – Affiche les principaux éléments liés à l'attente, à SQL, aux hôtes et aux utilisateurs contribuant à la charge de base de données.

Graphique Counter Metrics (Métriques de compteur)

Le graphique Counter Metrics (Métriques de compteur) affiche des données sur les compteurs de performances. Les métriques par défaut dépendent du moteur de base de données.

- MySQL et 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`

Modifiez les compteurs de performance en choisissant Manage Metrics (Gérer les métriques). Vous pouvez sélectionner plusieurs métriques de système d'exploitation ou métriques de base de données, comme illustré dans la capture d'écran suivante. Pour afficher les détails relatifs à une métrique, passez la souris sur le nom de la métrique.

Pour plus d'informations, consultez Personnalisation du tableau de bord de Performance Insights (p. 440).

Graphique Average Active Sessions (Sessions actives en moyenne)

Le graphique Database Load (charge de base de données) affiche la comparaison entre la charge de base de données et la capacité de l'instance de base de données représentée par la ligne Max CPU (UC virtuelle max). Par défaut, la charge s'affiche sous la forme de sessions actives regroupées par états d'attente dans un graphique à barres.

Vous pouvez choisir d'afficher la charge sous forme de sessions actives regroupées par éléments (attente, SQL, utilisateurs ou hôtes). Vous pouvez également choisir un graphique linéaire.

Pour afficher les détails d'un élément de charge de base de données tel qu'une instruction SQL, passez la souris sur le nom de l'élément.

Pour afficher les détails d'un élément pour la période sélectionnée dans la légende, survolez cet élément.

Table de chargement par le dessus

Le tableau Top Load (Principaux éléments de charge affiche les principaux éléments contribuant à la charge de la base de données. Par défaut, la console affiche les principales requêtes SQL contribuant à la charge de base de données, ainsi que des statistiques pertinentes pour chaque instruction. Vous pouvez choisir d'afficher plutôt les principaux éléments liés à l'attente, aux hôtes ou aux utilisateurs.

Pour afficher les composants d'une requête, sélectionnez cette dernière, puis choisissez le signe plus (« + »). Un récapitulatif SQL est composé de plusieurs requêtes réelles et structurellement similaires, mais pouvant avoir des valeurs littérales différentes. Dans la capture d'écran suivante, la requête sélectionnée est un récapitulatif.

Dans Top sql (Principaux éléments SQL), la colonne Load by waits (AAS) [Charge par attentes (AAS)] illustre le pourcentage de la charge de base de données associée à chacun des principaux éléments de charge. Cette colonne reflète la charge pour cet élément selon le regroupement actuellement sélectionné dans DB Load Chart (Graphique de charge de base de données). Par exemple, vous pouvez regrouper DB Load Chart (Graphique de charge de base de données) en fonction des états d'attente. Vous examinez les requêtes SQL dans le tableau des principaux éléments de charge. Dans ce cas, la dimension, la segmentation et le code de couleurs de la barre DB Load by Waits (Charge de base de données par attente) représentent la proportion du temps d'un état d'attente donné auquel cette requête contribue. Cette barre indique également les états d'attente qui affectent la requête sélectionnée.

Dans le tableau Top sql (Principaux éléments SQL), vous pouvez ouvrir une instruction pour afficher ses informations. Les informations s'affichent dans le volet inférieur.

Dans le tableau Top sql (Principaux éléments SQL), vous pouvez afficher les types suivants d'identifiants (ID) associés à des instructions SQL :

- ID SQL de support – Valeur de hachage de l'ID SQL. Cette valeur est uniquement destinée à référencer un ID SQL lorsque vous utilisez AWS Support. AWS Support n'a pas accès à vos ID SQL réels et au texte SQL.
- Support Digest ID (ID digest de support) – Valeur de hachage de l'ID digest. Cette valeur est uniquement destinée à référencer un ID digest lorsque vous utilisez AWS Support. AWS Support n'a pas accès à vos ID digest réels et au texte SQL.

Vous pouvez contrôler les statistiques affichées dans l'onglet Top sql (Principaux éléments SQL) en choisissant l'icône Preferences (Préférences).

Lorsque vous choisissez l'icône Préférences, la fenêtre Préférences s'ouvre.

Activez les statistiques que vous souhaitez afficher dans l'onglet Top sql (Principaux éléments SQL), utilisez votre souris pour faire défiler l'écran jusqu'au bas de la fenêtre, puis choisissez Continue (Continuer).

Analyse de la charge de la base de données à l'aide du tableau de bord de Performance Insights

Si le graphique Average Active Sessions (Sessions actives en moyenne) présente un goulot d'étranglement, vous pouvez déterminer la provenance de la charge. Pour ce faire, observez le tableau Top Load Items (Principaux éléments de charge) sous le graphique Average Active Sessions (Sessions actives en moyenne). Choisissez un élément précis (une requête SQL ou un utilisateur par exemple) pour approfondir son analyse et afficher les détails le concernant.

La vue par défaut du tableau de bord de Performance Insights affiche la charge de la base de données en fonction de l'attente et les principales requêtes SQL. Cette combinaison fournit en général la meilleure compréhension des problèmes de performances. L'affichage de la charge de la base de données en fonction de l'attente indique s'il existe des goulots d'étranglement liés aux ressources ou à des actions simultanées dans la base de données. Dans ce cas, l'onglet SQL du tableau Top Load Items (Principaux éléments de charge) indique les requêtes à l'origine de cette charge.

Votre flux de travail standard pour diagnostiquer les problèmes de performances se présente comme suit :

1. Examinez le graphique Average Active Sessions (Sessions actives en moyenne) et regardez s'il existe des incidents de charge de la base de données dépassant la ligne Max CPU (UC max).
2. Si tel est le cas, observez le graphique Average Active Sessions (Sessions actives en moyenne) et identifiez le ou les états d'attente principalement responsables.
3. Identifiez les requêtes de hachage à l'origine de la charge en déterminant les requêtes du tableau Top Load Items (Principaux éléments de charge) de l'onglet SQL qui contribuent le plus à ces états d'attente. Vous pouvez les identifier dans la colonne DB Load by Wait (Charge de base de données par attente).
4. Choisissez l'une de ces requêtes de hachage dans l'onglet SQL pour la développer et afficher les requêtes enfants qui la composent.

Par exemple, dans le tableau de bord suivant, les attentes log file sync (synchronisation de fichier journal) constituent la majeure partie de la charge de base de données. Les attentes LGWR all worker groups sont également élevées. Le graphique Top sql (Principaux éléments SQL) montre ce qui provoque les attentes log file sync (synchronisation de fichier journal) : instructions `COMMIT` fréquentes. Dans ce cas, une validation moins fréquente permet de réduire la charge de base de données.

Analyse des statistiques pour les requêtes en cours d'exécution

Dans Amazon RDS Performance Insights, vous trouverez les statistiques sur les requêtes en cours d'exécution dans la section Top load_items (Principaux load_items). Performance Insights collecte des statistiques uniquement pour les requêtes les plus courantes. Généralement, celles-ci correspondent aux requêtes les plus importantes par charge affichées dans le tableau de bord Performance Insights.

Statistiques pour MariaDB et MySQL

L'analyse des performances collecte des statistiques de synthèse SQL à partir de la table `events_statements_summary_by_digest`. Cette table est gérée par la base de données et n'a pas de stratégie d'expulsion. Si la table devient pleine, les nouvelles requêtes SQL ne sont pas suivies. Pour résoudre ce problème, l'analyse des performances tronque automatiquement la table lorsqu'elle est presque pleine.

Performance Insights ne tronque automatiquement la table que si votre groupe de paramètres n'a pas de valeur explicitement définie pour le paramètre `performance_schema`. Vous avez la possibilité d'examiner le paramètre `performance_schema` et, si la valeur de la source est `user`, de définir une valeur. Si vous souhaitez que Performance Insights tronque automatiquement la table, réinitialisez la valeur du paramètre `performance_schema`. Vous pouvez afficher la source de la valeur d'un paramètre en affichant le paramètre dans AWS Management Console ou en exécutant la commande describe-db-parameters de l'AWS CLI. Le message suivant est affiché dans l'AWS Management Console lorsque le tableau est plein :

```
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.
```

Les statistiques SQL suivantes sont disponibles pour les instances de bases de données MariaDB et MySQL.

Métrique	Unit
db.sql_tokenized.stats.count_star_per_sec	Appels par seconde
db.sql_tokenized.stats.sum_timer_wait_per_sec	Exécutions actives moyennes par seconde
db.sql_tokenized.stats.sum_select_full_join_per_sec	Sélections de jointures complètes par seconde
db.sql_tokenized.stats.sum_select_range_check_per_sec	Sélections de vérifications de plages par seconde
db.sql_tokenized.stats.sum_select_scan_per_sec	Sélections d'analyses par seconde
db.sql_tokenized.stats.sum_sort_merge_passes_per_sec	Tris de transmissions de fusion par seconde
db.sql_tokenized.stats.sum_sort_scan_per_sec	Tris d'analyses par seconde
db.sql_tokenized.stats.sum_sort_range_per_sec	Tris de plages par seconde
db.sql_tokenized.stats.sum_sort_rows_per_sec	Tris de lignes par seconde
db.sql_tokenized.stats.sum_rows_affected_per_sec	Lignes affectées par seconde
db.sql_tokenized.stats.sum_rows_examined_per_sec	Lignes examinées par seconde
db.sql_tokenized.stats.sum_rows_sent_per_sec	Lignes envoyées par seconde

Métrique	Unit
db.sql_tokenized.stats.sum_created_tmp_disk_tables_per_sec	Créations de tables de disques temporaires par seconde
db.sql_tokenized.stats.sum_created_tmp_tables_per_sec	Créations de tables temporaires par seconde
db.sql_tokenized.stats.sum_lock_time_per_sec	Temps de verrouillage par seconde (en millisecondes)

Les métriques suivantes fournissent les statistiques par appel pour une instruction SQL.

Métrique	Unit
db.sql_tokenized.stats.sum_timer_wait_per_call	Latence moyenne par appel (en millisecondes)
db.sql_tokenized.stats.sum_select_full_join_per_call	Sélections de jointures complètes par appel
db.sql_tokenized.stats.sum_select_range_check_per_call	Sélections de vérifications de plages par appel
db.sql_tokenized.stats.sum_select_scan_per_call	Sélections d'analyses par appel
db.sql_tokenized.stats.sum_sort_merge_passes_per_call	Tris de transmissions de fusion par appel
db.sql_tokenized.stats.sum_sort_scan_per_call	Tris d'analyses par appel
db.sql_tokenized.stats.sum_sort_range_per_call	Tris de plages par appel
db.sql_tokenized.stats.sum_sort_rows_per_call	Tris de lignes par appel
db.sql_tokenized.stats.sum_rows_affected_per_call	Lignes affectées par appel
db.sql_tokenized.stats.sum_rows_examined_per_call	Lignes examinées par appel
db.sql_tokenized.stats.sum_rows_sent_per_call	Lignes envoyées par appel
db.sql_tokenized.stats.sum_created_tmp_disk_tables_per_call	Créations de tables de disques temporaires par appel
db.sql_tokenized.stats.sum_created_tmp_tables_per_call	Créations de tables temporaires par appel
db.sql_tokenized.stats.sum_lock_time_per_call	Temps de verrouillage par appel (en ms)

Analyse des métriques MariaDB et MySQL pour exécuter les instructions SQL

À l'aide d'AWS Management Console, vous pouvez afficher les métriques d'une requête SQL en cours d'exécution en choisissant l'onglet SQL et en développant la requête.

Choisissez les statistiques à afficher en sélectionnant l'icône en forme d'engrenage dans le coin supérieur droit du graphique.

La capture d'écran suivante montre les préférences pour les instances de base de données MariaDB et MySQL.

Statistiques pour Amazon RDS pour Oracle

Les statistiques SQL suivantes sont disponibles pour les instances Oracle DB.

Métrique	Unit
db.sql.stats.executions_per_sec	Nombre d'exécutions par seconde
db.sql.stats.elapsed_time_per_sec	Exécutions actives moyennes
db.sql.stats.rows_processed_per_sec	Lignes traitées par seconde
db.sql.stats.buffer_gets_per_sec	Buffers obtenus par seconde
db.sql.stats.physical_read_requests_per_sec	Lectures physiques par seconde
db.sql.stats.physical_write_requests_per_sec	Écritures physiques par seconde
db.sql.stats.total_sharable_mem_per_sec	Mémoire totale partageable par seconde (en octets)
db.sql.stats.cpu_time_per_sec	Temps UC par seconde (en millisecondes)

Les métriques suivantes fournissent les statistiques par appel pour une instruction SQL.

Métrique	Unit
db.sql.stats.elapsed_time_per_exec	Temps écoulé par exécution (en millisecondes)

Métrique	Unit
db.sql.stats.rows_processed_per_exec	Lignes traitées par exécution
db.sql.stats.buffer_gets_per_exec	Buffers obtenus par exécution
db.sql.stats.physical_read_requests_per_exec	Lectures physiques par exécution
db.sql.stats.physical_write_requests_per_exec	Écritures physiques par exécution
db.sql.stats.total_sharable_mem_per_exec	Mémoire totale partageable par exécution (en octets)
db.sql.stats.cpu_time_per_exec	Temps UC par exécution (en millisecondes)

Analyse des métriques Oracle pour l'exécution des instructions SQL

À l'aide d'AWS Management Console, vous pouvez afficher les métriques d'une requête SQL en cours d'exécution en choisissant l'onglet SQL et en développant la requête.

Choisissez les statistiques à afficher en sélectionnant l'icône en forme d'engrenage dans le coin supérieur droit du graphique.

La capture d'écran suivante montre les préférences pour les instances de base de données Oracle.

La capture d'écran suivante montre les statistiques d'une instruction SQL.

SQL statements	executions/sec	elapsed time (ms)
Commit	-	-
Unknown	-	-
LGWR	-	-
CKPT	-	-
DBW0	-	-
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	-	-

Affichage de texte SQL supplémentaire dans le tableau de bord de Performance Insights

Par défaut, chaque ligne du tableau Top sql (Principaux éléments SQL) affiche 500 octets de texte SQL pour chaque instruction SQL. Lorsque la taille d'une instruction SQL est supérieure à 500 octets, vous pouvez la développer en ouvrant l'instruction dans le tableau de bord de Performance Insights. Le tableau de bord affiche le texte jusqu'aux limites suivantes par moteur :

- Amazon RDS for Microsoft SQL Server – 4 096 caractères
- Amazon RDS for MySQL et MariaDB – 1 024 octets
- Amazon RDS pour Oracle – 1 000 octets

Vous pouvez copier le texte affiché sur le tableau de bord ou choisir Download (Télécharger).

Amazon RDS for PostgreSQL gère le texte différemment. À l'aide du tableau de bord Performance Insights, vous pouvez afficher et télécharger jusqu'à 500 octets. Pour accéder à plus de 500 octets, définissez la limite de taille avec le paramètre d'instance de base de données `track_activity_query_size`. La valeur maximale est de 102 400 octets. Pour afficher ou télécharger du texte de plus de 500 octets, utilisez AWS Management Console et non l'interface de ligne de commande ou l'API Performance Insights. Pour de plus amples informations, veuillez consulter Définition de la limite de taille d'un texte SQL pour les instances de base de données Amazon RDS for PostgreSQL (p. 438).

Pour afficher du texte SQL supplémentaire dans le tableau de bord de Performance Insights

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Performance Insights.
3. Choisissez une instance de base de données. Le tableau de bord de Performance Insights s'affiche pour cette instance de base de données.

   Les instructions SQL dont la taille du texte est supérieure à 500 octets ressemblent à l'image ci-dessous.

4. Examinez la section relative aux informations SQL pour afficher plus de texte SQL.

Le tableau de bord de Performance Insights peut afficher jusqu'à 4 096 octets par instruction SQL.

5. (Facultatif) Choisissez Copy (Copier) pour copier l'instruction SQL affichée ou Download (Télécharger) pour télécharger l'instruction SQL et en afficher le texte jusqu'à la limite du moteur de base de données.

   Note

   Pour copier ou télécharger l'instruction SQL, désactivez les bloqueurs de fenêtres contextuelles.

Définition de la limite de taille d'un texte SQL pour les instances de base de données Amazon RDS for PostgreSQL

Pour les instances de base de données Amazon RDS for PostgreSQL, vous pouvez contrôler la limite pour le texte SQL qui peut être affiché dans le tableau de bord Analyse des performances.

Pour ce faire, modifiez le paramètre `track_activity_query_size` de l'instance de base de données. La valeur par défaut du paramètre `track_activity_query_size` est 1 024 octets.

Vous pouvez augmenter le nombre d'octets pour augmenter la taille du texte SQL visible dans le tableau de bord de Performance Insights. La valeur limite du paramètre est 102 400 octets. Pour de plus amples informations sur le paramètre `track_activity_query_size` d'instance de base de données, veuillez consulter Run-time Statistics dans la documentation PostgreSQL.

Pour modifier ce paramètre, modifiez sa valeur dans le groupe de paramètres associé à l'instance de base de données Amazon RDS for PostgreSQL.

Si l'instance de base de données Amazon RDS for PostgreSQL utilise le groupe de paramètres par défaut, procédez comme suit :

1. Créez un nouveau groupe de paramètres pour l'instance de base de données, associé au moteur de base de données et à sa version appropriés.
2. Définissez le paramètre dans le nouveau groupe de paramètres.
3. Associez le nouveau groupe de paramètres à l'instance de base de données.

Pour de plus amples informations sur la définition d'un paramètre d'instance de base de données, veuillez consulter Modification de paramètres dans un groupe de paramètres de bases de données (p. 229).

Zoom avant sur le graphique de charge de base de données

Vous pouvez utiliser d'autres fonctions de l'interface utilisateur Performance Insights pour vous aider à analyser les données de performance.

Zoom avant par cliquer et glisser

Dans l'interface Performance Insights, vous pouvez sélectionner une petite portion du graphique de charge et faire un zoom avant sur les détails.

Faites un zoom avant sur une portion du graphique de charge, choisissez l'heure de début et faites glisser jusqu'à la fin de la période souhaitée. Lorsque vous faites ceci, la zone sélectionnée est mise en évidence. Lorsque vous relâchez la souris, le graphique de charge fait un zoom avant sur la région AWS sélectionnée et la table Top items (Principaux éléments) est recalculée.

Personnalisation du tableau de bord de Performance Insights

Grâce aux métriques de compteur, vous pouvez personnaliser le tableau de bord de Performance Insights de sorte à inclure jusqu'à 10 graphiques supplémentaires. Ces graphiques affichent une sélection de douze métriques de performance de base de données et de système d'exploitation. Ces informations peuvent être corrélées avec la charge de la base de données pour aider à identifier et analyser les problèmes de performances.

Rubriques

- Compteurs de système d'exploitation Performance Insights (p. 441)
- Compteurs Performance Insights pour Amazon RDS for MariaDB et MySQL (p. 443)
- Compteurs d'analyse des performances pour Amazon RDS pour Microsoft SQL Server (p. 446)
- Compteurs Performance Insights pour Amazon RDS pour Oracle (p. 447)
- Compteurs d'Analyse des performances pour Amazon RDS for PostgreSQL (p. 449)

Compteurs de système d'exploitation Performance Insights

Les compteurs de système d'exploitation suivants sont disponibles avec Performance Insights pour Aurora PostgreSQL. La section Affichage de la surveillance améliorée à l'aide de CloudWatch Logs (p. 401) fournit les définitions de ces métriques.

Compteur	Type	Métrique
actif	memory	os.memory.active
buffers	memory	os.memory.buffers
mis en cache	memory	os.memory.cached
dirty	memory	os.memory.dirty
free	memory	os.memory.free
hugePagesFree	memory	os.memory.hugePagesFree
hugePagesRsvd	memory	os.memory.hugePagesRsvd
hugePagesSize	memory	os.memory.hugePagesSize
hugePagesSurp	memory	os.memory.hugePagesSurp
hugePagesTotal	memory	os.memory.hugePagesTotal
inactive	memory	os.memory.inactive
mapped	memory	os.memory.mapped
pageTables	memory	os.memory.pageTables
slab	memory	os.memory.slab
total	memory	os.memory.total
writeback	memory	os.memory.writeback
guest	cpuUtilization	os.cpuUtilization.guest
idle	cpuUtilization	os.cpuUtilization.idle
irq	cpuUtilization	os.cpuUtilization.irq
nice	cpuUtilization	os.cpuUtilization.nice
steal	cpuUtilization	os.cpuUtilization.steal
system	cpuUtilization	os.cpuUtilization.system
total	cpuUtilization	os.cpuUtilization.total
user	cpuUtilization	os.cpuUtilization.user
wait	cpuUtilization	os.cpuUtilization.wait
avgQueueLen	diskIO	os.diskIO.avgQueueLen
avgReqSz	diskIO	os.diskIO.avgReqSz

Compteur	Type	Métrique
await	diskIO	os.diskIO.await
readIOsPS	diskIO	os.diskIO.readIOsPS
readKb	diskIO	os.diskIO.readKb
readKbPS	diskIO	os.diskIO.readKbPS
rrqmPS	diskIO	os.diskIO.rrqmPS
tps	diskIO	os.diskIO.tps
util	diskIO	os.diskIO.util
writeIOsPS	diskIO	os.diskIO.writeIOsPS
writeKb	diskIO	os.diskIO.writeKb
writeKbPS	diskIO	os.diskIO.writeKbPS
wrqmPS	diskIO	os.diskIO.wrqmPS
blocked	tasks	os.tasks.blocked
running	tasks	os.tasks.running
sleeping	tasks	os.tasks.sleeping
stopped	tasks	os.tasks.stopped
total	tasks	os.tasks.total
zombie	tasks	os.tasks.zombie
one	loadAverageMinute	os.loadAverageMinute.one
fifteen	loadAverageMinute	os.loadAverageMinute.fifteen
five	loadAverageMinute	os.loadAverageMinute.five
mis en cache	swap	os.swap.cached
free	swap	os.swap.free
dans	swap	os.swap.in
out	swap	os.swap.out
total	swap	os.swap.total
maxFiles	fileSys	os.fileSys.maxFiles
usedFiles	fileSys	os.fileSys.usedFiles
usedFilePercent	fileSys	os.fileSys.usedFilePercent
usedPercent	fileSys	os.fileSys.usedPercent
used	fileSys	os.fileSys.used
total	fileSys	os.fileSys.total

Compteur	Type	Métrique
rx	network	os.network.rx
tx	network	os.network.tx
numVCPUs	general	os.general.numVCPUs

Compteurs Performance Insights pour Amazon RDS for MariaDB et MySQL

Les compteurs de base de données suivants sont disponibles avec Performance Insights pour Amazon RDS for MariaDB et MySQL.

Rubriques

- Compteurs natifs pour RDS MariaDB et RDS MySQL (p. 443)
- Compteurs non natifs pour Amazon RDS for MariaDB et MySQL (p. 444)

Compteurs natifs pour RDS MariaDB et RDS MySQL

La section Server Status Variables de la documentation MySQL fournit les définitions de ces métriques natives.

Compteur	Type	Unité	Métrique
Com_analyze	SQL	Requêtes par seconde	db.SQL.Com_analyze
Com_optimize	SQL	Requêtes par seconde	db.SQL.Com_optimize
Com_select	SQL	Requêtes par seconde	db.SQL.Com_select
Innodb_rows_deleted	SQL	Lignes par seconde	db.SQL.Innodb_rows_deleted
Innodb_rows_inserted	SQL	Lignes par seconde	db.SQL.Innodb_rows_inserted
Innodb_rows_read	SQL	Lignes par seconde	db.SQL.Innodb_rows_read
Innodb_rows_updated	SQL	Lignes par seconde	db.SQL.Innodb_rows_updated
Select_full_join	SQL	Requêtes par seconde	db.SQL.Select_full_join
Select_full_range_join	SQL	Requêtes par seconde	db.SQL.Select_full_range_join
Select_range	SQL	Requêtes par seconde	db.SQL.Select_range
Select_range_check	SQL	Requêtes par seconde	db.SQL.Select_range_check
Select_scan	SQL	Requêtes par seconde	db.SQL.Select_scan
Slow_queries	SQL	Requêtes par seconde	db.SQL.Slow_queries
Sort_merge_passes	SQL	Requêtes par seconde	db.SQL.Sort_merge_passes
Sort_range	SQL	Requêtes par seconde	db.SQL.Sort_range
Sort_rows	SQL	Requêtes par seconde	db.SQL.Sort_rows

Compteur	Type	Unité	Métrique
Sort_scan	SQL	Requêtes par seconde	db.SQL.Sort_scan
Questions	SQL	Requêtes par seconde	db.SQL.Questions
Innodb_row_lock_time	Locks	Millisecondes (moyenne)	db.Locks.Innodb_row_lock_time
Table_locks_immediate	Locks	Demandes par seconde	db.Locks.Table_locks_immediate
Table_locks_waited	Locks	Demandes par seconde	db.Locks.Table_locks_waited
Aborted_clients	Users	Connexions	db.Users.Aborted_clients
Aborted_connects	Users	Connexions	db.Users.Aborted_connects
Threads_created	Users	Connexions	db.Users.Threads_created
Threads_running	Users	Connexions	db.Users.Threads_running
Innodb_data_writes	E/S	Opérations par seconde	db.IO.Innodb_data_writes
Innodb_dblwr_writes	E/S	Opérations par seconde	db.IO.Innodb_dblwr_writes
Innodb_log_write_requests	E/S	Opérations par seconde	db.IO.Innodb_log_write_requests
Innodb_log_writes	E/S	Opérations par seconde	db.IO.Innodb_log_writes
Innodb_pages_written	E/S	Pages par seconde	db.IO.Innodb_pages_written
Created_tmp_disk_tables	Temp	Tables par seconde	db.Temp.Created_tmp_disk_tables
Created_tmp_tables	Temp	Tables par seconde	db.Temp.Created_tmp_tables
Innodb_buffer_pool_pages_data	Cache	Pages	db.Cache.Innodb_buffer_pool_pages_d
Innodb_buffer_pool_pages_total	Cache	Pages	db.Cache.Innodb_buffer_pool_pages_to
Innodb_buffer_pool_read_requests	Cache	Pages par seconde	db.Cache.Innodb_buffer_pool_read_req
Innodb_buffer_pool_reads	Cache	Pages par seconde	db.Cache.Innodb_buffer_pool_reads
Opened_tables	Cache	Tables	db.Cache.Opened_tables
Opened_table_definitions	Cache	Tables	db.Cache.Opened_table_definitions
Qcache_hits	Cache	Requêtes	db.Cache.Qcache_hits

Compteurs non natifs pour Amazon RDS for MariaDB et MySQL

Les métriques de compteur non natif sont des compteurs définis par Amazon RDS. Une métrique non native peut être obtenue avec une requête spécifique. Il peut également s'agir d'une métrique dérivée, pour laquelle deux compteurs natifs ou plus sont utilisés dans les calculs de rapport, de taux d'accès ou de latences.

Compteur	Type	Métrique	Description	Définition
innodb_buffer_pool_cache_hits	Cache	db.Cache.innodb_buffer_pool_cache_hits	Nombre de hits pouvant être réalisées par InnoDB à	`innodb_buffer_pool_read_requests` – `innodb_buffer_pool_reads`

Compteur	Type	Métrique	Description	Définition
			partir du pool de mémoires tampons.	
innodb_buffer_pool_cache_hit_rate	Cache	db.Cache.innodb_buffer_pool_cache_hit_rate	Pourcentage de lectures pouvant être réalisées par InnoDB à partir du pool de mémoires tampons.	`100 * innodb_buffer_pool_read_requests (innodb_buffer_pool_read_request + innodb_buffer_pool_reads)`
innodb_buffer_pool_cache_usage	Cache	db.Cache.innodb_buffer_pool_cache_usage	Pourcentage d'usage de mémoires tampons InnoDB contenant des données (pages). Note Cette valeur peut varier lors de l'utilisation de tables compressées. Pour de plus amples informations, veuillez consulter les informations relatives à `Innodb_buffer_pool_pages_data` et `Innodb_buffer_pool_pages_total` à la section Server Status Variables de la documentation MySQL.	`Innodb_buffer_pool_pages_data / Innodb_buffer_pool_pages_total * 100.0`
query_cache_hit_rate	Cache	db.Cache.query_cache_hit_rate	Taux d'accès au cache (de requête) de l'ensemble de résultats MySQL.	`Qcache_hits / (QCache_hits + Com_select) * 100`
innodb_datafile_writes_to_disk	IO	db.IO.innodb_datafile_writes_to_disk	Nombre d'écritures sur le fichier de données InnoDB sur le disque, sans compter les opérations double write et redo logging write.	`Innodb_data_writes - Innodb_log_writes - Innodb_dblwr_writes`
innodb_rows_changed	SQL	db.SQL.innodb_rows_changed	Nombre total d'opérations de ligne InnoDB.	`db.SQL.Innodb_rows_inserted + db.SQL.Innodb_rows_deleted + db.SQL.Innodb_rows_updated`
active_transactions	Transactions	db.Transactions.active_transactions	Nombre total de transactions actives.	`SELECT COUNT(1) AS active_transactions FROM INFORMATION_SCHEMA.INNODB_TRX`

Compteur	Type	Métrique	Description	Définition
innodb_deadlocks	Locks	db.Locks.innodb_deadlocks	Nombre total de blocages.	`SELECT COUNT AS innodb_deadlocks FROM INFORMATION_SCHEMA.INNODB_METRIC WHERE NAME='lock_deadlocks'`
innodb_lock_timeouts	Locks	db.Locks.innodb_lock_timeouts	Nombre total de blocages ayant expiré.	`SELECT COUNT AS innodb_lock_timeouts FROM INFORMATION_SCHEMA.INNODB_METRIC WHERE NAME='lock_timeouts'`
innodb_row_lock_waits	Locks	db.Locks.innodb_row_lock_waits	Nombre total de verrouillages de ligne ayant entraîné une attente.	`SELECT COUNT AS innodb_row_lock_waits FROM INFORMATION_SCHEMA.INNODB_METRIC WHERE NAME='lock_row_lock_waits'`

Compteurs d'analyse des performances pour Amazon RDS pour Microsoft SQL Server

Les compteurs de base de données suivants sont disponibles avec l'Analyse des performances pour RDS pour Microsoft SQL Server.

Compteurs natifs pour RDS pour Microsoft SQL Server

Vous trouverez les définitions de ces métriques natives dans Utilisation des objets SQL Server dans la documentation Microsoft SQL Server.

Compteur	Type	Unité	Métrique
Demandes transmises	Méthodes d'accès	Enregistrements par seconde	db.Access Methods.Forwarded Records
Fractionnements de page	Méthodes d'accès	Fractionnements par seconde	db.Access Methods.Page Splits
Buffer cache hit ratio	Gestionnaire des buffers	Ratio	db.Buffer Manager.Buffer cache hit ratio
Espérance de vie des pages	Gestionnaire des buffers	Espérance en secondes	db.Buffer Manager.Page life expectancy
Recherches de page	Gestionnaire des buffers	Recherches par seconde	db.Buffer Manager.Page lookups
Lectures de page	Gestionnaire des buffers	Lectures par seconde	db.Buffer Manager.Page reads

Compteur	Type	Unité	Métrique
Écritures de page	Gestionnaire des buffers	Écritures par seconde	db.Buffer Manager.Page writes
Transactions actives	Bases de données	Transactions	db.Databases.Active Transactions (_Total)
Octets de journal vidés	Bases de données	Octets vidés par seconde	db.Databases.Log Bytes Flushed (_Total)
Attentes de vidage de journal	Bases de données	Attentes par seconde	db.Databases.Log Flush Waits (_Total)
Vidages de journal	Bases de données	Vidages par seconde	db.Databases.Log Flushes (_Total)
Transactions en écriture	Bases de données	Transactions par seconde	db.Databases.Write Transactions (_Total)
Processus bloqués	Statistiques générales	Processus bloqués	db.General Statistics.Processes blocked
Connexions utilisateur	Statistiques générales	Connexions	db.General Statistics.User Connections
Attentes de verrou	Verrous	Attentes par seconde	db.Latches.Latch Waits
Nombre total de verrous	Locks	Verrous par minute	db.Locks.Number of Deadlocks (_Total)
Attributions mémoire en attente	Gestionnaire de la mémoire	Attributions mémoire	db.Memory Manager.Memory Grants Pending
Demandes par lots	Statistiques SQL	Demandes par seconde	db.SQL Statistics.Batch Requests
Compilations SQL	Statistiques SQL	Compilations par seconde	db.SQL Statistics.SQL Compilations
Recompilations SQL	Statistiques SQL	Recompilations par seconde	db.SQL Statistics.SQL Re-Compilations

Compteurs Performance Insights pour Amazon RDS pour Oracle

Les compteurs de base de données suivants sont disponibles avec l'Analyse des performances pour RDS Oracle.

Compteurs natifs pour RDS pour Oracle

La section Statistics Descriptions de la documentation Oracle fournit les définitions de ces métriques natives.

> **Note**
>
> Pour la métrique de compteur `CPU used by this session`, l'unité a été transformée des centisecondes natives en sessions actives pour simplifier l'utilisation de la valeur. Par exemple,

dans le graphique de la charge de travail de base de données, « CPU send » représente la demande en UC. La métrique de compteur `CPU used by this session` représente la quantité d'UC utilisée par les sessions Oracle. Vous pouvez comparer la valeur de « CPU send » à la métrique de compteur `CPU used by this session`. Lorsque la demande en UC est supérieure à la quantité d'UC utilisée, les sessions sont en attente du temps UC.

Compteur	Type	Unité	Métrique
Quantité d'UC utilisée par cette session	User	Sessions actives	Quantité d'UC utilisée par cette session
SQL*Net roundtrips to/from client	User	Allers-retours par seconde	db.User.SQL*Net roundtrips to/from client
Bytes received via SQL*Net from client	User	Octets par seconde	db.User.bytes received via SQL*Net from client
User commits	User	Validations par seconde	db.User.user commits
Logons cumulative	User	Connexions par seconde	db.User.logons cumulative
User calls	User	Appels par seconde	db.User.user calls
Bytes sent via SQL*Net to client	User	Octets par seconde	db.User.bytes sent via SQL*Net to client
User rollbacks	User	Restaurations par seconde	db.User.user rollbacks
Redo size	Redo	Octets par seconde	db.Redo.redo size
Parse count (total)	SQL	Analyses par seconde	db.SQL.parse count (total)
Parse count (hard)	SQL	Analyses par seconde	db.SQL.parse count (hard)
Table scan rows gotten	SQL	Lignes par seconde	db.SQL.table scan rows gotten
Sorts (memory)	SQL	Tris par seconde	db.SQL.sorts (memory)
Sorts (disk)	SQL	Tris par seconde	db.SQL.sorts (disk)
Sorts (rows)	SQL	Tris par seconde	db.SQL.sorts (rows)
Physical read bytes	Cache	Octets par seconde	db.Cache.physical read bytes
DB block gets	Cache	Blocs par seconde	db.Cache.db block gets
DBWR checkpoints	Cache	Points de contrôle par minute	db.Cache.DBWR checkpoints
Physical reads	Cache	Lectures par seconde	db.Cache.physical reads
Consistent gets from cache	Cache	Obtentions par seconde	db.Cache.consistent gets from cache

Compteur	Type	Unité	Métrique
DB block gets from cache	Cache	Obtentions par seconde	db.Cache.db block gets from cache
Consistent gets	Cache	Obtentions par seconde	db.Cache.consistent gets

Compteurs d'Analyse des performances pour Amazon RDS for PostgreSQL

Les compteurs de base de données suivants sont disponibles avec l'Analyse des performances pour Amazon RDS for PostgreSQL.

Rubriques

- Compteurs natifs pour Amazon RDS for PostgreSQL (p. 449)
- Compteurs non natifs pour Amazon RDS for PostgreSQL (p. 450)

Compteurs natifs pour Amazon RDS for PostgreSQL

La section Viewing Statistics de la documentation PostgreSQL fournit les définitions de ces métriques natives.

Compteur	Type	Unité	Métrique
blks_hit	Cache	Blocs par seconde	db.Cache.blks_hit
buffers_alloc	Cache	Blocs par seconde	db.Cache.buffers_alloc
buffers_checkpoint	Checkpoint	Blocs par seconde	db.Checkpoint.buffers_checkpoint
checkpoint_sync_time	Checkpoint	Millisecondes par point de contrôle	db.Checkpoint.checkpoint_sync_time
checkpoint_write_time	Checkpoint	Millisecondes par point de contrôle	db.Checkpoint.checkpoint_write_time
checkpoints_req	Checkpoint	Points de contrôle par minute	db.Checkpoint.checkpoints_req
checkpoints_timed	Checkpoint	Points de contrôle par minute	db.Checkpoint.checkpoints_timed
maxwritten_clean	Checkpoint	Arrêts de nettoyage Bgwriter par minute	db.Checkpoint.maxwritten_clean
deadlocks	Concurrency	Blocages par minute	db.Concurrency.deadlocks
blk_read_time	E/S	Millisecondes	db.IO.blk_read_time
blks_read	E/S	Blocs par seconde	db.IO.blks_read
buffers_backend	E/S	Blocs par seconde	db.IO.buffers_backend
buffers_backend_fsync	E/S	Blocs par seconde	db.IO.buffers_backend_fsync

Compteur	Type	Unité	Métrique
buffers_clean	E/S	Blocs par seconde	db.IO.buffers_clean
tup_deleted	SQL	Tuples par seconde	db.SQL.tup_deleted
tup_fetched	SQL	Tuples par seconde	db.SQL.tup_fetched
tup_inserted	SQL	Tuples par seconde	db.SQL.tup_inserted
tup_returned	SQL	Tuples par seconde	db.SQL.tup_returned
tup_updated	SQL	Tuples par seconde	db.SQL.tup_updated
temp_bytes	Temp	Octets par seconde	db.Temp.temp_bytes
temp_files	Temp	Fichiers par 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	Validations par seconde	db.Transactions.xact_commit
xact_rollback	Transactions	Restaurations par seconde	db.Transactions.xact_rollback
numbackends	User	Connexions	db.User.numbackends
archived_count	Journal WAL (Write-ahead log)	Fichiers par minute	db.WAL.archived_count
archive_failed_count	WAL	Fichiers par minute	db.WAL.archive_failed_count

Compteurs non natifs pour Amazon RDS for PostgreSQL

Les métriques de compteur non natif sont des compteurs définis par Amazon RDS. Une métrique non native peut être obtenue avec une requête spécifique. Il peut également s'agir d'une métrique dérivée, pour laquelle deux compteurs natifs ou plus sont utilisés dans les calculs de rapport, de taux d'accès ou de latences.

Compteur	Type	Métrique	Description	Définition
checkpoint_sync_latency	Checkpoint	db.Checkpoint.checkpoint_sync_latency	Durée totale consacrée à la partie du traitement de point de contrôle où les fichiers sont synchronisés sur le disque.	`checkpoint_sync_time / (checkpoints_timed + checkpoints_req)`
checkpoint_write_latency	Checkpoint	db.Checkpoint.checkpoint_write_latency	Durée totale consacrée à la partie du traitement de point de contrôle où les fichiers sont écrits sur le disque.	`checkpoint_write_time / (checkpoints_timed + checkpoints_req)`
read_latency	E/S	db.IO.read_latency	Durée consacrée à la lecture des blocs de fichier de données par	`blk_read_time / blks_read`

Compteur	Type	Métrique	Description	Définition
			les backends dans cette instance.	

Récupération de données avec l'API Performance Insights

L'API Amazon RDS Performance Insights offre une visibilité sur les performances de votre instance RDS lorsque Performance Insights est activé pour les types de moteurs pris en charge. Amazon CloudWatch Logs fournit une source officielle pour les métriques de surveillance vendues pour les services AWS. Performance Insights offre une vue spécifique d'un domaine de la charge de base de données mesurée en tant que moyenne des sessions activés et fournies aux utilisateurs de l'API sous la forme d'un jeu de données temporel bidimensionnel. La dimension temporelle des données offre des données de charge de base de données pour chaque point dans le temps de la plage de temps interrogée. Chaque point dans te temps décompose la charge globale par rapport aux dimensions demandées, par exemple `SQL`, `Wait-event`, `User` ou `Host`, mesurée à ce point dans le temps.

Amazon RDS Performance Insights surveille votre instance de base de données Amazon RDS pour vous permettre d'analyser les performances de votre base de données et de résoudre les problèmes associés. Vous pouvez consulter les données de Performance Insights dans AWS Management Console. Performance Insights fournit également une API publique qui vous permet d'interroger vos propres données. L'API peut être utilisée pour décharger les données dans une base de données, ajouter des données Performance Insights à des tableaux de bord de surveillance existants, ou créer des outils de surveillance. Pour utiliser l'API Performance Insights, activez Performance Insights sur l'une de vos instances de base de données Amazon RDS. Pour de plus amples informations sur l'activation de Performance Insights, veuillez consulter Activation et désactivation de Performance Insights (p. 413).

L'API Performance Insights fournit les opérations suivantes.

Opération Performance Insights	Commande de l'AWS CLI	Description
`DescribeDimensionKeys`	`aws pi describe-dimension-keys`	Récupère les N premières clés de dimension d'une mesure sur une période spécifique.
`GetResourceMetrics`	`aws pi get-resource-metrics`	Récupère les mesures Performance Insights d'un ensemble de sources de données, au cours d'une période. Vous pouvez fournir des groupes de dimensions et des dimensions spécifiques, ainsi que des critères d'agrégation et de filtrage, pour chaque groupe.

Pour de plus amples informations sur l'API Performance Insights, veuillez consulter la Référence d'API Amazon RDS Performance Insights.

AWS CLI pour Performance Insights

Vous pouvez consulter les données de Performance Insights à l'aide d'AWS CLI. Vous pouvez obtenir de l'aide sur les commandes AWS CLI relatives à Performance Insights en saisissant le code suivant sur la ligne de commande.

```
aws pi help
```

Si AWS CLI n'est pas installé, veuillez consulter Installation d'AWS Command Line Interface dans le Guide de l'utilisateur d'AWS CLI pour de plus amples informations sur son installation.

Récupération de métriques de série chronologique

L'opération `GetResourceMetrics` récupère une ou plusieurs métriques de série chronologique à partir des données de Performance Insights. `GetResourceMetrics` exige une métrique et une période, et renvoie une réponse contenant la liste des points de données.

Par exemple, AWS Management Console utilise `GetResourceMetrics` à deux endroits dans le tableau de bord de Performance Insights. `GetResourceMetrics` est utilisé pour renseigner le graphique Counter Metrics (Métriques de compteur) et dans le graphique Database Load (Charge de base de données), comme illustré dans l'image ci-dessous.

Toutes les métriques renvoyées par `GetResourceMetrics` sont des métriques de série chronologique standard, à une exception près. L'exception est `db.load`, qui est la métrique principale de Performance Insights. Elle apparaît dans le graphique Database Load (Charge de base de données). La métrique `db.load` est différente des autres métriques de série chronologique, car vous pouvez la décomposer en sous-composants appelés dimensions. Dans l'image précédente, `db.load` est décomposé et regroupé en fonction des états d'attente qui constituent `db.load`.

> **Note**
>
> `GetResourceMetrics` peut également renvoyer la métrique `db.sampleload`, mais la métrique `db.load` est appropriée dans la plupart des cas.

Pour de plus amples informations sur les métriques de compteur renvoyées par `GetResourceMetrics`, veuillez consulter Personnalisation du tableau de bord de Performance Insights (p. 440).

Les calculs suivants sont pris en charge pour les métriques :

- Moyenne – Moyenne de la métrique sur une période. Ajoutez `.avg` au nom de la métrique.
- Minimum – Valeur minimale de la métrique sur une période. Ajoutez `.min` au nom de la métrique.

- Maximum – Valeur maximale de la métrique sur une période. Ajoutez `.max` au nom de la métrique.
- Somme – Somme des valeurs de la métrique sur une période. Ajoutez `.sum` au nom de la métrique.
- Nombre échantillon – Nombre de fois où la métrique a été collectée sur une période. Ajoutez `.sample_count` au nom de la métrique.

Par exemple, supposons qu'une métrique soit collectée pendant 300 secondes (5 minutes) et qu'elle soit collectée une fois toutes les minutes. Les valeurs pour chaque minute sont 1, 2, 3, 4 et 5. Dans ce cas, les calculs suivants sont renvoyés :

- Moyenne – 3
- Minimum – 1
- Maximum – 5
- Somme – 15
- Nombre échantillon – 5

Pour de plus amples informations sur l'utilisation de la commande AWS CLI `get-resource-metrics`, veuillez consulter `get-resource-metrics`.

Pour l'option `--metric-queries`, spécifiez une ou plusieurs requêtes pour lesquelles vous souhaitez obtenir les résultats. Chaque requête se compose d'un paramètre `Metric` obligatoire et des paramètres `GroupBy` et `Filter` facultatifs. Voici un exemple de spécification de l'option `--metric-queries`.

```
{
   "Metric": "string",
   "GroupBy": {
     "Group": "string",
     "Dimensions": ["string", ...],
     "Limit": integer
   },
   "Filter": {"string": "string"
     ...}
}
```

Exemples AWS CLI pour Performance Insights

Les exemples suivants utilisent AWS CLI pour Performance Insights.

Rubriques

- Récupération de métriques de compteur (p. 453)
- Récupération de la charge de base de données moyenne pour les principaux événements d'attente (p. 456)
- Récupération de la charge de base de données moyenne pour les principales instructions SQL (p. 458)
- Récupération de la charge de base de données moyenne filtrée par instruction SQL (p. 461)

Récupération de métriques de compteur

L'image suivante illustre deux graphiques de métriques de compteur dans AWS Management Console.

L'exemple suivant décrit comment collecter les mêmes données utilisées par AWS Management Console pour générer les deux graphiques Counter Metrics (Métriques de compteur).

Pour Linux, macOS ou 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"}]'
```

Pour 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"}]'
```

Vous pouvez également simplifier la lecture d'une commande en spécifiant un fichier pour l'option `--metrics-query`. L'exemple suivant utilise un fichier nommé query.json pour l'option. Le contenu du fichier est le suivant.

```
[
    {
        "Metric": "os.cpuUtilization.user.avg"
    },
    {
        "Metric": "os.cpuUtilization.idle.avg"
```

```
    }
]
```

Exécutez la commande suivante pour utiliser le fichier.

Pour Linux, macOS ou 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
```

Pour 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
```

L'exemple précédent spécifie les valeurs suivantes pour les options :

- `--service-type` – `RDS` pour Amazon RDS
- `--identifier` – ID de ressource de l'instance de base de données
- `--start-time` et `--end-time` – Valeurs `DateTime` conformes à l'ISO 8601 pour la période à interroger, avec plusieurs formats pris en charge

L'interrogation se déroule pendant un intervalle d'une heure :

- `--period-in-seconds` – `60` pour une requête toutes les minutes
- `--metric-queries` – Tableau de deux requêtes s'appliquant chacune à une métrique.

  Le nom de la métrique utilise des points pour classifier la métrique dans une catégorie utile, l'élément final étant une fonction. Dans l'exemple, la fonction est `avg` pour chaque requête. Comme pour Amazon CloudWatch, les fonctions prises en charge sont `min`, `max`, `total` et `avg`.

La réponse ressemble à ce qui suit.

```
{
    "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
```

La réponse contient les éléments `Identifier`, `AlignedStartTime` et `AlignedEndTime`. Étant donné que la valeur de `--period-in-seconds` était définie sur `60`, les heures de début et de fin ont été arrondies à la minute près. Si `--period-in-seconds` était défini sur `3600`, les heures de début et de fin auraient été arrondies à l'heure près.

L'élément `MetricList` dans la réponse comporte un certain nombre d'entrées, chacune associée à une entrée `Key` et `DataPoints`. Chaque élément `DataPoint` comporte une entrée `Timestamp` et `Value`. Chaque liste `Datapoints` répertorie 60 points de données, car les requêtes sont exécutées toutes les minutes pendant une heure, avec `Timestamp1/Minute1`, `Timestamp2/Minute2`, etc. jusqu'à `Timestamp60/Minute60`.

Étant donné que la requête s'applique à deux métriques de compteur différentes, `MetricList` contient deux éléments.

Récupération de la charge de base de données moyenne pour les principaux événements d'attente

L'exemple suivant illustre la même requête utilisée par AWS Management Console pour générer un graphique en aires empilées. Il récupère la valeur de `db.load.avg` sur la dernière heure en divisant la charge conformément aux sept principaux événements d'attente. La commande est identique à la commande de la rubrique Récupération de métriques de compteur (p. 453). Le contenu du fichier query.json est cependant différent :

```
[
```

```
    {
        "Metric": "db.load.avg",
        "GroupBy": { "Group": "db.wait_event", "Limit": 7 }
    }
]
```

Exécutez la commande suivante.

Pour Linux, macOS ou 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
```

Pour 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
```

L'exemple spécifie la métrique de `db.load.avg` et exécute une action `GroupBy` pour les sept principaux événements d'attente. Pour plus de détails sur les valeurs valides pour cet exemple, veuillez consulter DimensionGroup dans la Référence d'API Performance Insights.

La réponse ressemble à ce qui suit.

```
{
    "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": 0.38333333333333336
                },
                {
                    "Timestamp": 1540857780.0, //Minute 3
```

```
                    "Value": 0.26666666666666666
                }
                //... 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
```

Dans cette réponse, `MetricList` comporte huit entrées. Une entrée s'applique à la valeur totale de `db.load.avg` et les sept autres entrées s'appliquent à chacune des valeurs de `db.load.avg` divisées conformément à l'un des sept principaux événements d'attente. Contrairement au premier exemple qui comportait une dimension de regroupement, cet exemple doit définir un élément Key pour chaque regroupement de la métrique. Un seul élément Key peut être associé à chaque métrique, comme dans le cas d'utilisation de la métrique de compteur de base.

Récupération de la charge de base de données moyenne pour les principales instructions SQL

L'exemple suivant regroupe `db.wait_events` par les 10 principales instructions SQL. Il existe deux groupes différents pour les instructions SQL :

- `db.sql` – Instruction SQL complète, telle que `select * from customers where customer_id = 123`
- `db.sql_tokenized` – Instruction SQL tokenisée, telle que `select * from customers where customer_id = ?`

Lors de l'analyse des performances de base de données, il peut s'avérer utile de considérer les instructions SQL dont les paramètres sont différents comme un seul élément logique. Vous pouvez donc utiliser `db.sql_tokenized` lors de l'interrogation. Toutefois, en particulier si vous êtes intéressé par les plans d'explication, il est parfois plus utile d'examiner les instructions SQL complètes avec leurs paramètres, et le regroupement des requêtes par `db.sql`. Il existe une relation parent-enfant entre une instruction SQL tokenisée et une instruction SQL complète, où plusieurs instructions SQL complètes (enfants) sont regroupées sous la même instruction SQL tokenisée (parent).

La commande illustrée dans cet exemple est identique à la commande de la rubrique Récupération de la charge de base de données moyenne pour les principaux événements d'attente (p. 456). Le contenu du fichier query.json est cependant différent :

```
[
    {
        "Metric": "db.load.avg",
        "GroupBy": { "Group": "db.sql_tokenized", "Limit": 10 }
    }
]
```

L'exemple suivant utilise `db.sql_tokenized`.

Pour Linux, macOS ou 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
```

Pour 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
```

Cet exemple procède à une interrogation pendant 24 heures, avec une période en secondes (period-in-seconds) d'une heure.

L'exemple spécifie la métrique de `db.load.avg` et exécute une action `GroupBy` pour les sept principaux événements d'attente. Pour plus de détails sur les valeurs valides pour cet exemple, veuillez consulter DimensionGroup dans la Référence d'API Performance Insights.

La réponse ressemble à ce qui suit.

```
{
    "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
```

Cette réponse comporte 11 entrées dans `MetricList` (1 correspondant au total, les 10 autres correspondant aux principales instructions SQL tokenisées), chaque entrée étant associée à 24 `DataPoints` par heure.

Pour les instructions SQL tokenisées, chaque liste de dimensions répertorie trois entrées :

- `db.sql_tokenized.statement` – Instruction SQL tokenisée.
- `db.sql_tokenized.db_id` – ID de base de données native utilisé pour faire référence à l'instruction SQL, ou ID synthétique généré par Performance Insights si l'ID de base de données native n'est pas disponible. Cet exemple renvoie l'ID synthétique `pi-2372568224`.
- `db.sql_tokenized.id` – ID de la requête dans Analyse des performances.

  Dans AWS Management Console, cet ID se nomme ID de support. Il porte ce nom car l'ID représente les données qu'AWS Support peut examiner pour vous aider à résoudre un problème lié à votre base de données. AWS prend la sécurité et la confidentialité de vos données très au sérieux, et presque toutes les données sont stockées en mode chiffré avec votre clé principale client (CMK) AWS KMS. Personne au sein d'AWS ne peut ainsi consulter ces données. Dans l'exemple précédent, `tokenized.statement` et `tokenized.db_id` sont tous les deux stockés sous forme chiffrée. Si vous rencontrez un problème avec votre base de données, AWS Support peut vous aider en fournissant l'ID de support.

Lors de l'interrogation, il peut s'avérer utile de spécifier une entrée `Group` dans `GroupBy`. Toutefois, pour contrôler les données renvoyées de manière plus précise, spécifier la liste des dimensions. Par exemple, si `db.sql_tokenized.statement` est le seul élément nécessaire, un attribut `Dimensions` peut être ajouté au fichier query.json.

```
[
    {
        "Metric": "db.load.avg",
        "GroupBy": {
            "Group": "db.sql_tokenized",
            "Dimensions":["db.sql_tokenized.statement"],
            "Limit": 10
        }
    }
]
```

Récupération de la charge de base de données moyenne filtrée par instruction SQL

L'image précédente indique qu'une requête particulière est sélectionnée et que le graphique en aires empilées Average active sessions (Sessions actives en moyenne) qui apparaît dans la section supérieure s'y applique. Bien que la requête concerne toujours les sept principaux événements d'attente globaux, la valeur de la réponse est filtrée. Le filtre permet à la requête de prendre uniquement en compte les sessions qui correspondent à un filtre en particulier.

La requête d'API correspondante illustrée dans cet exemple est identique à la commande de la rubrique Récupération de la charge de base de données moyenne pour les principales instructions SQL (p. 458). Le contenu du fichier query.json est cependant différent :

```
[
 {
        "Metric": "db.load.avg",
        "GroupBy": { "Group": "db.wait_event", "Limit": 5  },
        "Filter": { "db.sql_tokenized.id": "AKIAIOSFODNN7EXAMPLE" }
    }
]
```

Pour Linux, macOS ou 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
```

Pour 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
```

La réponse ressemble à ce qui suit.

```
{
    "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
```

Dans cette réponse, toutes les valeurs sont filtrées selon la contribution de l'instruction SQL tokenisée AKIAIOSFODNN7EXAMPLE spécifiée dans le fichier query.json. Les éléments Key peuvent également suivre un ordre différent d'une requête sans filtre, car ils correspondent aux cinq principaux événements d'attente qui ont affecté l'instruction SQL filtrée.

Métriques Performance Insights publiées dans Amazon CloudWatch

Performance Insights publie automatiquement les métriques dans Amazon CloudWatch. Les mêmes données peuvent être interrogées à partir de Performance Insights, mais le fait que les métriques figurent dans CloudWatch facilite l'ajout d'alarmes CloudWatch, ainsi que l'ajout des métriques à des tableaux de bord CloudWatch existants.

Métrique	Description
DBLoad	Nombre de sessions actives pour le moteur de base de données. Vous souhaitez généralement obtenir les données relatives au nombre moyen de sessions actives. Dans Performance Insights, ces données sont interrogées sous la forme `db.load.avg`.
DBLoadCPU	Nombre de sessions actives dans lesquelles le type d'événement d'attente est CPU (UC). Dans Performance Insights, ces données sont interrogées sous la forme `db.load.avg`, filtrées par le type d'événement d'attente `CPU`.
DBLoadNonCPU	Nombre de sessions actives dans lesquelles le type d'événement d'attente n'est pas CPU (UC).

> **Note**
>
> Ces métriques ne sont publiées sur CloudWatch qu'en cas de chargement sur l'instance de bases de données.

Vous pouvez examiner ces métriques à l'aide de la console CloudWatch de l'AWS CLI ou de l'API CloudWatch.

Par exemple, vous pouvez obtenir les statistiques pour la métrique `DBLoad` en exécutant la commande get-metric-statistics.

```
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
```

Cet exemple génère une sortie similaire à la suivante.

```
{
  "Datapoints": [
  {
  "Timestamp": "2018-07-19T21:30:00Z",
  "Unit": "None",
  "Average": 2.1
  },
  {
```

```
"Timestamp": "2018-07-19T21:34:00Z",
"Unit": "None",
"Average": 1.7
},
{
"Timestamp": "2018-07-19T21:35:00Z",
"Unit": "None",
"Average": 2.8
},
{
"Timestamp": "2018-07-19T21:31:00Z",
"Unit": "None",
"Average": 1.5
},
{
"Timestamp": "2018-07-19T21:32:00Z",
"Unit": "None",
"Average": 1.8
},
{
"Timestamp": "2018-07-19T21:29:00Z",
"Unit": "None",
"Average": 3.0
},
{
"Timestamp": "2018-07-19T21:33:00Z",
"Unit": "None",
"Average": 2.4
}
],
"Label": "DBLoad"
}
```


Pour de plus amples informations sur CloudWatch, veuillez consulter Qu'est-ce qu'Amazon CloudWatch ? dans le Guide de l'utilisateur Amazon CloudWatch.

Journalisation des appels d'Analyse des performances à l'aide d'AWS CloudTrail

Performance Insights est intégré à AWS CloudTrail, un service qui fournit un enregistrement des actions réalisées par un utilisateur, un rôle ou un service AWS dans Performance Insights. CloudTrail capture tous les appels d'API pour Performance Insights en tant qu'événements. Cette capture inclut les appels de la console Amazon RDS et les appels de code aux opérations de l'API Performance Insights.

Si vous créez un journal de suivi, vous pouvez activer la diffusion en continu des événements CloudTrail dans un compartiment Amazon S3, y compris les événements concernant l'Analyse des performances. Si vous ne configurez pas de journal de suivi, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Event history (Historique des événements). Grâce aux données collectées par CloudTrail, vous pouvez déterminer certaines informations. Ces informations incluent la demande qui a été envoyée à l'Analyse des performances, l'adresse IP à partir de laquelle la demande a été effectuée, l'auteur de la demande et sa date. Elles comprennent également des détails supplémentaires.

Pour en savoir plus sur CloudTrail, consultez AWS CloudTrail User Guide.

Utilisation des informations d'Analyse des performances dans CloudTrail

CloudTrail est activé sur votre compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans l'Analyse des performances, cette activité est enregistrée dans un événement CloudTrail avec

d'autres événements de service AWS dans la console CloudTrail, dans Event history (Historique des événements). Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte AWS. Pour de plus amples informations, veuillez consulter Affichage des événements avec l'historique des événements CloudTrail dans le AWS CloudTrail User Guide.

Pour un enregistrement continu des événements dans votre compte AWS, y compris des événements concernant l'Analyse des performances, créez un journal de suivi. Une journal de suivi permet à CloudTrail de livrer les fichiers journaux dans un compartiment Amazon S3. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions AWS. Le journal de suivi consigne les événements de toutes les régions AWS dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres services AWS pour analyser plus en profondeur les données d'événement collectées dans les journaux CloudTrail et agir sur celles-ci. Pour de plus amples informations, veuillez consulter les rubriques suivantes dans le AWS CloudTrail User Guide :

- Présentation de la création d'un journal de suivi
- Intégrations et services pris en charge par CloudTrail
- Configuration des Notifications de Amazon SNS pour CloudTrail
- Réception de fichiers journaux CloudTrail de plusieurs régions et Réception de fichiers journaux CloudTrail de plusieurs comptes

Toutes les opérations de Performance Insights sont consignées par CloudTrail et documentées dans la Référence d'API Performance Insights. Par exemple, les appels aux opérations `DescribeDimensionKeys` et `GetResourceMetrics` génèrent des entrées dans les fichiers journaux CloudTrail.

Chaque événement ou entrée du journal contient des informations sur la personne qui a généré la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou IAM.
- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré.
- Si la requête a été effectuée par un autre service AWS.

Pour plus d'informations, consultez la section Élément userIdentity CloudTrail.

Entrées du fichier journal Performance Insights

Un journal de suivi est une configuration qui active la livraison d'événements en tant que fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Les fichiers journaux CloudTrail contiennent une ou plusieurs entrées de journal. Un événement représente une demande individuelle d'une source quelconque. Chaque événement comprend les informations sur l'opération demandée, la date et l'heure de l'opération, les paramètres de la demande, etc. Les fichiers journaux CloudTrail ne constituent pas une pile ordonnée retraçant les appels d'API publics. Par conséquent, ils ne suivent aucun ordre précis.

L'exemple suivant montre une entrée de journal CloudTrail qui illustre l'opération `GetResourceMetrics`.

```
{
    "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"
}
```


Utilisation de la notification d'événement Amazon RDS

Rubriques

- Catégories d'événements et messages d'événements Amazon RDS (p. 469)
- Abonnement à la notification d'événement Amazon RDS (p. 478)
- Liste des abonnements aux notifications d'événements Amazon RDS (p. 480)
- Modification d'un abonnement aux notifications d'événements Amazon RDS (p. 481)
- Ajout d'un identifiant source à un abonnement aux notifications d'événements Amazon RDS (p. 482)
- Suppression d'un identifiant source d'un abonnement aux notifications d'événements Amazon RDS (p. 483)
- Affichage des catégories aux notifications d'événements Amazon RDS (p. 484)
- Suppression d'un abonnement aux notifications d'événements Amazon RDS (p. 485)

Amazon RDS utilise Amazon Simple Notification Service (Amazon SNS) pour adresser une notification lorsqu'un événement Amazon RDS se produit. Ces notifications peuvent être sous l'une des formes prises en charge par Amazon SNS pour une région AWS, telles qu'un e-mail, un SMS ou un appel à un point de terminaison HTTP.

Amazon RDS regroupe ces événements en catégories auxquelles vous pouvez vous abonner afin d'être informé lorsqu'un événement de cette catégorie se produit. Vous pouvez vous abonner à une catégorie d'événement pour une instance de base de données, un instantané de base de donnéesun groupe de paramètres de base de données ou un groupe de sécurité de base de données. Par exemple, si vous vous abonnez à la catégorie de sauvegarde d'une instance de base de données donnée, vous recevez une notification chaque fois que survient un événement lié à la sauvegarde et qui affecte l'instance de base de

données. Si vous vous abonnez à la catégorie de modification de configuration pour un groupe de sécurité de base de données, vous recevez une notification en cas de modification de ce groupe. Vous recevez également une notification en cas de modification d'un abonnement à une notification d'événements.

Les notifications d'événements sont envoyées aux adresses que vous fournissez lorsque vous créez l'abonnement. Il se peut que vous souhaitiez créer plusieurs abonnements différents, tel qu'un abonnement recevant toutes les notifications d'événements et un autre incluant uniquement les événements critiques pour vos instances de base de données de production. Vous pouvez facilement désactiver la notification sans supprimer un abonnement en définissant l'option Activé sur Non dans la console Amazon RDS, ou en définissant le paramètre `Enabled` sur `false` à l'aide de l'AWS CLI ou de l'API Amazon RDS.

> **Important**
>
> Amazon RDS ne garantie pas l'ordre des événements envoyés dans un flux d'événements. L'ordre des événements est susceptible de changer.

> **Note**
>
> Les notifications d'événements Amazon RDS à l'aide de SMS sont actuellement disponibles pour les ARN (Amazon Resource Name) de rubrique et les ressources Amazon RDS dans la région Région USA Est (Virginie du Nord). Pour de plus amples informations sur l'utilisation des SMS avec SNS, veuillez consulter Envoi et réception de notifications par SMS à l'aide d'Amazon SNS dans le Manuel du développeur Amazon Simple Notification Service.

Amazon RDS utilise l'ARN d'une rubrique Amazon SNS pour identifier chaque abonnement. La console Amazon RDS crée l'ARN lorsque vous créez l'abonnement. Si vous utilisez l'interface de ligne de commande ou l'API, vous devez créer l'ARN à l'aide de la console Amazon SNS ou de l'API Amazon SNS quand vous créez un abonnement.

La facturation de la notification d'événement Amazon RDS s'effectue via Amazon Simple Notification Service (Amazon SNS). Des frais Amazon SNS s'appliquent quand la notification d'événement est utilisée. Pour plus d'informations sur la tarification Amazon SNS, consultez la section Tarification Amazon Simple Notification Service.

La procédure d'abonnement à une notification d'événement Amazon RDS est la suivante :

1. Créez un abonnement à une notification d'événement Amazon RDS à l'aide de la console Amazon RDS, de l'AWS CLI ou de l'API.
2. Amazon RDS envoie un e-mail d'approbation ou un SMS aux adresses que vous avez fournies avec votre abonnement. Pour valider votre abonnement, choisissez le lien dans la notification qui vous a été envoyée.
3. Lorsque vous avez confirmé l'abonnement, le statut de celui-ci est mis à jour dans la section My Event Subscriptions (Mes abonnements d'événements) de la console Amazon RDS.
4. Vous commencez alors à recevoir des notifications d'événements.

> **Note**
>
> Lorsqu'Amazon SNS envoie une notification à un point de terminaison HTTP ou HTTPS abonné, le corps du message POST envoyé au point de terminaison contient un document JSON. Pour de plus amples informations, veuillez consulter Formats de message et JSON Amazon SNS dans le Manuel du développeur Amazon Simple Notification Service.
> Vous pouvez utiliser AWS Lambda pour traiter les notifications d'événements à partir d'une instance de base de données. Pour de plus amples informations, veuillez consulter Utilisation de AWS Lambda avec Amazon RDS dans le manuel du développeur AWS Lambda.

La section suivante répertorie l'ensemble des catégories et événements dont vous pouvez être informé. Elle contient aussi des informations sur l'abonnement et sur l'utilisation des abonnements aux événements Amazon RDS.

Catégories d'événements et messages d'événements Amazon RDS

Amazon RDS génère un nombre significatif d'événements dans les catégories auxquelles vous pouvez vous abonner à l'aide de la console Amazon RDS de l'AWS CLI ou de l'API. Chaque catégorie s'applique à un type source, qui peut être une instance de base de données, un instantané de base de données, un groupe de sécurité de base de données ou un groupe de paramètres de base de données.

Le tableau suivant recense la catégorie d'événement et la liste des événements lorsqu'une instance de base de données est le type source.

Catégorie	ID d'événement Amazon RDS	Description
disponibilité	RDS-EVENT-0006	L'instance de base de données a redémarré.
disponibilité	RDS-EVENT-0004	L'instance de base de données s'est arrêtée.
disponibilité	RDS-EVENT-0022	Une erreur s'est produite lors du redémarrage de MySQL ou MariaDB.
sauvegarde	RDS-EVENT-0001	Sauvegarde de l'instance de base de données.
sauvegarde	RDS-EVENT-0002	Sauvegarde de l'instance de base de données terminée.
modification de configuration	RDS-EVENT-0009	L'instance de base de données a été ajoutée à un groupe de sécurité.
modification de configuration	RDS-EVENT-0024	L'instance de base de données est en cours de conversion en une instance de base de données Multi-AZ.
modification de configuration	RDS-EVENT-0030	L'instance de base de données est en cours de conversion en une instance de base de données mono-AZ.
modification de configuration	RDS-EVENT-0012	Application de la modification à la classe d'instance de base de données.
modification de configuration	RDS-EVENT-0018	Les paramètres de stockage de l'instance de base de données sont en cours de modification.
modification de configuration	RDS-EVENT-0011	Un groupe de paramètres de l'instance de base de données a changé.
modification de configuration	RDS-EVENT-0092	Un groupe de paramètres de l'instance de base de données a terminé sa mise à jour.
modification de configuration	RDS-EVENT-0028	Les sauvegardes automatiques de l'instance de base de données ont été désactivées.
modification de configuration	RDS-EVENT-0032	Les sauvegardes automatiques de l'instance de base de données ont été activées.
modification de configuration	RDS-EVENT-0033	Il existe [count] utilisateurs dont le nom correspond à celui de l'utilisateur maître. Les utilisateurs non liés à un hôte spécifique ont été réinitialisés.

Catégorie	ID d'événement Amazon RDS	Description
modification de configuration	RDS-EVENT-0025	L'instance de base de données a été convertie en une instance de base de données Multi-AZ.
modification de configuration	RDS-EVENT-0029	L'instance de base de données a été convertie en une instance de base de données mono-AZ.
modification de configuration	RDS-EVENT-0014	La classe d'instance de base de données de l'instance de base de données a été modifiée.
modification de configuration	RDS-EVENT-0017	Les paramètres de stockage de l'instance de base de données ont été modifiés.
modification de configuration	RDS-EVENT-0010	L'instance de base de données a été supprimée d'un groupe de sécurité.
modification de configuration	RDS-EVENT-0016	Le mot de passe principal de l'instance de base de données a été réinitialisé.
modification de configuration	RDS-EVENT-0067	Une tentative de réinitialisation du mot de passe principal de l'instance de base de données a échoué.
modification de configuration	RDS-EVENT-0078	La configuration Supervision améliorée a été modifiée.
création	RDS-EVENT-0005	Instance de base de données créée.
suppression	RDS-EVENT-0003	L'instance de base de données a été supprimée.
basculement	RDS-EVENT-0034	Amazon RDS ne tente pas le basculement demandé, car un basculement s'est récemment produit sur l'instance de base de données.
basculement	RDS-EVENT-0013	Un basculement Multi-AZ ayant entraîné la promotion d'une instance de secours a commencé.
basculement	RDS-EVENT-0015	Un basculement Multi-AZ ayant entraîné la promotion d'une instance de secours est terminé. Le transfert du DNS vers la nouvelle instance de base de données principale peut prendre plusieurs minutes.
basculement	RDS-EVENT-0065	L'instance a récupéré à partir d'un basculement partiel.
basculement	RDS-EVENT-0049	Un basculement Multi-AZ est terminé.
basculement	RDS-EVENT-0050	Une activation Multi-AZ a commencé après une récupération d'instance réussie.
basculement	RDS-EVENT-0051	Une activation Multi-AZ est terminée. Votre base de données doit être accessible maintenant.
échec	RDS-EVENT-0031	L'instance de base de donnée a échoué en raison d'une configuration incompatible ou d'un problème de stockage sous-jacent. Commencez une restauration à un instant dans le passé pour l'instance de base de données.

Catégorie	ID d'événement Amazon RDS	Description
échec	RDS-EVENT-0036	L'instance de base de données se trouve sur un réseau non compatible. Certains des ID de sous-réseau spécifiés ne sont pas valides ou n'existent pas.
échec	RDS-EVENT-0035	L'instance de base de données a des paramètres non valides. Par exemple, si l'instance de base de données n'a pas pu démarrer, un paramètre lié à la mémoire étant défini avec une valeur trop élevée pour cette classe d'instance, l'action du client consiste à modifier le paramètre et à redémarrer l'instance de base de données.
échec	RDS-EVENT-0058	Erreur lors de la création du compte d'utilisateur Statspack PERFSTAT. Supprimez le compte avant d'ajouter l'option Statspack.
échec	RDS-EVENT-0079	La supervision améliorée ne peut pas être activée sans le rôle IAM de supervision améliorée. Pour plus d'informations sur la création du rôle IAM de supervision améliorée, consultez Pour créer un rôle IAM pour la surveillance améliorée Amazon RDS (p. 395).
échec	RDS-EVENT-0080	La supervision améliorée a été désactivée en raison d'une erreur lors de la modification de configuration. Il est probable que le rôle IAM de supervision améliorée ne soit pas configuré correctement. Pour plus d'informations sur la création du rôle IAM de supervision améliorée, consultez Pour créer un rôle IAM pour la surveillance améliorée Amazon RDS (p. 395).
échec	RDS-EVENT-0081	Le rôle IAM que vous utilisez pour accéder à votre compartiment Amazon S3 pour la sauvegarde et la restauration natives SQL Server est mal configuré. Pour plus d'informations, consultez Configuration pour les sauvegarde et restauration natives (p. 637).
stockage faible	RDS-EVENT-0089	L'instance de base de données a consommé plus de 90 % de son stockage alloué. Vous pouvez surveiller l'espace de stockage pour une instance de base de données à l'aide de la métrique Free Storage Space (Espace de stockage libre). Pour plus d'informations, consultez Affichage des métriques d'instances de base de données (p. 384).

Catégorie	ID d'événement Amazon RDS	Description
stockage faible	RDS-EVENT-0007	L'espace de stockage alloué pour l'instance de base de données a été épuisé. Pour résoudre le problème, vous devez allouer un stockage supplémentaire pour l'instance de base de données. Pour plus d'informations, consultez la FAQ RDS. Vous pouvez surveiller l'espace de stockage pour une instance de base de données à l'aide de la métrique Free Storage Space (Espace de stockage libre). Pour plus d'informations, consultez Affichage des métriques d'instances de base de données (p. 384).
maintenance	RDS-EVENT-0026	La maintenance hors connexion de l'instance de base de données est en cours. L'instance de base de données n'est pas disponible actuellement.
maintenance	RDS-EVENT-0027	La maintenance hors connexion de l'instance de base de données est terminée. L'instance de base de données est désormais disponible.
maintenance	RDS-EVENT-0047	L'application des correctifs de l'instance de base de données s'est terminée.
maintenance	RDS-EVENT-0155	Une mise à niveau de version mineure du moteur de base de données est disponible pour l'instance de base de données.
notification	RDS-EVENT-0044	Notification émise par l'opérateur. Pour plus d'informations, consultez le message de l'événement.
notification	RDS-EVENT-0048	L'application des correctifs de l'instance de base de données a été retardée.
notification	RDS-EVENT-0054	Le moteur de stockage MySQL que vous utilisez n'est pas InnoDB, lequel est le moteur de stockage MySQL recommandé pour Amazon RDS. Pour plus d'informations sur les moteurs de stockage MySQL, consultez Moteurs de stockage pris en charge pour MySQL sur Amazon RDS.
notification	RDS-EVENT-0055	Le nombre de tables de votre instance de base de données dépasse les bonnes pratiques recommandées pour Amazon RDS. Réduisez le nombre de tables de votre instance de base de données. Pour plus d'informations sur les bonnes pratiques recommandées, consultez Directives opérationnelles de base Amazon RDS (p. 135).

Catégorie	ID d'événement Amazon RDS	Description
notification	RDS-EVENT-0056	Le nombre de bases de données de votre instance de base de données dépasse les bonnes pratiques recommandées pour Amazon RDS. Réduisez le nombre de bases de données de votre instance de base de données. Pour plus d'informations sur les bonnes pratiques recommandées, consultez Directives opérationnelles de base Amazon RDS (p. 135).
notification	RDS-EVENT-0064	La clé TDE a été inversée. Pour plus d'informations sur les bonnes pratiques recommandées, consultez Directives opérationnelles de base Amazon RDS (p. 135).
notification	RDS-EVENT-0084	Vous avez essayé de convertir une instance de base de données en environnement Multi-AZ, mais elle contient des groupes de fichiers en mémoire qui ne sont pas pris en charge pour plusieurs environnements Multi-AZ. Pour plus d'informations, consultez Déploiements multi-AZ pour Microsoft SQL Server (p. 664).
notification	RDS-EVENT-0087	L'instance de base de données a été arrêtée.
notification	RDS-EVENT-0088	L'instance de base de données a été démarrée.
notification	RDS-EVENT-0154	L'instance de base de données est en cours de démarrage dans la mesure où elle a dépassé le temps maximum autorisé pour son arrêt.
notification	RDS-EVENT-0157	RDS ne peut pas modifier la classe d'instance de base de données car la classe d'instance cible ne peut pas prendre en charge le nombre de bases de données figurant dans l'instance de base de données source. Le message d'erreur suivant apparaît : "The instance has N databases, but after conversion it would only support N" (L'instance comporte N bases de données, mais après la conversion, elle n'en prendrait en charge que N). Pour de plus amples informations, veuillez consulter Limites propres aux instances de bases de données Microsoft SQL Server (p. 594).
notification	RDS-EVENT-0158	L'instance de base de données est dans un état qui ne peut pas être mis à niveau.

Catégorie	ID d'événement Amazon RDS	Description
réplica en lecture	RDS-EVENT-0045	Une erreur s'est produite lors du processus de réplication en lecture. Pour plus d'informations, consultez le message de l'événement. En outre, consultez la section de dépannage pour les réplicas en lecture de votre moteur de base de données. • Résolution d'un problème de réplica en lecture MariaDB (p. 576) • Résolution d'un problème de réplica en lecture SQL Server (p. 663) • Résolution d'un problème de réplica en lecture MySQL (p. 856) • Dépannage des réplicas Oracle (p. 1009) • Dépannage d'un problème de réplica en lecture PostgreSQL (p. 1387)
réplica en lecture	RDS-EVENT-0046	Le réplica en lecture a repris la réplication. Ce message s'affiche lorsque vous créez un réplica en lecture, ou comme message de surveillance lorsque vous confirmez que la réplication fonctionne correctement. Si ce message fait suite à une notification RDS-EVENT-0045, la réplication a repris suite à une erreur ou à un arrêt de la réplication.
réplica en lecture	RDS-EVENT-0057	La réplication sur le réplica en lecture est terminée.
réplica en lecture	RDS-EVENT-0062	La réplication sur le réplica en lecture a été arrêtée manuellement.
réplica en lecture	RDS-EVENT-0063	La réplication sur le réplica en lecture a été réinitialisée.
récupération	RDS-EVENT-0020	La récupération de l'instance de base de données a démarré. Le temps de récupération varie selon la quantité de données à restaurer.
récupération	RDS-EVENT-0021	La récupération de l'instance de base de données est terminée.
récupération	RDS-EVENT-0023	Une sauvegarde manuelle a été demandée, mais Amazon RDS est actuellement en cours de création d'un instantané de base de données. Soumettez à nouveau la demande après que Amazon RDS a terminé l'instantané de base de données.
récupération	RDS-EVENT-0052	La récupération de l'instance Multi-AZ a commencé. Le temps de récupération varie selon la quantité de données à restaurer.
récupération	RDS-EVENT-0053	La récupération de l'instance Multi-AZ est terminée.

Catégorie	ID d'événement Amazon RDS	Description
récupération	RDS-EVENT-0066	L'instance de base de données SQL Server est en train de rétablir son miroir. Les performances seront dégradées tant que le miroir n'est pas restauré. Il a été trouvé une base de données avec un modèle de récupération autre que FULL. Le modèle de récupération a été remodifié en FULL et la récupération de la mise en miroir a démarré. (<dbname>: <recovery model found>[,...])”
restauration	RDS-EVENT-0008	L'instance de base de données a été restaurée à partir d'un instantané de base de données.
restauration	RDS-EVENT-0019	L'instance de base de données a été restaurée à partir d'une sauvegarde à un instant dans le passé.

Le tableau suivant affiche la catégorie d'événement et la liste des événements lorsqu'un groupe de paramètres de base de données est le type source.

Catégorie	ID d'événement RDS	Description
modification de configuration	RDS-EVENT-0037	Le groupe de paramètres a été modifié.

Le tableau suivant affiche la catégorie d'événement et la liste des événements lorsqu'un groupe de sécurité de base de données est le type source.

Catégorie	ID d'événement RDS	Description
modification de configuration	RDS-EVENT-0038	Le groupe de sécurité a été modifié.
échec	RDS-EVENT-0039	Le groupe de sécurité dont [utilisateur] est propriétaire n'existe pas ; l'autorisation pour le groupe de sécurité a été révoquée.

Le tableau suivant affiche la catégorie d'événement et la liste des événements lorsqu'un instantané de base de données est le type source.

Catégorie	ID d'événement RDS	Description
création	RDS-EVENT-0040	Un instantané de base de données manuel est en cours de création.
création	RDS-EVENT-0042	Un instantané de base de données manuel a été créé.
création	RDS-EVENT-0090	Un instantané de base de données automatisé est en cours de création.
création	RDS-EVENT-0091	Un instantané de base de données automatisé a été créé.

Catégorie	ID d'événement RDS	Description
suppression	RDS-EVENT-0041	Un instantané de base de données a été supprimé.
notification	RDS-EVENT-0059	La copie de l'instantané de base de données entre régions [nom de l'instantané de base de données] à partir de la région source [nom de la région] a démarré.
notification	RDS-EVENT-0060	La copie de l'instantané de base de données entre régions [nom de l'instantané de base de données] à partir de la région source [nom de la région] a fini en [durée] minutes.
notification	RDS-EVENT-0061	La copie d'un instantané de base de données entre régions a échoué.
notification	RDS-EVENT-0159	Échec de la tâche d'exportation de l'instantané de bases de données.
notification	RDS-EVENT-0160	La tâche d'exportation de l'instantané de bases de données a été annulée.
notification	RDS-EVENT-0161	La tâche d'exportation de l'instantané de bases de données est terminée.
restauration	RDS-EVENT-0043	Une instance de base de données est en cours de restauration à partir d'un instantané de base de données.

Le tableau suivant affiche la catégorie d'événement et la liste des événements lorsqu'un cluster de base de données Aurora est le type source.

Catégorie	ID d'événement RDS	Description
basculement	RDS-EVENT-0069	Un basculement pour le cluster de base de données a échoué.
basculement	RDS-EVENT-0070	Un basculement pour le cluster de base de données a redémarré.
basculement	RDS-EVENT-0071	Un basculement pour le cluster de base de données s'est terminé.
basculement	RDS-EVENT-0072	Un basculement pour le cluster de base de données a commencé dans la même zone de disponibilité.
basculement	RDS-EVENT-0073	Un basculement pour le cluster de base de données a commencé sur les zones de disponibilité.
échec	RDS-EVENT-0083	Aurora n'a pas pu copier les données de sauvegarde d'un compartiment Amazon S3. Il est probable que les autorisations devant permettre à Aurora d'accéder au compartiment Amazon S3 soient mal configurées. Pour de plus amples informations, veuillez consulter Migration des données d'une base de données MySQL externe vers un cluster de base de données Amazon Aurora MySQL.

Catégorie	ID d'événement RDS	Description
maintenance	RDS-EVENT-0156	Une mise à niveau de version mineure du moteur de base de données est disponible pour le cluster de base de données.
notification	RDS-EVENT-0076	La migration vers un cluster de base de données Aurora a échoué.
notification	RDS-EVENT-0077	Une tentative de conversion d'une table de la base de données source en InnoDB a échoué lors de la migration vers un cluster de base de données Aurora.
notification	RDS-EVENT-0141	Dimensionnement initié pour le cluster de bases de données Aurora Serverless.
notification	RDS-EVENT-0142	Dimensionnement terminé pour le cluster de bases de données Aurora Serverless.
notification	RDS-EVENT-0143	Échec du dimensionnement pour le cluster de bases de données Aurora Serverless.
notification	RDS-EVENT-0144	Pause automatique initiée pour le cluster de bases de données Aurora Serverless.
notification	RDS-EVENT-0145	Pause du cluster de bases de données Aurora Serverless.
notification	RDS-EVENT-0146	Annulation de la pause pour le cluster de bases de données Aurora Serverless.
notification	RDS-EVENT-0147	Reprise initiée pour le cluster de bases de données Aurora Serverless.
notification	RDS-EVENT-0148	Reprise terminée pour le cluster de bases de données Aurora Serverless.
notification	RDS-EVENT-0149	Dimensionnement transparent terminé avec l'option force pour le cluster de bases de données Aurora Serverless. Les connexions peuvent avoir été interrompues en fonction des besoins.
notification	RDS-EVENT-0150	Le cluster de base de données s'est arrêté.
notification	RDS-EVENT-0151	Le cluster de base de données a démarré.
notification	RDS-EVENT-0152	L'arrêt du cluster de base de données a échoué.
notification	RDS-EVENT-0153	Le cluster de base de données est en cours de démarrage car il a dépassé le temps maximal autorisé pour son arrêt.

Le tableau suivant affiche la catégorie d'événement et la liste des événements lorsqu'un instantané de cluster de base de données Aurora est le type source.

Catégorie	ID d'événement RDS	Description
sauvegarde	RDS-EVENT-0074	La création d'un instantané de cluster de base de données manuel a commencé.

Catégorie	ID d'événement RDS	Description
sauvegarde	RDS-EVENT-0075	Un instantané de cluster de base de données manuel a été créé.
notification	RDS-EVENT-0162	Échec de la tâche d'exportation de l'instantané de cluster de bases de données.
notification	RDS-EVENT-0163	La tâche d'exportation de l'instantané de cluster de bases de données a été annulée.
notification	RDS-EVENT-0164	La tâche d'exportation de l'instantané de cluster de bases de données est terminée.
sauvegarde	RDS-EVENT-0168	Création d'instantané de cluster automatisé.
sauvegarde	RDS-EVENT-0169	Instantané de cluster automatisé créé.
création	RDS-EVENT-0170	cluster de bases de données créé.
suppression	RDS-EVENT-0171	cluster de bases de données supprimé.
notification	RDS-EVENT-0172	Cluster de bases de données renommé de [ancien nom de cluster de bases de données] en [nouveau nom de cluster de bases de données].

Abonnement à la notification d'événement Amazon RDS

Vous pouvez créer un abonnement à une notification d'événement Amazon RDS afin de pouvoir être informé quand un événement se produit pour une instance de base de données, un instantané de base de données, un groupe de sécurité de base de données ou un groupe de paramètres de base de données. La solution la plus simple pour créer un abonnement consiste à utiliser la console RDS. Si vous choisissez de créer un abonnement à une notification d'événement à l'aide de l'interface de ligne de commande ou de l'API, vous devez créer une rubrique Amazon Simple Notification Service et vous abonner à cette rubrique avec la console Amazon SNS ou l'API Amazon SNS. Vous devrez également conserver l'Amazon Resource Name (ARN) de la rubrique, car il est utilisé lors de la soumission de commandes de l'interface de ligne de commande ou d'opérations d'API. Pour de plus amples informations sur la création d'une rubrique SNS et sur l'abonnement à cette rubrique, veuillez consulter Mise en route d'Amazon SNS dans le Manuel du développeur d'Amazon Simple Notification Service.

Vous pouvez spécifier le type de source dont vous voulez être informé et la source Amazon RDS qui déclenche l'événement. Ces informations sont définies par SourceType (type de source) et SourceIdentifier (source Amazon RDS générant l'événement). Si vous spécifiez à la fois SourceType et SourceIdentifier, comme `SourceType = db-instance` et `SourceIdentifier = myDBInstance1`, vous recevez tous les événements d'instance de base de données de la source spécifiée. Si vous spécifiez SourceType, mais que vous ne spécifiez pas SourceIdentifier, vous êtes informé des événements de ce type de source pour toutes vos sources Amazon RDS. Si vous ne spécifiez ni SourceType ni SourceIdentifier, vous êtes informé des événements générés à partir de toutes les sources Amazon RDS appartenant à votre compte client.

> **Note**
>
> Les notifications d'événement peuvent prendre jusqu'à cinq minutes pour être livrées.
> La notification d'événement Amazon RDS n'est disponible que pour les rubriques SNS non chiffrées. Si vous spécifiez une rubrique SNS chiffrée, les notifications d'événement ne sont pas envoyées pour la rubrique.

Console

Pour s'abonner à la notification d'événement RDS

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Abonnements aux événements.
3. Dans le volet Abonnements aux événements, choisissez Créer un abonnement aux événements.
4. Dans la boîte de dialogue Créer un abonnement aux événements, exécutez l'une des actions suivantes :

   a. Dans le champ Nom, entrez un nom pour l'abonnement à la notification d'événements.
   b. Pour Envoyez des notifications à, choisissez un ARN Amazon SNS existant pour une rubrique Amazon SNS ou choisissez créer une rubrique pour entrer le nom d'une rubrique et une liste de destinataires.
   c. Pour Type de source, choisissez un type de source.
   d. Choisissez Oui pour activer l'abonnement. Si vous souhaitez créer l'abonnement mais qu'aucune notification ne soit envoyée pour l'instant, choisissez Non.
   e. Selon le type de source que vous avez sélectionné, choisissez les catégories d'événement et les sources pour lesquelles vous souhaitez recevoir des notifications d'événements.
   f. Sélectionnez Create.

La console Amazon RDS indique que l'abonnement est en cours de création.

AWS CLI

Pour vous abonner à la notification d'événement RDS, utilisez la commande `create-event-subscription` de l'AWS CLI. Incluez les paramètres requis suivants :

- `--subscription-name`
- `--sns-topic-arn`

Example

Pour Linux, macOS ou Unix :

```
aws rds create-event-subscription \
    --subscription-name myeventsubscription \
    --sns-topic-arn arn:aws:sns:us-east-1:802#########:myawsuser-RDS \
    --enabled
```

Pour Windows :

```
aws rds create-event-subscription ^
    --subscription-name myeventsubscription ^
    --sns-topic-arn arn:aws:sns:us-east-1:802#########:myawsuser-RDS ^
    --enabled
```

API

Pour vous abonner à la notification d'événement Amazon RDS, appelez la fonction d'API Amazon RDS `CreateEventSubscription`. Incluez les paramètres requis suivants :

- `SubscriptionName`
- `SnsTopicArn`

Liste des abonnements aux notifications d'événements Amazon RDS

Vous pouvez afficher vos abonnements aux notifications d'événement Amazon RDS.

Console

Pour afficher vos abonnements aux notifications d'événements Amazon RDS

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Abonnements aux événements. Le volet Abonnements aux événements affiche tous les abonnements aux notifications d'événements.

AWS CLI

Pour afficher vos abonnements aux notifications d'événements Amazon RDS, utilisez la commande `describe-event-subscriptions` de l'AWS CLI.

Example

L'exemple suivant décrit tous les abonnements aux événements.

```
aws rds describe-event-subscriptions
```

L'exemple suivant décrit l'abonnement `myfirsteventsubscription`.

```
aws rds describe-event-subscriptions --subscription-name myfirsteventsubscription
```

API

Pour afficher vos abonnements aux notifications d'événements Amazon RDS, appelez l'action d'API Amazon RDS `DescribeEventSubscriptions`.

Example

L'exemple de code suivant répertorie jusqu'à 100 abonnements aux événements.

```
https://rds.us-east-1.amazonaws.com/
   ?Action=DescribeEventSubscriptions
   &MaxRecords=100
   &SignatureMethod=HmacSHA256
   &SignatureVersion=4
   &Version=2014-10-31
   &X-Amz-Algorithm=AWS4-HMAC-SHA256
   &X-Amz-Credential=AKIADQKE4SARGYLE/20140428/us-east-1/rds/aws4_request
   &X-Amz-Date=20140428T161907Z
   &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
   &X-Amz-Signature=4208679fe967783a1a149c826199080a066085d5a88227a80c6c0cadb3e8c0d4
```

L'exemple suivant décrit l'abonnement `myfirsteventsubscription`.

```
https://rds.us-east-1.amazonaws.com/
   ?Action=DescribeEventSubscriptions
   &SignatureMethod=HmacSHA256
   &SignatureVersion=4
   &SubscriptionName=myfirsteventsubscription
   &Version=2014-10-31
   &X-Amz-Algorithm=AWS4-HMAC-SHA256
   &X-Amz-Credential=AKIADQKE4SARGYLE/20140428/us-east-1/rds/aws4_request
   &X-Amz-Date=20140428T161907Z
   &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
   &X-Amz-Signature=4208679fe967783a1a149c826199080a066085d5a88227a80c6c0cadb3e8c0d4
```

Modification d'un abonnement aux notifications d'événements Amazon RDS

Une fois que vous avez créé un abonnement, vous pouvez en changer le nom, l'identifiant de la source, les catégories ou l'ARN de la rubrique.

Console

Pour modifier un abonnement aux notifications d'événements Amazon RDS

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Abonnements aux événements.
3. Dans le volet Abonnements aux événements, choisissez l'abonnement que vous voulez modifier, puis choisissez Modifier.
4. Apportez les modifications requises à l'abonnement dans la section Cible ou Source.
5. Choisissez Edit. La console Amazon RDS indique que l'abonnement est en cours de modification.

AWS CLI

Pour modifier un abonnement aux notifications d'événements Amazon RDS, utilisez la commande `modify-event-subscription` de l'AWS CLI. Incluez le paramètre requis suivant :

- `--subscription-name`

Example

Le code suivant active `myeventsubscription`.

Pour Linux, macOS ou Unix :

```
aws rds modify-event-subscription \
    --subscription-name myeventsubscription \
    --enabled
```

Pour Windows :

```
aws rds modify-event-subscription ^
    --subscription-name myeventsubscription ^
    --enabled
```

API

Pour modifier un événement Amazon RDS, appelez l'opération d'API Amazon RDS `ModifyEventSubscription`. Incluez le paramètre requis suivant :

- `SubscriptionName`

Ajout d'un identifiant source à un abonnement aux notifications d'événements Amazon RDS

Vous pouvez ajouter un identifiant source (la source Amazon RDS générant l'événement) à l'abonnement existant.

Console

Vous pouvez facilement ajouter ou supprimer des identificateurs source à l'aide de la console Amazon RDS en les sélectionnant ou en annulant leur sélection lors de la modification d'un abonnement. Pour plus d'informations, consultez Modification d'un abonnement aux notifications d'événements Amazon RDS (p. 481).

AWS CLI

Pour ajouter un identificateur source à un abonnement aux notifications d'événements Amazon RDS, utilisez la commande `add-source-identifier-to-subscription` de l'AWS CLI. Incluez les paramètres requis suivants :

- `--subscription-name`
- `--source-identifier`

Example

L'exemple suivant ajoute l'identifiant source `mysqldb` à l'abonnement `myrdseventsubscription`

Pour Linux, macOS ou Unix :

```
aws rds add-source-identifier-to-subscription \
    --subscription-name myrdseventsubscription \
    --source-identifier mysqldb
```

Pour Windows :

```
aws rds add-source-identifier-to-subscription ^
    --subscription-name myrdseventsubscription ^
    --source-identifier mysqldb
```

API

Pour ajouter un identificateur source à un abonnement aux notifications d'événements Amazon RDS, appelez l'API Amazon RDS `AddSourceIdentifierToSubscription`. Incluez les paramètres requis suivants :

- `SubscriptionName`
- `SourceIdentifier`

Suppression d'un identifiant source d'un abonnement aux notifications d'événements Amazon RDS

Vous pouvez supprimer un identifiant source (la source Amazon RDS générant l'événement) d'un abonnement si vous ne souhaitez plus être informé des événements de cette source.

Console

Vous pouvez facilement ajouter ou supprimer des identificateurs source à l'aide de la console Amazon RDS en les sélectionnant ou en annulant leur sélection lors de la modification d'un abonnement. Pour plus d'informations, consultez Modification d'un abonnement aux notifications d'événements Amazon RDS (p. 481).

AWS CLI

Pour supprimer un identificateur source d'un abonnement aux notifications d'événements Amazon RDS, utilisez la commande `remove-source-identifier-from-subscription` de l'AWS CLI. Incluez les paramètres requis suivants :

- `--subscription-name`
- `--source-identifier`

Example

L'exemple suivant supprime l'identifiant source `mysqldb` de l'abonnement `myrdseventsubscription`.

Pour Linux, macOS ou Unix :

```
aws rds remove-source-identifier-from-subscription \
    --subscription-name myrdseventsubscription \
    --source-identifier mysqldb
```

Pour Windows :

```
aws rds remove-source-identifier-from-subscription ^
    --subscription-name myrdseventsubscription ^
    --source-identifier mysqldb
```

API

Pour supprimer un identificateur source d'un abonnement aux notifications d'événements Amazon RDS, utilisez la commande d'API `RemoveSourceIdentifierFromSubscription` de l'Amazon RDS. Incluez les paramètres requis suivants :

- `SubscriptionName`
- `SourceIdentifier`

Affichage des catégories aux notifications d'événements Amazon RDS

Tous les événements d'un type de ressource sont regroupés en catégories. Pour afficher la liste des catégories disponibles, utilisez les procédures suivantes.

Console

Lorsque vous créez ou modifiez un abonnement aux notifications d'événements, les catégories d'événements sont affichées dans la console Amazon RDS. Pour plus d'informations, consultez Modification d'un abonnement aux notifications d'événements Amazon RDS (p. 481).

AWS CLI

Pour lister les catégories de notifications d'événements Amazon RDS, utilisez la commande `describe-event-categories` de l'AWS CLI. Cette commande n'a aucun paramètre requis.

Example

```
aws rds describe-event-categories
```

API

Pour lister les catégories de notifications d'événements Amazon RDS, utilisez la commande d'API `DescribeEventCategories` de l'Amazon RDS. Cette commande n'a aucun paramètre requis.

Suppression d'un abonnement aux notifications d'événements Amazon RDS

Vous pouvez supprimer un abonnement lorsque vous n'en avez plus besoin. Tous les abonnés à la rubrique ne reçoivent plus les notifications d'événements spécifiées par l'abonnement.

Console

Pour supprimer un abonnement aux notifications d'événements Amazon RDS

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez DB Event Subscriptions (Abonnements aux événements de base de données).
3. Dans le volet My DB Event Subscriptions (Mes abonnements aux événements de base de données), cliquez sur l'abonnement que vous souhaitez supprimer.
4. Sélectionnez Delete.
5. La console Amazon RDS indique que l'abonnement est en cours de suppression.

AWS CLI

Pour supprimer un abonnement aux notifications d'événements Amazon RDS, utilisez la commande `delete-event-subscription` de l'AWS CLI. Incluez le paramètre requis suivant :

- `--subscription-name`

Example

L'exemple suivant supprime l'abonnement `myrdssubscription`.

```
aws rds delete-event-subscription --subscription-name myrdssubscription
```

API

Pour supprimer un abonnement aux notifications d'événements Amazon RDS, utilisez la commande `DeleteEventSubscription` de l'API. Incluez le paramètre requis suivant :

- `SubscriptionName`

Affichage d'événements Amazon RDS

Amazon RDS consigne les événements associés à vos instances de base de données, snapshots DB, groupes de sécurité DB et groupes de paramètres DB. Les informations consignées comprennent la date et l'heure de l'événement, le nom et le type de source de l'événement, ainsi qu'un message associé à l'événement.

Vous pouvez récupérer les événements pour vos ressources RDS via la console AWS Management Console, qui affiche les événements des dernières 24 heures. Vous pouvez également récupérer des événements pour vos ressources RDS à l'aide de la commande describe-events de l'AWS CLI, ou de l'opération d'API RDS DescribeEvents. Si vous utilisez l'AWS CLI ou l'API RDS pour afficher les événements, vous pouvez récupérer les événements datant de 14 jours maximum.

> **Note**
>
> Si vous devez stocker des événements pendant des périodes plus longues, vous pouvez envoyer des événements Amazon RDS à CloudWatch Events. Pour de plus amples informations, veuillez consulter Obtention d'événements CloudWatch Events et Amazon EventBridge pour Amazon RDS (p. 487)

Console

Pour afficher tous les événements des instances Amazon RDS des dernières 24 heures

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, sélectionnez Events. Les événements disponibles s'affichent sous forme de liste.
3. Utilisez la liste Filtrer pour filtrer les événements par type, et utilisez la zone de texte à droite de la liste Filtrer pour affiner vos résultats. Par exemple, la capture d'écran ci-dessous montre une liste des événements filtrés par le type d'événement d'instance de base de données et contenant les caractères **`1318`**.

AWS CLI

Pour afficher tous les événements des instances Amazon RDS des 7 derniers jours

Vous pouvez afficher tous les événements des instances Amazon RDS des 7 derniers jours en appelant la commande describe-events de l'AWS CLI et en définissant le paramètre `--duration` sur `10080`.

```
aws rds describe-events --duration 10080
```

API

Pour afficher tous les événements des instances Amazon RDS des 14 derniers jours

Vous pouvez afficher tous les événements des instances Amazon RDS des 14 derniers jours en appelant l'opération d'API RDS DescribeEvents et en définissant le paramètre `Duration` sur `20160`.

```
https://rds.us-west-2.amazonaws.com/
   ?Action=DescribeEvents
   &Duration=20160
   &MaxRecords=100
   &SignatureMethod=HmacSHA256
   &SignatureVersion=4
   &Version=2014-10-31
   &X-Amz-Algorithm=AWS4-HMAC-SHA256
   &X-Amz-Credential=AKIADQKE4SARGYLE/20140421/us-west-2/rds/aws4_request
   &X-Amz-Date=20140421T194733Z
   &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
   &X-Amz-Signature=8e313cabcdbd9766c56a2886b5b298fd944e0b7cfa248953c82705fdd0374f27
```

Obtention d'événements CloudWatch Events et Amazon EventBridge pour Amazon RDS

Amazon CloudWatch Events et Amazon EventBridge vous permettent tous les deux d'automatiser des services AWS et de répondre à des événements système tels que des problèmes de disponibilité d'application ou des modifications de ressource. Les événements de services AWS sont transmis à CloudWatch Events et EventBridge presque en temps réel. Vous pouvez écrire des règles simples pour préciser les événements qui vous intéressent et les actions automatisées à effectuer quand un événement correspond à une règle.

Vous pouvez définir une variété de cibles (par exemple, une fonction AWS Lambda ou une rubrique Amazon SNS) qui reçoivent des événements au format JSON. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur Amazon CloudWatch Events et le Guide de l'utilisateur Amazon EventBridge.

Par exemple, vous pouvez configurer Amazon RDS pour envoyer des événements à CloudWatch Events ou Amazon EventBridge chaque fois qu'une instance de base de données est créée ou supprimée.

Rubriques

- Envoi d'événements Amazon RDS à CloudWatch Events (p. 488)
- Événements d'instance de base de données (p. 488)

- Événements de groupe de paramètres de base de données (p. 489)
- Événements de groupe de sécurité de base de données (p. 489)
- Événements d'instantané de bases de données (p. 490)

Envoi d'événements Amazon RDS à CloudWatch Events

Vous pouvez créer des règles CloudWatch Events pour envoyer des événements Amazon RDS à CloudWatch Events.

Utilisez les étapes suivantes pour créer une règle CloudWatch Events qui se déclenche sur un événement émis par un service AWS.

Pour créer une règle qui se déclenche sur un événement :

1. Ouvrez la console CloudWatch à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Sous Événements dans le panneau de navigation, choisissez Règles.
3. Choisissez Create rule.
4. Dans Event source, effectuez l'une des opérations suivantes :
   a. Choisissez Modèle d'événement.
   b. Pour Nom du service, choisissez Relational Database Service (RDS).
   c. Pour Type d'événement, choisissez le type de ressource Amazon RDS qui déclenche l'événement. Par exemple, si une instance de base de données déclenche l'événement, choisissez RDS DB Instance Event (Événement d'instance de base de données RDS).
5. Pour Cibles, choisissez Ajouter une cible, puis Groupe de journaux CloudWatch.
6. Pour Groupe de journaux, entrez un nom pour le groupe de journaux destiné au stockage des événements.
7. Sélectionnez Configure details. Dans Rule definition, saisissez un nom et une description pour la règle.
8. Choisissez Create rule.

Événements d'instance de base de données

Voici un exemple d'événement d'instance de base de données.

```
{
  "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",
    "SourceIdentifier": "rds:my-db-instance",
    "Message": "A Multi-AZ failover has completed."
  }
}
```

Événements de groupe de paramètres de base de données

Voici un exemple d'événement de groupe de paramètres de base de données.

```
{
  "version": "0",
  "id": "844e2571-85d4-695f-b930-0153b71dcb42",
  "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",
    "SourceIdentifier": "rds:my-db-param-group",
    "Message": "Updated parameter time_zone to UTC with apply method immediate"
  }
}
```

Événements de groupe de sécurité de base de données

Voici un exemple d'événement de groupe de sécurité de base de données.

```
{
  "version": "0",
  "id": "844e2571-85d4-695f-b930-0153b71dcb42",
  "detail-type": "RDS DB Security 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:secgrp:my-security-group"
  ],
  "detail": {
    "EventCategories": [
      "configuration change"
```

```
    ],
    "SourceType": "SECURITY_GROUP",
    "SourceArn": "arn:aws:rds:us-east-1:123456789012:secgrp:my-security-group",
    "Date": "2018-10-06T12:26:13.882Z",
    "SourceIdentifier": "rds:my-security-group",
    "Message": "Applied change to security group"
  }
}
```

Événements d'instantané de bases de données

Voici un exemple d'événement d'instantané de bases de données.

```
{
  "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",
    "SourceIdentifier": "rds:my-db-snapshot",
    "Message": "Deleted manual snapshot"
  }
}
```

Amazon RDS Fichiers journaux de base de données

Vous pouvez afficher, télécharger et consulter les journaux de base de données à l'aide d'AWS Management Console, de l'AWS Command Line Interface (AWS CLI) ou de l'API Amazon RDS. L'affichage, le téléchargement ou la consultation des journaux de transactions ne sont pas pris en charge.

Pour accéder aux informations spécifiques à chaque moteur de base de données, consultez le tableau suivant :

- Fichiers journaux de base de données MariaDB (p. 494)
- Fichiers journaux de base de données Microsoft SQL Server (p. 503)
- Fichiers journaux de base de données MySQL (p. 506)
- Fichiers journaux de base de données Oracle (p. 515)
- Fichiers journaux de base de données PostgreSQL (p. 521)

Liste et affichage des fichiers journaux de base de données

Vous pouvez afficher les fichiers journaux de base de données pour votre moteur de base de données à l'aide d'AWS Management Console. Vous pouvez répertorier les fichiers journaux disponibles pour téléchargement ou surveillance à l'aide de l'AWS CLI ou de l'API Amazon RDS.

> Note
>
> Si vous ne parvenez pas à afficher la liste des fichiers journaux pour une instance de base de données Oracle existante, redémarrez l'instance.

Console

Pour afficher un fichier journal de base de données

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez le nom de l'instance de base de données qui contient le fichier journal que vous voulez consulter.
4. Choisissez l'onglet Logs & events (Journaux et événements).
5. Faites défiler jusqu'à la section Journaux.
6. Dans la section Journaux, choisissez le journal que vous souhaitez afficher, puis choisissez Afficher.

AWS CLI

Pour répertorier les fichiers journaux de base de données disponibles pour une instance de base de données, utilisez la commande `describe-db-log-files` de l'AWS CLI.

L'exemple suivant renvoie une liste des fichiers journaux pour une instance DB nommée `my-db-instance`.

Example

```
aws rds describe-db-log-files --db-instance-identifier my-db-instance
```

API RDS

Pour répertorier les fichiers journaux de base de données disponibles pour une instance de base de données, utilisez l'action `DescribeDBLogFiles` de l'API Amazon RDS.

Téléchargement d'un fichier journal de base de données

Vous pouvez utiliser AWS Management Console, l'AWS CLI ou l'API pour télécharger un fichier journal de base de données.

Console

Pour télécharger un fichier journal de base de données

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.

2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez le nom de l'instance de base de données qui contient le fichier journal que vous voulez consulter.
4. Choisissez l'onglet Logs & events (Journaux et événements).
5. Faites défiler jusqu'à la section Journaux.
6. Dans la section Journaux, sélectionnez le bouton en regard du journal que vous voulez télécharger, puis choisissez Télécharger.
7. Ouvrez le menu contextuel (clic droit) pour le lien fourni, puis choisissez Enregistrer le lien sous. Saisissez l'emplacement souhaité pour l'enregistrement du fichier journal, puis cliquez sur Enregistrer.

AWS CLI

Pour télécharger un fichier journal de base de données, utilisez la commande `download-db-log-file-portion` de l'AWS CLI. Par défaut, cette commande télécharge uniquement la portion la plus récente d'un fichier journal. Vous pouvez toutefois télécharger un fichier complet en spécifiant le paramètre `--starting-token 0`.

L'exemple suivant montre comment télécharger le contenu d'un fichier journal appelé log/ERROR.4 et le stocker dans un fichier local appelé errorlog.txt.

Example

Pour Linux, macOS ou 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
```

Pour 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
```

API RDS

Pour télécharger un fichier journal de base de données, utilisez l'action `DownloadDBLogFilePortion` de l'API Amazon RDS.

Consultation d'un fichier journal de base de données

Vous pouvez surveiller le contenu d'un fichier journal à l'aide d'AWS Management Console.

Console

Pour consulter un fichier journal de base de données

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez le nom de l'instance de base de données qui contient le fichier journal que vous voulez consulter.
4. Choisissez l'onglet Logs & events (Journaux et événements).
5. Dans la section Journaux, choisissez un fichier journal, puis Consulter.

Publication des journaux de base de données dans Amazon CloudWatch Logs

Outre l'affichage et le téléchargement des journaux d'instance de base de données, vous pouvez publier des journaux dans Amazon CloudWatch Logs. CloudWatch Logs permet d'effectuer une analyse en temps réel des données de journaux, de stocker les données dans un stockage hautement durable et de gérer les données grâce à l'agent CloudWatch Logs. AWS conserve les données de journaux publiées dans CloudWatch Logs pendant une période indéterminée, sauf si vous précisez une durée de conservation. Pour de plus amples informations, veuillez consulter Modification de la conservation des données de journaux dans CloudWatch Logs.

Pour accéder aux informations spécifiques à chaque moteur de base de données, consultez le tableau suivant :

- the section called “Publication des journaux MariaDB dans Amazon CloudWatch Logs” (p. 496)
- the section called “Publication des journaux MySQL dans CloudWatch Logs” (p. 509)
- the section called “Publication des journaux Oracle dans Amazon CloudWatch Logs” (p. 518)
- the section called “Publication de journaux PostgreSQL dans CloudWatch Logs” (p. 523)
- the section called “Publication de journaux SQL Server dans Amazon CloudWatch Logs” (p. 504)

Lecture du contenu des fichiers journaux avec REST

Amazon RDS fournit un point de terminaison REST qui permet d'accéder aux fichiers journaux des instances de base de données. Ceci est utile si vous devez écrire une application pour diffuser en continu le contenu de fichiers journaux Amazon RDS.

La syntaxe est la suivante :

```
GET /v13/downloadCompleteLogFile/DBInstanceIdentifier/LogFileName HTTP/1.1
Content-type: application/json
host: rds.region.amazonaws.com
```

Les paramètres suivants sont obligatoires :

- *DBInstanceIdentifier*—le nom assigné par le client de l'instance de base de données qui contient le fichier journal que vous souhaitez télécharger.
- *LogFileName*—le nom du fichier journal à télécharger.

La réponse contient les contenus du fichier journal demandé, en tant que flux.

L'exemple suivant télécharge le fichier journal appelé log/ERROR.6 pour l'instance de base de données appelée sample-sql dans la région us-west-2.

```
GET /v13/downloadCompleteLogFile/sample-sql/log/ERROR.6 HTTP/1.1
host: rds.us-west-2.amazonaws.com
X-Amz-Security-Token: AQoDYXdzEIH//////////
wEa0AIXLhngC5zp9CyB1R6abwKrXHVR5efnAVN3XvR7IwqKYalFSn6UyJuEFTft9nObglx4QJ+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
```

Si vous spécifiez une instance de base de données qui n'existe pas, la réponse se compose de l'erreur suivante :

- `DBInstanceNotFound`—*DBInstanceIdentifier* ne fait pas référence à une instance de base de données existante. (HTTP status code: 404)

Fichiers journaux de base de données MariaDB

Vous pouvez contrôler le journal des erreurs, le journal des requêtes lentes et le journal général MariaDB. Le fichier journal des erreurs MariaDB est généré par défaut ; vous pouvez générer les journaux des requêtes lentes et général en définissant des paramètres dans votre groupe de paramètres de base de données. Amazon RDS fait tourner tous les fichiers de journaux MariaDB. Les intervalles pour chaque type sont indiquées ci-après.

Vous pouvez contrôler les journaux MariaDB directement via la console Amazon RDS, l'API Amazon RDS, l'interface en ligne de commande Amazon RDS ou les kits SDK AWS. Vous pouvez également accéder aux journaux MariaDB en dirigeant les journaux vers une table de base de données de la base de données principale et interroger cette table. Vous pouvez utiliser l'utilitaire mysqlbinlog pour télécharger un journal binaire.

Pour plus d'informations sur l'affichage, le téléchargement ou la consultation des journaux de base de données basés sur des fichiers, consultez Amazon RDS Fichiers journaux de base de données (p. 490).

Accès aux journaux des erreurs MariaDB

Le journal des erreurs MariaDB est écrit dans le fichier `<host-name>.err`. Vous pouvez afficher ce fichier à l'aide de la console Amazon RDS ou en récupérant le journal à l'aide de l'API Amazon RDS, de l'interface de ligne de commande Amazon RDS ou des kits SDK AWS. Le fichier `<host-name>.err` est vidé toutes les 5 minutes, et son contenu est ajouté à `mysql-error-running.log`. Le fichier `mysql-error-running.log` fait ensuite l'objet d'une rotation toutes les heures et les fichiers générés toutes les heures au cours des 24 dernières heures sont conservés. Le nom du fichier journal comporte l'heure à laquelle le fichier a été généré (au format UTC). Les fichiers journaux comportent également un horodatage permettant de déterminer le moment où les entrées du journal ont été écrites.

MariaDB écrit des informations dans le fichier des erreurs uniquement au moment du démarrage, de l'arrêt et lorsqu'une erreur survient. Une instance de base de données peut fonctionner pendant des heures ou

des jours sans qu'aucune nouvelle entrée soit écrite dans le journal des erreurs. Si aucune entrée récente ne figure, cela signifie que le serveur n'a pas rencontré d'erreur justifiant une entrée de journal.

Accès au journal des requêtes lentes et au journal général MariaDB

Le journal des requêtes lentes et le journal général MariaDB peuvent être écrits dans un fichier ou dans une table de base de données en définissant les paramètres nécessaires dans votre groupe de paramètres DB. Pour plus d'informations sur la création et la modification d'un groupe de paramètres DB, consultez Utilisation de groupes de paramètres de base de données (p. 225). Vous devez définir ces paramètres avant de pouvoir consulter le journal des requêtes lentes ou le journal général dans la console Amazon RDS ou à l'aide de l'API Amazon RDS, de l'AWS CLI ou des kits SDK AWS.

Vous pouvez contrôler la journalisation MariaDB à l'aide des paramètres de cette liste :

- `slow_query_log` : Pour créer le journal des requêtes lentes, définir sur 1. La valeur par défaut est 0.
- `general_log` : Pour créer le journal général, définir sur 1. La valeur par défaut est 0.
- `long_query_time` : Pour empêcher l'enregistrement des requêtes rapides dans le journal des requêtes lentes, indiquez la valeur de la durée d'exécution de requête la plus courte devant être enregistrée, en secondes. La valeur par défaut est de 10 secondes et la valeur minimum est 0. Si log_output = FILE, vous pouvez indiquer une valeur à virgule flottante avec une résolution en microseconde. Si log_output = TABLE, vous devez indiquer un nombre entier avec une résolution en seconde. Seules les requêtes dont la durée d'exécution dépasse la valeur `long_query_time` sont enregistrées. Par exemple, si vous définissez `long_query_time` sur 0,1, les requêtes s'exécutant pendant moins de 100 millisecondes ne sont pas enregistrées.
- `log_queries_not_using_indexes` : Pour enregistrer toutes les requêtes n'utilisant pas d'index dans le journal des requêtes lentes, définir ce paramètre sur 1. La valeur par défaut est 0. Les requêtes n'utilisant pas d'index sont enregistrées même si la durée de leur exécution est inférieure à la valeur du paramètre `long_query_time`.
- `log_output` *`option`* : Vous pouvez spécifier l'une des options suivantes pour le paramètre `log_output` :
  - TABLEAU (par défaut) – Écrit les requêtes générales dans le tableau `mysql.general_log` et les requêtes lentes dans le tableau `mysql.slow_log`.
  - FILE (FICHIER) – Écrit les fichiers des requêtes générales et lentes dans le fichier système. Les fichiers journaux font l'objet d'une rotation horaire.
  - NONE (AUCUNE)– Désactive la journalisation.

Lorsque la journalisation est activée, Amazon RDS effectue une rotation des journaux des tables ou supprime les fichiers journaux à intervalles réguliers. Cette précaution permet de limiter la possibilité qu'un fichier journal volumineux ne bloque l'utilisation de la base de données ou n'affecte les performances. Rotation et suppression de l'approche de journalisation `FILE` et `TABLE` comme suit :

- Lorsque la journalisation `FILE` est activée, les fichiers journaux sont examinés toutes les heures et ceux dont l'ancienneté est supérieure à 24 heures sont supprimés. Dans certains cas, la taille des fichiers journaux combinés restant après la suppression peut dépasser le seuil de 2 % de l'espace alloué à une instance de base de données. Dans ces cas, les fichiers journaux les plus volumineux sont supprimés jusqu'à ce que la taille des fichiers journaux ne soit plus supérieure au seuil.
- Lorsque la journalisation de `TABLE` est activée, les journaux des tables font dans certains cas l'objet d'une rotation toutes les 24 heures. Cette rotation se produit si l'espace utilisé par les journaux des tables est supérieur à 20 % de l'espace de stockage alloué ou si la taille de l'ensemble des journaux est supérieure à 10 Go. Si l'espace utilisé pour une instance de base de données est supérieur à 90 % de l'espace de stockage alloué à l'instance de base de données, alors les seuils correspondant à la rotation des journaux est réduite. Les tables de journaux font alors l'objet d'une rotation si l'espace utilisé par les

journaux des tables est supérieur à 10 % de l'espace de stockage alloué ou si la taille de l'ensemble des journaux est supérieure à 5 Go.

Lors de la rotation des tables de journaux, la table de journal actuelle est copiée vers une table de journal de sauvegarde et les entrées de la table de journal actuelle sont supprimées. Si la table de journal de sauvegarde existe déjà, elle est supprimée avant que la table de journal actuelle ne soit copiée dans la sauvegarde. Si besoin, vous pouvez interroger la table de journal de sauvegarde. La table de journal de sauvegarde de la table `mysql.general_log` est nommée `mysql.general_log_backup`. La table de journal de sauvegarde de la table `mysql.slow_log` est nommée `mysql.slow_log_backup`.

Vous pouvez effectuer une rotation de la table `mysql.general_log` en appelant la procédure `mysql.rds_rotate_general_log`. Vous pouvez effectuer une rotation de la table `mysql.slow_log` en appelant la procédure `mysql.rds_rotate_slow_log`.

La rotation des journaux des tables est effectuée pendant la mise à niveau de la version d'une base de données.

Amazon RDS enregistre la rotation des journaux `TABLE` et `FILE` dans un événement Amazon RDS et vous envoie une notification.

Pour utiliser les journaux depuis la console Amazon RDS, l'API Amazon RDS, la CLI Amazon RDS ou les kits SDK AWS, définissez le paramètre `log_output` sur FILE. A l'instar du journal des erreurs MariaDB, ces fichiers journaux font l'objet d'une rotation horaire. Les fichiers journaux qui ont été générés au cours des dernières 24 heures sont conservés.

Pour plus d'informations sur le journal des requêtes lentes et le journal général, accédez aux rubriques suivantes dans la documentation MariaDB :

- Journal des requêtes lentes
- Journal des requêtes générales

Publication des journaux MariaDB dans Amazon CloudWatch Logs

Vous pouvez configurer votre instance de base de données MariaDB Amazon RDS de sorte à publier des données de journaux dans un groupe de journaux dans Amazon CloudWatch Logs. CloudWatch Logs vous permet d'effectuer une analyse en temps réel des données de journaux et d'utiliser CloudWatch pour créer des alarmes et afficher des métriques. CloudWatch Logs permet de conserver les enregistrements des journaux dans une solution de stockage hautement durable.

Amazon RDS publie chaque journal de base de données MariaDB sous la forme d'un flux de base de données distinct dans le groupe de journaux. Par exemple, si vous configurez la fonction d'exportation de sorte à inclure le journal de requêtes lentes, les données de requêtes lentes sont stockées dans un flux de journal de requêtes lentes dans le groupe de journaux `/aws/rds/instance/`*`my_instance`*`/slowquery`.

Le journal d'erreurs est activé par défaut. Le tableau ci-dessous récapitule les conditions requises pour les autres journaux MariaDB.

Log	Exigence
Journal d'audit	L'instance de base de données doit disposer d'un groupe d'options personnalisées avec l'option `MARIADB_AUDIT_PLUGIN`.

Log	Exigence
Journal général	L'instance de base de données doit disposer d'un groupe de paramètres personnalisés avec le paramètre `general_log = 1` pour autoriser la journalisation générale.
Journal des requêtes lentes	L'instance de base de données doit disposer d'un groupe de paramètres personnalisés avec le paramètre `slow_query_log = 1` pour autoriser la journalisation de requête lente.
Sortie de journal	L'instance de base de données doit disposer d'un groupe de paramètres personnalisés avec le paramètre `log_output = FILE` pour écrire de journaux dans le système de fichier et les publier dans CloudWatch Logs.

Console

Pour publier des journaux MariaDB dans CloudWatch Logs à partir de la console

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Bases de données, puis l'instance de base de données que vous souhaitez modifier.
3. Sélectionnez Modify.
4. Dans la section Exportations des journaux, choisissez les journaux que vous voulez commencer à publier dans CloudWatch Logs.
5. Choisissez Continuer, puis Modifier l'instance de base de données sur la page récapitulative.

AWS CLI

Vous pouvez publier un journal MariaDB avec l'interface de ligne de commande AWS. Vous pouvez appeler la commande `modify-db-instance` avec les paramètres suivants :

- `--db-instance-identifier`
- `--cloudwatch-logs-export-configuration`

> **Note**
>
> Une modification apportée à l'option `--cloudwatch-logs-export-configuration` est toujours appliquée immédiatement à l'instance de base de données. Par conséquent, les options `--apply-immediately` et `--no-apply-immediately` sont sans effet.

Vous pouvez également publier des journaux MariaDB en appelant les commandes de l'interface de ligne de commande AWS suivantes :

- `create-db-instance`
- `restore-db-instance-from-db-snapshot`
- `restore-db-instance-from-s3`
- `restore-db-instance-to-point-in-time`

Exécutez l'une de ces commandes de l'interface de ligne de commande AWS avec les options suivantes :

- `--db-instance-identifier`
- `--enable-cloudwatch-logs-exports`
- `--db-instance-class`
- `--engine`

D'autres options peuvent être requises en fonction de la commande de l'AWS CLI que vous exécutez.

Example

L'exemple suivant modifie une instance de base de données MariaDB existante pour publier les fichiers journaux dans CloudWatch Logs. La valeur `--cloudwatch-logs-export-configuration` n'est pas un objet JSON. La clé pour cet objet est `EnableLogTypes` et sa valeur est un tableau de chaînes avec une combinaison quelconque de `audit`, `error`, `general` et `slowquery`.

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --cloudwatch-logs-export-configuration '{"EnableLogTypes":
["audit","error","general","slowquery"]}'
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration '{"EnableLogTypes":
["audit","error","general","slowquery"]}'
```

Example

La commande suivante crée une instance de base de données MariaDB et publie les fichiers journaux dans CloudWatch Logs. La valeur `--enable-cloudwatch-logs-exports` est un tableau de chaînes JSON. Les chaînes peuvent être une combinaison de `audit`, `error`, `general` et `slowquery`.

Pour Linux, macOS ou 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
```

Pour 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
```

API RDS

Vous pouvez publier des journaux MariaDB avec l'API RDS. Vous pouvez appeler l'opération `ModifyDBInstance` avec les paramètres suivants :

- `DBInstanceIdentifier`
- `CloudwatchLogsExportConfiguration`

> **Note**
>
> Une modification apportée au paramètre `CloudwatchLogsExportConfiguration` est toujours appliquée immédiatement à l'instance de base de données. Par conséquent, le paramètre `ApplyImmediately` est sans effet.

Vous pouvez également publier des journaux MariaDB en appelant les opérations d'API RDS suivantes :

- `CreateDBInstance`
- `RestoreDBInstanceFromDBSnapshot`
- `RestoreDBInstanceFromS3`
- `RestoreDBInstanceToPointInTime`

Exécutez l'une de ces opérations d'API RDS avec les paramètres suivants :

- `DBInstanceIdentifier`
- `EnableCloudwatchLogsExports`
- `Engine`
- `DBInstanceClass`

D'autres paramètres peuvent être requis en fonction de la commande d'interface de ligne de commande AWS que vous exécutez.

Taille des fichiers journaux

Les tailles du journal des requêtes lentes, du journal des erreurs et du journal général MariaDB sont limitées à 2 %maximum de l'espace de stockage alloué à une instance de base de données. Pour respecter ce seuil, les journaux font l'objet d'une rotation automatique toutes les heures et les fichiers dont l'ancienneté est supérieure à 24 heures sont supprimés. Si la taille de l'ensemble des fichiers journaux après la suppression dépasse le seuil, les fichiers journaux les plus volumineux sont supprimés jusqu'à ce que la taille des fichiers journaux ne soit plus supérieure au seuil.

Gestion des journaux MariaDB sous forme de table

Vous pouvez diriger le journal des requêtes lentes et le journal général vers des tables sur l'instance de base de données en créant un groupe de paramètres DB et en définissant le paramètre du serveur `log_output` sur `TABLE`. Les requêtes générales sont ensuite enregistrées dans la table `mysql.general_log` et les requêtes lentes dans la table `mysql.slow_log`. Vous pouvez interroger les tables pour accéder aux informations des journaux. L'activation de cette journalisation augmente le volume de données écrites dans la base de données, ce qui peut dégrader les performances.

Par défaut, le journal général et le journal des requêtes lentes sont désactivés. Afin d'activer la journalisation dans les tables, vous devez également définir les paramètres `general_log` et `slow_query_log` sur `1`.

Les tables de journaux continuent de grossir jusqu'à ce que les activités de journalisation correspondantes soient désactivées en redéfinissant le paramètre approprié sur `0`. Avec le temps, une grande quantité de données s'accumule et risque d'utiliser une part considérable de l'espace de stockage alloué. Amazon RDS ne vous permet pas de tronquer les tableaux de journaux, mais vous pouvez déplacer leurs contenus. Lorsque vous procédez à la rotation d'une table, son contenu est enregistré dans une table de sauvegarde et une nouvelle table de journal vide est créée. Vous pouvez effectuer une rotation manuelle des tables de

journaux avec les procédures de ligne de commande suivantes, dans lesquelles l'invite de commande est indiquée par `PROMPT>` :

```
PROMPT> CALL mysql.rds_rotate_slow_log;
PROMPT> CALL mysql.rds_rotate_general_log;
```

Pour supprimer totalement les anciennes données et récupérer l'espace de disque, appelez deux fois à la suite la procédure appropriée.

Format de journalisation binaire

MariaDB sur Amazon RDS prend en charge les formats de journalisation binaire basés sur les lignes, basés sur les instructions et mixtes. Le format de journalisation binaire par défaut est mixte. Pour plus de détails sur les différents formats de journalisation binaire MariaDB, consultez Formats de journalisation binaire dans la documentation MariaDB.

Si vous prévoyez d'utiliser la réplication, le format de journalisation binaire est important car il détermine le dossier de modifications de données qui est enregistré dans la source et envoyés aux cibles de réplication. Pour de plus amples informations sur les avantages et les inconvénients des différents formats de journalisation binaire pour la réplication, veuillez consulter la section Advantages and Disadvantages of Statement-Based and Row-Based Replication de la documentation MySQL.

> **Important**
>
> Lorsque vous définissez le format de journalisation binaire sur « basé sur les lignes », vous risquez de générer des fichiers journaux binaires très volumineux. Ces derniers réduisent le stockage disponible pour une instance de base de données et peuvent augmenter la durée nécessaire pour effectuer une opération de restauration d'une instance de base de données. La réplication basée sur les instructions peut provoquer des incohérences entre l'instance de base de données source et un réplica en lecture. Pour plus d'informations, consultez la section Unsafe Statements for Statement-based Replication dans la documentation MariaDB.

Pour définir le format de journalisation binaire MariaDB :

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes de paramètres.
3. Choisissez le groupe de paramètres utilisé par l'instance de base de données que vous souhaitez modifier.

   Vous ne pouvez pas modifier un groupe de paramètres par défaut. Si l'instance de base de données utilise un groupe de paramètres par défaut, créez un nouveau groupe et associez-le à l'instance.

   Pour plus d'informations sur les groupes de paramètres de base de données, consultez Utilisation de groupes de paramètres de base de données (p. 225).
4. Sous Parameter group actions (Actions de groupe de paramètres), choisissez Edit (Modifier).
5. Définissez le paramètre `binlog_format` au format de journalisation binaire de votre choix (ROW, STATEMENT ou MIXED).
6. Choisissez Enregistrer les modifications pour enregistrer les mises à jour apportées au groupe de paramètres de base de données.

Accès aux journaux binaires MariaDB

Vous pouvez utiliser l'utilitaire mysqlbinlog pour télécharger les journaux binaires au format texte à partir d'instances de base de données MariaDB. Le journal binaire est téléchargé dans votre ordinateur local.

Pour plus d'informations sur l'utilisation de l'utilitaire mysqlbinlog, accédez à Utilisation de mysqlbinlog dans la documentation MariaDB.

Pour exécuter à nouveau l'utilitaire mysqlbinlog sur une instance Amazon RDS, utilisez les options suivantes :

- Spécifiez l'option `--read-from-remote-server`.
- `--host` : Spécifiez le nom DNS du point de terminaison de l'instance.
- `--port` : Spécifiez le port utilisé par l'instance.
- `--user` : Spécifiez un utilisateur MariaDB ayant l'autorisation de réplication esclave.
- `--password` : Spécifiez le mot de passe de l'utilisateur ou omettez la valeur de mot de passe pour que l'utilitaire vous invite à saisir un mot de passe.
- `--result-file` : Spécifiez le fichier local qui recevra la sortie.
- Spécifiez les noms pour un ou plusieurs fichiers journaux binaires. Pour obtenir la liste des journaux disponibles, utilisez la commande SQL SHOW BINARY LOGS.

Pour plus d'informations sur les options mysqlbinlog, accédez aux Options mysqlbinlog dans la documentation MariaDB.

Voici un exemple :

Pour Linux, macOS ou Unix :

```
mysqlbinlog \
    --read-from-remote-server \
    --host=mariadbinstance1.1234abcd.region.rds.amazonaws.com \
    --port=3306  \
    --user ReplUser \
    --password <password> \
    --result-file=/tmp/binlog.txt
```

Pour 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 purge normalement un journal binaire dès que possible, mais le journal binaire doit toujours être disponible sur l'instance afin que mysqlbinlog puisse y accéder. Pour spécifier le nombre d'heures pendant lesquelles RDS conservera les journaux binaires, utilisez la procédure stockée `mysql.rds_set_configuration` et spécifiez une période suffisamment longue pour pouvoir télécharger les journaux. Après avoir défini la période de rétention, surveillez l'utilisation du stockage pour l'instance de bases de données afin de garantir que les journaux binaires conservés n'utilisent pas trop d'espace de stockage.

L'exemple suivant définit la période de rétention sur 1 jour :

```
call mysql.rds_set_configuration('binlog retention hours', 24);
```

Pour afficher les paramètres actuels, utilisez la procédure stockée `mysql.rds_show_configuration` :

```
call mysql.rds_show_configuration;
```

Annotation des journaux binaires

Dans une instance de base de données MariaDB, vous pouvez utiliser l'événement `Annotate_rows` pour annoter un événement de ligne avec une copie de la requête SQL ayant provoqué cet événement. Cette approche offre une fonctionnalité similaire à l'activation du paramètre `binlog_rows_query_log_events` sur une instance de base de données sur une version MySQL 5.6 ou ultérieure.

Vous pouvez activer globalement les annotations des journaux binaires en créant un groupe de paramètres personnalisé et en définissant le paramètre `binlog_annotate_row_events` sur **`1`**. Vous pouvez également activer les annotations au niveau de la session, en appelant `SET SESSION binlog_annotate_row_events = 1`. Utilisez `replicate_annotate_row_events` pour répliquer les annotations des journaux binaires dans l'instance esclave si la journalisation binaire est activée pour cette instance. Aucun privilège spécial n'est nécessaire pour utiliser ces paramètres.

L'exemple suivant illustre une transaction basée sur les lignes dans MariaDB. L'utilisation de la journalisation basée sur les lignes est déclenchée en définissant le niveau d'isolement des transactions sur 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;
```

Sans les annotations, les entrées du journal binaire pour la transaction ressemblent à :

```
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/*!*/;
```

L'instruction suivante active les annotations au niveau de la session pour cette même transaction, et les désactive après validation de la 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;
```

Avec les annotations, les entrées du journal binaire pour la transaction ressemblent à :

```
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/*!*/;
```

Fichiers journaux de base de données Microsoft SQL Server

Vous pouvez accéder aux journaux des erreurs Microsoft SQL Server, aux journaux de l'agent, aux fichiers de trace et aux fichiers de vidage à l'aide de la console Amazon RDS, de l'AWS CLI ou de l'API RDS. Pour plus d'informations sur l'affichage, le téléchargement ou la consultation des journaux de base de données basés sur des fichiers, consultez Amazon RDS Fichiers journaux de base de données (p. 490).

Programme de rétention

Les fichiers journaux font l'objet d'une rotation chaque jour et chaque fois que votre instance de base de données est redémarrée. Voici le programme de rétention des journaux Microsoft SQL Server sur Amazon RDS.

Log type (Type de journal)	Programme de rétention
Journaux des erreurs	Un maximum de 30 journaux d'erreur sont retenus. Amazon RDS peut supprimer les journaux d'erreur de plus de 7 jours d'âge.
Journaux de l'agent	Un maximum de 10 journaux d'agent sont retenus. Amazon RDS peut supprimer les journaux d'agent de plus de 7 jours d'âge.
Fichiers de trace	Les fichiers de trace sont conservés selon la période de rétention des fichiers de trace de votre instance de base de données. La période de rétention par défaut des fichiers de trace est de 7 jours. Pour modifier la période de rétention des fichiers de trace pour votre instance de base de données, consultez Configuration de la période de rétention pour les fichiers de trace et de vidage (p. 777).
Fichiers de vidage	Les fichiers de vidage sont conservés selon la période de rétention des fichiers de vidage de votre instance de base de données. La période de rétention par défaut des fichiers de vidage est de 7 jours. Pour modifier la période de rétention des fichiers de vidage pour votre instance de base de données, consultez Configuration de la période de rétention pour les fichiers de trace et de vidage (p. 777).

Affichage du journal des erreurs SQL Server à l'aide de la procédure rds_read_error_log

Vous pouvez utiliser la procédure stockée Amazon RDS `rds_read_error_log` pour afficher les journaux des erreurs et les journaux de l'agent. Pour plus d'informations, consultez Affichage des journaux des erreurs et des agents (p. 777).

Publication de journaux SQL Server dans Amazon CloudWatch Logs

Avec Amazon RDS pour SQL Server, vous pouvez publier des événements de journal des erreurs et de l'agent directement sur Amazon CloudWatch Logs. Analysez les données de journaux avec CloudWatch Logs, puis utilisez CloudWatch pour créer des alarmes et afficher des métriques.

CloudWatch Logs vous permet d'effectuer les actions suivantes :

- Stocker des journaux dans un espace de stockage hautement durable pour lequel vous définissez la période de rétention.
- Chercher et filtrer les données de journaux.
- Partager des données de journaux entre les comptes.
- Exporter des journaux vers Amazon S3.
- Diffuser des données vers Amazon Elasticsearch Service.
- Traiter des données de journaux en temps réel avec Amazon Kinesis Data Streams.

Amazon RDS publie chaque journal de base de données SQL Server sous la forme d'un flux de base de données distinct dans le groupe de journaux. Par exemple, si vous publiez des journaux des erreurs, les données d'erreurs sont stockées dans un flux de journal des erreurs dans le groupe de journaux `/aws/rds/instance/`*`my_instance`*`/error`.

> **Note**
>
> La publication de journaux SQL Server dans CloudWatch Logs n'est pas activée par défaut. La publication de fichiers de trace et de vidage n'est pas prise en charge. La publication de journaux SQL Server dans CloudWatch Logs est prise en charge pour toutes les régions, sauf pour Asie-Pacifique (Hong Kong).

Console

Pour publier des journaux de base de données SQL Server dans CloudWatch Logs à partir d'AWS Management Console

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Bases de données, puis l'instance de base de données que vous souhaitez modifier.
3. Sélectionnez Modify.
4. Dans la section Exportations des journaux, choisissez les journaux que vous voulez commencer à publier dans CloudWatch Logs.

   Vous pouvez sélectionner erreur, agent, ou les deux.
5. Choisissez Continuer, puis Modifier l'instance de base de données sur la page récapitulative.

AWS CLI

Pour publier des journaux SQL Server, vous pouvez utiliser la commande `modify-db-instance` avec les paramètres suivants :

- `--db-instance-identifier`
- `--cloudwatch-logs-export-configuration`

> **Note**
>
> Une modification apportée à l'option `--cloudwatch-logs-export-configuration` est toujours appliquée immédiatement à l'instance de base de données. Par conséquent, les options `--apply-immediately` et `--no-apply-immediately` sont sans effet.

Vous pouvez également publier des journaux SQL Server en utilisant les commandes suivantes :

- `create-db-instance`
- `restore-db-instance-from-db-snapshot`
- `restore-db-instance-to-point-in-time`

Example

L'exemple suivant crée une instance de base de données SQL Server avec la publication CloudWatch Logs activée. La valeur `--enable-cloudwatch-logs-exports` est un tableau de chaînes JSON qui peut inclure `error`, `agent` ou les deux.

Pour Linux, macOS ou 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
```

Pour 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**
>
> Lorsque vous utilisez l'invite de commande Windows, vous devez utiliser des guillemets doubles (") d'échappement dans le code JSON en les préfixant d'une barre oblique inverse (\).

Example

L'exemple suivant modifie une instance de base de données SQL Server existante pour publier les fichiers journaux dans CloudWatch Logs. La valeur `--cloudwatch-logs-export-configuration` n'est pas un objet JSON. La clé pour cet objet est `EnableLogTypes` et sa valeur est un tableau de chaînes qui peut inclure `error`, `agent` ou les deux.

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --cloudwatch-logs-export-configuration '{"EnableLogTypes":["error","agent"]}'
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration "{\"EnableLogTypes\":[\"error\",\"agent\"]}"
```

> **Note**
>
> Lorsque vous utilisez l'invite de commande Windows, vous devez utiliser des guillemets doubles (") d'échappement dans le code JSON en les préfixant d'une barre oblique inverse (\).

Example

L'exemple suivant modifie une instance de base de données SQL Server existante pour désactiver la publication de fichiers journaux d'agent dans CloudWatch Logs. La valeur `--cloudwatch-logs-export-configuration` n'est pas un objet JSON. La clé pour cet objet est `DisableLogTypes` et sa valeur est un tableau de chaînes qui peut inclure `error`, `agent` ou les deux.

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --cloudwatch-logs-export-configuration '{"DisableLogTypes":["agent"]}'
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration "{\"DisableLogTypes\":[\"agent\"]}"
```

> **Note**
>
> Lorsque vous utilisez l'invite de commande Windows, vous devez utiliser des guillemets doubles (") d'échappement dans le code JSON en les préfixant d'une barre oblique inverse (\).

Fichiers journaux de base de données MySQL

Vous pouvez contrôler le journal des erreurs, le journal des requêtes lentes et le journal général MySQL. Le fichier journal des erreurs MySQL est généré par défaut ; vous pouvez générer les journaux des requêtes lentes et général en définissant des paramètres dans votre groupe de paramètres de base de données que vous créez pour vos instances MySQL. Amazon RDS fait tourner tous les fichiers de journaux MySQL. Les intervalles pour chaque type sont indiquées ci-après.

Vous pouvez surveiller les journaux MySQL directement via la console Amazon RDS, l'API Amazon RDS, l'interface en ligne de commande AWS CLI ou les SDK AWS. Vous pouvez également accéder aux journaux MySQL en dirigeant les journaux vers une table de base de données de la base de données principale et interroger cette table. Vous pouvez utiliser l'utilitaire mysqlbinlog pour télécharger un journal binaire.

Pour plus d'informations sur l'affichage, le téléchargement ou la consultation des journaux de base de données basés sur des fichiers, consultez Amazon RDS Fichiers journaux de base de données (p. 490).

Rubriques

- Accès aux journaux d'erreurs MySQL (p. 507)
- Accès au journal des requêtes lentes et au journal général MySQL (p. 507)
- Accès au journal d'audit MySQL (p. 509)
- Publication des journaux MySQL dans CloudWatch Logs (p. 509)
- Taille des fichiers journaux (p. 512)
- Gestion des journaux MySQL sous forme de table (p. 512)
- Format de journalisation binaire (p. 513)
- Accès aux journaux binaires MySQL (p. 514)

Accès aux journaux d'erreurs MySQL

Le journal des erreurs MySQL est écrit dans le fichier `mysql-error.log`. Vous pouvez afficher `mysql-error.log` à l'aide de la console Amazon RDS ou en récupérant le journal à l'aide de l'API Amazon RDS, de l'interface de ligne de commande Amazon RDS ou des SDK AWS. `mysql-error.log` est vidé toutes les 5 minutes et son contenu est ajouté à `mysql-error-running.log`. Le fichier `mysql-error-running.log` fait ensuite l'objet d'une rotation toutes les heures et les fichiers générés toutes les heures au cours des 24 dernières heures sont conservés. Veuillez noter que la période de rétention est différente pour Amazon RDS et pour Aurora.

Le nom du fichier journal comporte l'heure à laquelle le fichier a été généré (au format UTC). Les fichiers journaux comportent également un horodatage permettant de déterminer le moment où les entrées du journal ont été écrites.

MySQL écrit des informations dans le journal des erreurs uniquement au moment du démarrage, de l'arrêt et lorsqu'une erreur survient. Une instance de base de données peut fonctionner pendant des heures ou des jours sans qu'aucune nouvelle entrée soit écrite dans le journal des erreurs. Si aucune entrée récente ne figure, cela signifie que le serveur n'a pas rencontré d'erreur justifiant une entrée de journal.

Accès au journal des requêtes lentes et au journal général MySQL

Le journal des requêtes lentes et le journal général MySQL peuvent être écrits dans un fichier ou dans une table de base de données en définissant les paramètres nécessaires dans votre groupe de paramètres DB. Pour plus d'informations sur la création et la modification d'un groupe de paramètres DB, consultez Utilisation de groupes de paramètres de base de données (p. 225). Vous devez définir ces paramètres avant de pouvoir consulter le journal des requêtes lentes ou le journal général dans la console Amazon RDS ou à l'aide de l'API Amazon RDS, de l'interface de ligne de commande Amazon RDS ou des SDK AWS.

Vous pouvez contrôler la journalisation MySQL à l'aide des paramètres de cette liste :

- `slow_query_log` : Pour créer le journal des requêtes lentes, définir sur 1. La valeur par défaut est 0.
- `general_log` : Pour créer le journal général, définir sur 1. La valeur par défaut est 0.
- `long_query_time` : Pour empêcher l'enregistrement des requêtes rapides dans le journal des requêtes lentes, indiquez la valeur de la durée d'exécution de requête la plus courte devant être enregistrée, en secondes. La valeur par défaut est de 10 secondes et la valeur minimum est 0. Si log_output = FILE, vous pouvez indiquer une valeur à virgule flottante avec une résolution en microseconde. Si log_output = TABLE, vous devez indiquer un nombre entier avec une résolution en seconde. Seules les requêtes dont la durée d'exécution dépasse la valeur `long_query_time` sont enregistrées. Par exemple, si vous définissez `long_query_time` sur 0,1, les requêtes s'exécutant pendant moins de 100 millisecondes ne sont pas enregistrées.

- `log_queries_not_using_indexes` : Pour enregistrer toutes les requêtes n'utilisant pas d'index dans le journal des requêtes lentes, définir sur 1. La valeur par défaut est 0. Les requêtes n'utilisant pas d'index sont enregistrées même si la durée de leur exécution est inférieure à la valeur du paramètre `long_query_time`.
- `log_output` *`option`* : Vous pouvez spécifier l'une des options suivantes pour le paramètre `log_output`.
  - TABLEAU (par défaut) – Écrit les requêtes générales dans le tableau `mysql.general_log` et les requêtes lentes dans le tableau `mysql.slow_log`.
  - FICHIER – Écrit les fichiers des requêtes générales et lentes dans le fichier système. Les fichiers journaux font l'objet d'une rotation horaire.
  - AUCUNE– Désactive la journalisation.

Lorsque la journalisation est activée, Amazon RDS effectue une rotation des journaux des tables ou supprime les fichiers journaux à intervalles réguliers. Cette précaution permet de limiter la possibilité qu'un fichier journal volumineux ne bloque l'utilisation de la base de données ou n'affecte les performances. Rotation et suppression de l'approche de journalisation `FILE` et `TABLE` comme suit :

- Lorsque la journalisation `FILE` est activée, les fichiers journaux sont examinés toutes les heures et ceux dont l'ancienneté est supérieure à 24 heures sont supprimés. Dans certains cas, la taille des fichiers journaux combinés restant après la suppression peut dépasser le seuil de 2 % de l'espace alloué à une instance de base de données. Dans ces cas, les fichiers journaux les plus volumineux sont supprimés jusqu'à ce que la taille des fichiers journaux ne soit plus supérieure au seuil.
- Lorsque la journalisation de `TABLE` est activée, les journaux des tables font dans certains cas l'objet d'une rotation toutes les 24 heures. Cette rotation se produit si l'espace utilisé par les journaux des tables est supérieur à 20 % de l'espace de stockage alloué ou si la taille de l'ensemble des journaux est supérieure à 10 Go. Si l'espace utilisé pour une instance de base de données est supérieur à 90 % de l'espace de stockage alloué à l'instance de base de données, alors les seuils correspondant à la rotation des journaux est réduite. Les tables de journaux font alors l'objet d'une rotation si l'espace utilisé par les journaux des tables est supérieur à 10 % de l'espace de stockage alloué ou si la taille de l'ensemble des journaux est supérieure à 5 Go. Vous pouvez vous abonner à l'événement `low_free_storage` pour être informé lorsque les tables de journal font l'objet d'une rotation pour libérer de l'espace. Pour plus d'informations, consultez Utilisation de la notification d'événement Amazon RDS (p. 467).

  Lors de la rotation des tables de journaux, la table de journal actuelle est copiée vers une table de journal de sauvegarde et les entrées de la table de journal actuelle sont supprimées. Si la table de journal de sauvegarde existe déjà, elle est supprimée avant que la table de journal actuelle ne soit copiée dans la sauvegarde. Si besoin, vous pouvez interroger la table de journal de sauvegarde. La table de journal de sauvegarde de la table `mysql.general_log` est nommée `mysql.general_log_backup`. La table de journal de sauvegarde de la table `mysql.slow_log` est nommée `mysql.slow_log_backup`.

  Vous pouvez effectuer une rotation de la table `mysql.general_log` en appelant la procédure `mysql.rds_rotate_general_log`. Vous pouvez effectuer une rotation de la table `mysql.slow_log` en appelant la procédure `mysql.rds_rotate_slow_log`.

  La rotation des journaux des tables est effectuée pendant la mise à niveau de la version d'une base de données.

Pour utiliser les journaux depuis la console Amazon RDS, l'API Amazon RDS, la CLI Amazon RDS ou les kits SDK AWS, définissez le paramètre `log_output` sur FILE. A l'instar du journal des erreurs MySQL, ces fichiers journaux font l'objet d'une rotation horaire. Les fichiers journaux qui ont été générés au cours des dernières 24 heures sont conservés. Veuillez noter que la période de rétention est différente pour Amazon RDS et pour Aurora.

Pour plus d'informations sur le journal des requêtes lentes et le journal général, accédez aux rubriques suivantes dans la documentation MySQL :

- Journal des requêtes lentes
- Journal des requêtes générales

Accès au journal d'audit MySQL

Pour accéder au journal d'audit, l'instance de base de données doit utiliser un groupe d'options personnalisé avec l'option `MARIADB_AUDIT_PLUGIN`. Pour de plus amples informations, veuillez consulter Prise en charge du plug-in d'audit MariaDB (p. 874).

Publication des journaux MySQL dans CloudWatch Logs

Vous pouvez configurer votre instance de base de données MySQL Amazon RDS de sorte à publier des données de journaux dans un groupe de journaux dans Amazon CloudWatch Logs. CloudWatch Logs vous permet d'effectuer une analyse en temps réel des données de journaux et d'utiliser CloudWatch pour créer des alarmes et afficher des métriques. CloudWatch Logs permet de conserver les enregistrements des journaux dans une solution de stockage hautement durable.

Amazon RDS publie chaque journal de base de données MySQL sous la forme d'un flux de base de données distinct dans le groupe de journaux. Par exemple, si vous configurez la fonction d'exportation de sorte à inclure le journal de requêtes lentes, les données de requêtes lentes sont stockées dans un flux de journal de requêtes lentes dans le groupe de journaux `/aws/rds/instance/`*`my_instance`*`/slowquery`.

Le journal d'erreurs est activé par défaut. Le tableau ci-dessous récapitule les conditions requises pour les autres journaux MySQL.

Log	Exigence
Journal d'audit	L'instance de base de données doit disposer d'un groupe d'options personnalisées avec l'option `MARIADB_AUDIT_PLUGIN`.
Journal général	L'instance de base de données doit disposer d'un groupe de paramètres personnalisés avec le paramètre `general_log = 1` pour autoriser la journalisation générale.
Journal des requêtes lentes	L'instance de base de données doit disposer d'un groupe de paramètres personnalisés avec le paramètre `slow_query_log = 1` pour autoriser la journalisation de requête lente.
Sortie de journal	L'instance de base de données doit disposer d'un groupe de paramètres personnalisés avec le paramètre `log_output = FILE` pour écrire de journaux dans le système de fichier et les publier dans CloudWatch Logs.

> **Note**
>
> La publication de fichiers journaux dans CloudWatch Logs n'est prise en charge pour les versions 5.6, 5.7 et 8.0 de MySQL.

Console

Pour publier des journaux MySQL dans CloudWatch Logs à l'aide de la console

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Bases de données, puis l'instance de base de données que vous souhaitez modifier.
3. Sélectionnez Modify.
4. Dans la section Exportations des journaux, choisissez les journaux que vous voulez commencer à publier dans CloudWatch Logs.
5. Choisissez Continuer, puis Modifier l'instance de base de données sur la page récapitulative.

AWS CLI

Vous pouvez publier des journaux MySQL avec l'interface de ligne de commande AWS. Vous pouvez appeler la commande `modify-db-instance` avec les paramètres suivants :

- `--db-instance-identifier`
- `--cloudwatch-logs-export-configuration`

> **Note**
>
> Une modification apportée à l'option `--cloudwatch-logs-export-configuration` est toujours appliquée immédiatement à l'instance de base de données. Par conséquent, les options `--apply-immediately` et `--no-apply-immediately` sont sans effet.

Vous pouvez également publier des journaux MySQL en appelant les commandes de l'interface de ligne de commande AWS suivantes :

- `create-db-instance`
- `restore-db-instance-from-db-snapshot`
- `restore-db-instance-from-s3`
- `restore-db-instance-to-point-in-time`

Exécutez l'une de ces commandes de l'interface de ligne de commande AWS avec les options suivantes :

- `--db-instance-identifier`
- `--enable-cloudwatch-logs-exports`
- `--db-instance-class`
- `--engine`

D'autres options peuvent être requises en fonction de la commande d'interface de ligne de commande AWS que vous exécutez.

Example

L'exemple suivant modifie une instance de base de données MySQL existante pour publier les fichiers journaux dans CloudWatch Logs. La valeur `--cloudwatch-logs-export-configuration` n'est pas un objet JSON. La clé pour cet objet est `EnableLogTypes` et sa valeur est un tableau de chaînes avec une combinaison quelconque de `audit`, `error`, `general` et `slowquery`.

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --cloudwatch-logs-export-configuration '{"EnableLogTypes":
["audit","error","general","slowquery"]}'
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration '{"EnableLogTypes":
["audit","error","general","slowquery"]}'
```

Example

L'exemple suivant crée une instance de base de données MySQL et publie les fichiers journaux dans CloudWatch Logs. La valeur `--enable-cloudwatch-logs-exports` est un tableau de chaînes JSON. Les chaînes peuvent être une combinaison de `audit`, `error`, `general` et `slowquery`.

Pour Linux, macOS ou 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
```

Pour 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
```

API RDS

Vous pouvez publier des journaux MySQL avec l'API RDS. Vous pouvez appeler l'action `ModifyDBInstance` avec les paramètres suivants :

- `DBInstanceIdentifier`
- `CloudwatchLogsExportConfiguration`

> **Note**
>
> Une modification apportée au paramètre `CloudwatchLogsExportConfiguration` est toujours appliquée immédiatement à l'instance de base de données. Par conséquent, le paramètre `ApplyImmediately` est sans effet.

Vous pouvez également publier des journaux MySQL en appelant les opérations d'API RDS suivantes :

- `CreateDBInstance`

- `RestoreDBInstanceFromDBSnapshot`
- `RestoreDBInstanceFromS3`
- `RestoreDBInstanceToPointInTime`

Exécutez l'une de ces opérations d'API RDS avec les paramètres suivants :

- `DBInstanceIdentifier`
- `EnableCloudwatchLogsExports`
- `Engine`
- `DBInstanceClass`

D'autres paramètres peuvent être requis en fonction de la commande d'interface de ligne de commande AWS que vous exécutez.

Taille des fichiers journaux

Les tailles du journal des requêtes lentes, du journal des erreurs et du journal général MySQL sont limitées à 2 %maximum de l'espace de stockage alloué à une instance de base de données. Pour respecter ce seuil, les journaux font l'objet d'une rotation automatique toutes les heures et les fichiers dont l'ancienneté est supérieure à 24 heures sont supprimés. Si la taille de l'ensemble des fichiers journaux après la suppression dépasse le seuil, les fichiers journaux les plus volumineux sont supprimés jusqu'à ce que la taille des fichiers journaux ne soit plus supérieure au seuil.

Pour MySQL, une taille limite est appliquée aux objets BLOB écrits dans le fichier journal redo. Pour prendre en compte cette limite, vérifiez que le paramètre `innodb_log_file_size` de votre instance de base de données MySQL est dix fois supérieur à la taille des données BLOB les plus volumineuses figurant dans vos tables, plus la longueur des autres champs de longueur variable (`VARCHAR`, `VARBINARY`, `TEXT`) dans ces tables. Pour plus d'informations sur la manière de définir les valeurs des paramètres, consultez Utilisation de groupes de paramètres de base de données (p. 225). Pour plus d'informations sur la taille limite des objets BLOB du fichier journal redo, accédez à Changements dans MySQL 5.6.20.

Gestion des journaux MySQL sous forme de table

Vous pouvez diriger le journal des requêtes lentes et le journal général vers des tables sur l'instance de base de données en créant un groupe de paramètres DB et en définissant le paramètre du serveur `log_output` sur `TABLE`. Les requêtes générales sont ensuite enregistrées dans la table `mysql.general_log` et les requêtes lentes dans la table `mysql.slow_log`. Vous pouvez interroger les tables pour accéder aux informations des journaux. L'activation de cette journalisation augmente le volume de données écrites dans la base de données, ce qui peut dégrader les performances.

Par défaut, le journal général et le journal des requêtes lentes sont désactivés. Afin d'activer la journalisation dans les tables, vous devez également définir les paramètres `general_log` et `slow_query_log` sur `1`.

Les tables de journaux continuent de grossir jusqu'à ce que les activités de journalisation correspondantes soient désactivées en redéfinissant le paramètre approprié sur `0`. Avec le temps, une grande quantité de données s'accumule et risque d'utiliser une part considérable de l'espace de stockage alloué. Amazon RDS ne vous permet pas de tronquer les tableaux de journaux, mais vous pouvez déplacer leurs contenus. Lorsque vous procédez à la rotation d'une table, son contenu est enregistré dans une table de sauvegarde et une nouvelle table de journal vide est créée. Vous pouvez effectuer une rotation manuelle des tables de journaux avec les procédures de ligne de commande suivantes, dans lesquelles l'invite de commande est indiquée par `PROMPT>` :

```
PROMPT> CALL mysql.rds_rotate_slow_log;
```

```
PROMPT> CALL mysql.rds_rotate_general_log;
```

Pour supprimer totalement les anciennes données et récupérer l'espace de disque, appelez deux fois à la suite la procédure appropriée.

Format de journalisation binaire

MySQL sur Amazon RDS prend en charge les formats de journalisation binaire basés sur les lignes, basés sur les instructions et mixtes pour les versions MySQL 5.6 et ultérieures. Le format de journalisation binaire par défaut est « mixte ». Pour les instances de bases de données s'exécutant sur les versions MySQL 5.1 et 5.5, seule la journalisation binaire est prise en charge. Pour plus de détails sur les différents formats de journalisation binaire MySQL, veuillez consulter Binary Logging Formats de la documentation MySQL.

Si vous prévoyez d'utiliser la réplication, le format de journalisation binaire est important car il détermine le dossier de modifications de données qui est enregistré dans la source et envoyés aux cibles de réplication. Pour de plus amples informations sur les avantages et les inconvénients des différents formats de journalisation binaire pour la réplication, veuillez consulter la section Advantages and Disadvantages of Statement-Based and Row-Based Replication de la documentation MySQL.

> **Important**
>
> Lorsque vous définissez le format de journalisation binaire sur « basé sur les lignes », vous risquez de générer des fichiers journaux binaires très volumineux. Ces derniers réduisent le stockage disponible pour une instance de base de données et peuvent augmenter la durée nécessaire pour effectuer une opération de restauration d'une instance de base de données. La réplication basée sur les instructions peut provoquer des incohérences entre l'instance de base de données source et un réplica en lecture. Pour de plus amples informations, veuillez consulter Determination of Safe and Unsafe Statements in Binary Logging dans la documentation MySQL.

Pour définir le format de journalisation binaire MySQL

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes de paramètres.
3. Choisissez le groupe de paramètres utilisé par l'instance de base de données que vous souhaitez modifier.

   Vous ne pouvez pas modifier un groupe de paramètres par défaut. Si l'instance de base de données utilise un groupe de paramètres par défaut, créez un nouveau groupe et associez-le à l'instance.

   Pour plus d'informations sur les groupes de paramètres, consultez Utilisation de groupes de paramètres de base de données (p. 225).
4. Dans Parameter group actions (Actions de groupe de paramètres), choisissez Edit (Modifier).
5. Définissez le paramètre `binlog_format` au format de journalisation binaire de votre choix (ROW, STATEMENT ou MIXED).
6. Choisissez Enregistrer les modifications pour enregistrer les mises à jour apportées au groupe de paramètres de de base de données.

> **Important**
>
> La modification d'un groupe de paramètres de base de données affecte toutes les instances de base de données qui utilisent ce dernier. Si vous souhaitez spécifier des formats de journalisation binaire différents pour différentes instances de base de données MySQL dans une région AWS, les instances de base de données doivent utiliser différents groupes de paramètres de base de données. Ces groupes de paramètres identifient différents formats de journalisation. Affectez le groupe de paramètres de base de données approprié à chaque instance de base de données.

Accès aux journaux binaires MySQL

Vous pouvez utiliser l'utilitaire mysqlbinlog pour télécharger ou diffuser des journaux binaires à partir d'instances Amazon RDS exécutant la version MySQL 5.6 ou une version ultérieure. Le journal binaire est téléchargé dans votre ordinateur local et vous pouvez effectuer des actions comme relire le journal à l'aide de l'utilitaire mysql. Pour de plus amples informations sur l'utilisation de l'utilitaire mysqlbinlog, veuillez accéder à Utilisation de mysqlbinlog pour sauvegarder les fichiers journaux binaires.

Pour exécuter à nouveau l'utilitaire mysqlbinlog sur une instance Amazon RDS, utilisez les options suivantes :

- Spécifiez l'option `--read-from-remote-server`.
- `--host` : Spécifiez le nom DNS du point de terminaison de l'instance.
- `--port` : Spécifiez le port utilisé par l'instance.
- `--user` : Spécifiez un utilisateur MySQL ayant l'autorisation de réplication esclave.
- `--password` : Spécifiez le mot de passe de l'utilisateur ou omettez la valeur de mot de passe pour que l'utilitaire vous invite à saisir un mot de passe.
- Pour que le fichier soit téléchargé au format binaire, spécifiez l'option `--raw`.
- `--result-file` : Spécifiez le fichier local qui recevra la sortie brute.
- Spécifiez les noms pour un ou plusieurs fichiers journaux binaires. Pour obtenir la liste des journaux disponibles, utilisez la commande SQL SHOW BINARY LOGS.
- Pour diffuser les fichiers journaux binaires, spécifiez l'option `--stop-never`.

Pour de plus amples informations sur les options mysqlbinlog, veuillez accéder à mysqlbinlog - Utilitaire de traitement des fichiers journaux binaires.

Par exemple, consultez ce qui suit.

Pour Linux, macOS ou Unix :

```
mysqlbinlog \
    --read-from-remote-server \
    --host=MySQL56Instance1.cg034hpkmmjt.region.rds.amazonaws.com \
    --port=3306  \
    --user ReplUser \
    --password \
    --raw \
    --result-file=/tmp/ \
    binlog.00098
```

Pour Windows :

```
mysqlbinlog ^
    --read-from-remote-server ^
    --host=MySQL56Instance1.cg034hpkmmjt.region.rds.amazonaws.com ^
    --port=3306  ^
    --user ReplUser ^
    --password ^
    --raw ^
    --result-file=/tmp/ ^
    binlog.00098
```

Amazon RDS purge normalement un journal binaire dès que possible, mais le journal binaire doit toujours être disponible sur l'instance afin que mysqlbinlog puisse y accéder. Pour spécifier le nombre d'heures pendant lesquelles RDS conservera les journaux binaires, utilisez la procédure stockée `mysql.rds_set_configuration` et spécifiez une période suffisamment longue pour pouvoir

télécharger les journaux. Après avoir défini la période de rétention, surveillez l'utilisation du stockage de l'instance de base de données afin de garantir que les journaux binaires conservés n'utilisent pas un espace de stockage trop grand.

> **Note**
>
> La procédure stockée `mysql.rds_set_configuration` est uniquement disponible pour les versions MySQL 5.6 ou ultérieures.

L'exemple suivant définit la période de conservation sur 1 jour.

```
call mysql.rds_set_configuration('binlog retention hours', 24);
```

Pour afficher les paramètres actuels, utilisez la procédure stockée `mysql.rds_show_configuration`.

```
call mysql.rds_show_configuration;
```

Fichiers journaux de base de données Oracle

Vous pouvez accéder aux journaux des alertes, aux fichiers d'audits et aux fichiers de trace Oracle à l'aide de la console Amazon RDS ou de l'API. Pour plus d'informations sur l'affichage, le téléchargement ou la consultation des journaux de base de données basés sur des fichiers, consultez Amazon RDS Fichiers journaux de base de données (p. 490).

Les fichiers d'audit Oracle fournis sont les fichiers d'audit Oracle standard. Amazon RDS prend en charge la fonction d'audit fine (FGA) Oracle. Cependant, l'accès aux journaux ne donne pas accès aux événements FGA stockés dans la table `SYS.FGA_LOG$`, accessibles via la vue `DBA_FGA_AUDIT_TRAIL`.

L'opération de l'API `DescribeDBLogFiles` qui répertorie les fichiers journaux Oracle disponibles pour une instance de base de données ignore le paramètre `MaxRecords` et renvoie jusqu'à 1 000 enregistrements.

Programme de rétention

Le moteur de base de données Oracle peut peut-être procéder à la rotation des fichiers journaux si leur volume devient très important. Pour conserver les fichiers d'audit ou de trace, vous devez les télécharger. Si vous stockez les fichiers localement, vous réduisez vos coûts de stockage Amazon RDS et libérez plus d'espace pour vos données.

Le tableau suivant présente le programme de rétention des journaux d'alertes, des fichiers d'audit et des fichiers de trace Oracle sur Amazon RDS.

Log type (Type de journal)	Programme de rétention
Journaux des alertes	Le journal d'alerte de texte fait l'objet d'une rotation quotidienne avec une conservation de 30 jours gérée par Amazon RDS. Le journal d'alerte XML est conservé au moins 7 jours. Vous pouvez accéder à ce journal grâce à la vue `ALERTLOG`.
Fichiers d'audit	La période de rétention par défaut des fichiers d'audit est de sept jours. Il se peut que Amazon RDS supprime des fichiers d'audit de plus de sept jours d'âge.
Fichiers de trace	La période de rétention par défaut des fichiers de trace est de sept jours. Il se peut que Amazon RDS supprime des fichiers de trace de plus de sept jours d'âge.

Log type (Type de journal)	Programme de rétention
Journaux de l'écouteur	La période de rétention par défaut des journaux d'écoute est de sept jours. Il se peut que Amazon RDS supprime des journaux d'écoute de plus de sept jours d'âge.

Note

Les fichiers d'audit et les fichiers de trace partagent la même configuration de rétention.

Changement de fichiers journaux en ligne

Vous pouvez utiliser la procédure Amazon RDS `rdsadmin.rdsadmin_util.switch_logfile` pour changer des fichiers journaux en ligne. Pour plus d'informations, consultez Changement de fichiers journaux en ligne (p. 1131).

Récupération des journaux redo archivés

Vous pouvez conserver les journaux redo archivés. Pour plus d'informations, consultez Conservation des journaux redo archivés (p. 1134).

Utilisation des fichiers de trace Oracle

Vous trouverez ci-après de descriptions de procédures Amazon RDS permettant de créer, d'actualiser, de supprimer les fichiers de trace ou d'y accéder.

Liste de fichiers

Vous pouvez utiliser l'une ou l'autre de deux procédures permettent d'accéder à tous les fichiers dans le chemin `background_dump_dest`. La première actualise la liste de l'ensemble des fichiers actuellement dans `background_dump_dest`.

```
EXEC rdsadmin.manage_tracefiles.refresh_tracefile_listing;
```

Une fois la liste actualisée, interrogez la vue suivante pour accéder aux résultats.

```
SELECT * FROM rdsadmin.tracefile_listing;
```

Vous pouvez également utiliser `FROM table` pour diffuser des données non relationnelles dans un format de table afin de répertorier le contenu de l'annuaire de bases de données.

```
SELECT * FROM TABLE(rdsadmin.rds_file_util.listdir('BDUMP'));
```

La requête suivante affiche le texte d'un fichier journal.

```
SELECT text FROM
 TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP','alert_dbname.log.date'));
```

Sur un réplica en lecture, obtenez le nom du répertoire BDUMP en interrogeant `V$DATABASE.DB_UNIQUE_NAME`. Si le nom unique est `DATABASE_B`, le répertoire BDUMP est `BDUMP_B`. L'exemple suivant interroge le nom BDUMP sur un réplica, puis utilise ce nom pour interroger le contenu de `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'));
```

Génération de fichiers de trace et suivi d'une session

Puisqu'il n'existe aucune restriction sur `ALTER SESSION`, un grand nombre de méthodes standard permettant de générer des fichiers de trace dans Oracle restent disponibles pour les instances de base de données Amazon RDS. Les procédures suivantes sont fournies pour les fichiers de trace pour lesquels l'accès doit être élargi.

Méthode Oracle	Méthode Amazon RDS
`oradebug hanganalyze 3`	`EXEC rdsadmin.manage_tracefiles.hanganalyze;`
`oradebug dump systemstate 266`	`EXEC rdsadmin.manage_tracefiles.dump_systemstate;`

Vous pouvez utiliser de nombreuses méthodes standard pour suivre des sessions individuelles connectées à une instance de base de données Oracle dans Amazon RDS. Pour activer le suivi d'une session, vous pouvez exécuter des sous-programmes dans des packages PL/SQL fournis par Oracle, tels que `DBMS_SESSION` et `DBMS_MONITOR`. Pour plus d'informations, consultez Activation du suivi d'une session dans la documentation d'Oracle.

Récupération de fichiers de trace

Vous pouvez récupérer tous les fichiers dans `background_dump_dest` à l'aide d'une requête SQL standard sur un tableau Amazon RDS externe gérée. Pour utiliser cette méthode, vous devez exécuter la procédure définissant l'emplacement de cette table sur le fichier de trace spécifique.

Par exemple, vous pouvez utiliser la vue `rdsadmin.tracefile_listing` indiquée ci-dessus pour répertorier tous les fichiers de trace sur le système. Vous pouvez ensuite définir la vue `tracefile_table` afin qu'elle pointe vers le fichier de trace souhaité à l'aide de la procédure suivante.

```
EXEC
 rdsadmin.manage_tracefiles.set_tracefile_table_location('CUST01_ora_3260_SYSTEMSTATE.trc');
```

L'exemple suivant créé une table externe selon le schéma actuel. L'emplacement est défini sur le fichier fourni. Vous pouvez récupérer le contenu dans un fichier local à l'aide d'une requête SQL.

```
SPOOL /tmp/tracefile.txt
SELECT * FROM tracefile_table;
SPOOL OFF;
```

Purge des fichiers de trace

Les fichiers de traçage peuvent accumuler et consommer de l'espace de disque. Amazon RDS purge les fichiers de trace par défaut, ainsi que les fichiers journaux dont l'ancienneté est supérieure à sept jours. Vous pouvez afficher et définir la période de rétention des fichiers à l'aide de la procédure

`show_configuration`. Vous devez exécuter la commande `SET SERVEROUTPUT ON` afin de pouvoir afficher les résultats de la configuration.

L'exemple suivant affiche la période de rétention des fichiers de trace actuelle, puis définit une nouvelle période.

```
# 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
 bdump are automatically deleted.

# Set the tracefile retention to 24 hours:
SQL> EXEC rdsadmin.rdsadmin_util.set_configuration('tracefile retention',1440);

#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
 bdump are automatically deleted.
```

En complément du processus de purge périodique, vous pouvez supprimer manuellement des fichiers de `background_dump_dest`. L'exemple suivant montre comment purger tous les fichiers datant de plus de cinq minutes.

```
EXEC rdsadmin.manage_tracefiles.purge_tracefiles(5);
```

Vous pouvez également purger tous les fichiers correspondant à un modèle spécifique (dans ce cas, n'incluez pas l'extension de fichier, par exemple .trc). L'exemple suivant montre comment purger tous les fichiers commençant par `SCHPOC1_ora_5935`.

```
EXEC rdsadmin.manage_tracefiles.purge_tracefiles('SCHPOC1_ora_5935');
```

Publication des journaux Oracle dans Amazon CloudWatch Logs

Vous pouvez configurer votre instance de base de données Oracle Amazon RDS de sorte à publier des données de journaux dans un groupe de journaux dans Amazon CloudWatch Logs. CloudWatch Logs vous permet d'analyser les données de journaux et d'utiliser CloudWatch pour créer des alarmes et afficher des métriques. CloudWatch Logs permet de conserver les enregistrements des journaux dans une solution de stockage hautement durable.

Amazon RDS publie chaque journal de base de données Oracle sous la forme d'un flux de base de données distinct dans le groupe de journaux. Par exemple, si vous configurez la fonction d'exportation de sorte à inclure le journal d'audit, les données d'audit sont stockées dans un flux de journal d'audit dans le groupe de journaux `/aws/rds/instance/my_instance/audit`.

Console

Pour publier des journaux de base de données Oracle dans CloudWatch Logs à partir d'AWS Management Console

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Bases de données, puis l'instance de base de données que vous souhaitez modifier.
3. Sélectionnez Modify.

4. Dans la section Exportations des journaux, choisissez les journaux que vous voulez commencer à publier dans CloudWatch Logs.
5. Choisissez Continuer, puis Modifier l'instance de base de données sur la page récapitulative.

AWS CLI

Pour publier les journaux Oracle vous pouvez utiliser la commande `modify-db-instance` avec les paramètres suivants :

- `--db-instance-identifier`
- `--cloudwatch-logs-export-configuration`

> **Note**
>
> Une modification apportée à l'option `--cloudwatch-logs-export-configuration` est toujours appliquée immédiatement à l'instance de base de données. Par conséquent, les options `--apply-immediately` et `--no-apply-immediately` sont sans effet.

Vous pouvez également publier des journaux Oracle en utilisant les commandes suivantes :

- `create-db-instance`
- `restore-db-instance-from-db-snapshot`
- `restore-db-instance-from-s3`
- `restore-db-instance-to-point-in-time`

Example

L'exemple suivant crée une instance de base de données Oracle avec la publication CloudWatch Logs activée. La valeur `--enable-cloudwatch-logs-exports` est un tableau de chaînes JSON. Les chaînes peuvent être une combinaison de `alert`, `audit`, `listener` et `trace`.

Pour Linux, macOS ou Unix :

```
aws rds create-db-instance \
    --db-instance-identifier mydbinstance \
    --enable-cloudwatch-logs-exports '["trace","audit","alert","listener"]' \
    --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
```

Pour Windows :

```
aws rds create-db-instance ^
    --db-instance-identifier mydbinstance ^
    --enable-cloudwatch-logs-exports trace alert audit listener ^
    --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

L'exemple suivant modifie une instance de base de données Oracle existante pour publier les fichiers journaux dans CloudWatch Logs. La valeur `--cloudwatch-logs-export-configuration` n'est pas un objet JSON. La clé pour cet objet est `EnableLogTypes` et sa valeur est un tableau de chaînes avec une combinaison quelconque de `alert`, `audit`, `listener` et `trace`.

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --cloudwatch-logs-export-configuration '{"EnableLogTypes":
["trace","alert","audit","listener"]}'
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration EnableLogTypes=\"trace\",\"alert\",\"audit\",
\"listener\"
```

Example

L'exemple suivant modifie une instance de base de données Oracle existante pour désactiver la publication de fichiers journaux d'audit et d'écouteur dans CloudWatch Logs. La valeur `--cloudwatch-logs-export-configuration` n'est pas un objet JSON. La clé pour cet objet est `DisableLogTypes` et sa valeur est un tableau de chaînes avec une combinaison quelconque de `alert`, `audit`, `listener` et `trace`.

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --cloudwatch-logs-export-configuration '{"DisableLogTypes":["audit","listener"]}'
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration DisableLogTypes=\"audit\",\"listener\"
```

API RDS

Vous pouvez publier des journaux Oracle Database avec l'API RDS. Vous pouvez appeler l'action `ModifyDBInstance` avec les paramètres suivants :

- `DBInstanceIdentifier`
- `CloudwatchLogsExportConfiguration`

> **Note**
>
> Une modification apportée au paramètre `CloudwatchLogsExportConfiguration` est toujours appliquée immédiatement à l'instance de base de données. Par conséquent, le paramètre `ApplyImmediately` est sans effet.

Vous pouvez également publier des journaux Oracle en appelant les opérations de l'API RDS suivantes :

- `CreateDBInstance`
- `RestoreDBInstanceFromDBSnapshot`
- `RestoreDBInstanceFromS3`
- `RestoreDBInstanceToPointInTime`

Exécutez l'une de ces opérations d'API RDS avec les paramètres suivants :

- `DBInstanceIdentifier`
- `EnableCloudwatchLogsExports`
- `Engine`
- `DBInstanceClass`

D'autres paramètres peuvent être requis en fonction de l'opération RDS que vous exécutez.

Méthodes précédentes pour accéder aux journaux des alertes et aux journaux de l'écouteur

Vous pouvez consulter le journal d'alertes à l'aide de la console Amazon RDS. Vous pouvez également utiliser l'instruction SQL suivante pour accéder au journal d'alertes.

```
SELECT message_text FROM alertlog;
```

La vue `listenerlog` contient des entrées pour Oracle Database version 12.1.0.2 et antérieure. Pour accéder au journal de l'écouteur pour ces versions de base de données, utilisez la requête suivante.

```
SELECT message_text FROM listenerlog;
```

Pour Oracle Database versions 12.2.0.1 et ultérieures, accédez au journal de l'écouteur via Amazon CloudWatch Logs.

> **Note**
>
> Oracle procède à la rotation des journaux des alertes et de l'écouteur lorsqu'ils dépassent 10 Mo. A ce moment là, ils ne sont pas disponibles dans les vues Amazon RDS.

Fichiers journaux de base de données PostgreSQL

Amazon RDS for PostgreSQL génère des journaux de requêtes et des erreurs. RDS PostgreSQL écrit les informations relatives au processus autovacuum et les actions rds_admin dans le journal des erreurs. PostgreSQL consigne également les connexions, les déconnexions et les points de contrôle dans le journal des erreurs. Pour plus d'informations, consultez la section Error Reporting and Logging dans la documentation PostgreSQL.

Pour définir les paramètres de journalisation d'une instance de base de données, définissez les paramètres dans un groupe de paramètres de base de données et associez-le à l'instance de base de données. Pour plus d'informations, consultez Utilisation de groupes de paramètres de base de données (p. 225).

Rubriques

- Définition de la période de conservation des journaux (p. 522)
- Utilisation de la journalisation des requêtes (p. 522)
- Publication de journaux PostgreSQL dans CloudWatch Logs (p. 523)

Définition de la période de conservation des journaux

Pour définir la période de conservation des journaux du système, utilisez le paramètre `rds.log_retention_period`. Le paramètre `rds.log_retention_period` se trouve dans le groupe de paramètres de base de données associé à votre instance de base de données. L'unité par défaut pour ce paramètre est la minute. Par exemple, la valeur 1 440 conserve les journaux pendant un jour. La valeur par défaut est 4 320 (trois jours). La valeur maximale est 10 080 (sept jours). La capacité de stockage allouée à votre instance doit être suffisante pour contenir les fichiers journaux conservés.

Pour conserver les journaux plus anciens, publiez-les dans Amazon CloudWatch Logs. Pour de plus amples informations, veuillez consulter Publication de journaux PostgreSQL dans CloudWatch Logs (p. 523).

Utilisation de la journalisation des requêtes

Pour activer la journalisation des requêtes pour votre instance de base de données PostgreSQL, définissez deux paramètres dans le groupe de paramètres de base de données associé à votre instance de base de données : `log_statement` et `log_min_duration_statement`.

Le paramètre `log_statement` contrôle les instructions SQL qui sont enregistrées. Nous vous recommandons de définir ce paramètre sur `all` afin de journaliser toutes les instructions lorsque vous résolvez des problèmes dans votre instance de base de données. La valeur par défaut est `none`. Pour journaliser toutes les instructions DDL (Data Definition Language) (CREATE, ALTER, DROP, etc.), définissez cette valeur sur `ddl`. Pour journaliser toutes les instructions DDL et DML (Data Manipulation Language) (INSERT, UPDATE, DELETE, etc.), définissez cette valeur sur `mod`.

Le paramètre `log_min_duration_statement` définit la limite en millisecondes pour l'enregistrement d'une instruction. Toutes les instructions SQL s'exécutant plus longtemps que la durée définie pour le paramètre sont enregistrées. Par défaut, ce paramètre est désactivé et défini sur -1. L'activation de ce paramètre vous permet d'identifier les requêtes non optimisées.

Pour configurer la journalisation des requêtes, procédez comme suit :

1. Définissez le paramètre `log_statement` sur `all`. L'exemple suivant illustre les informations écrites dans le fichier `postgres.log`.

   ```
   2013-11-05 16:48:56 UTC::@:[2952]:LOG:  received SIGHUP, reloading configuration files
   2013-11-05 16:48:56 UTC::@:[2952]:LOG:  parameter "log_statement" changed to "all"
   ```

   Des informations supplémentaires sont écrites dans le fichier postgres.log lorsque vous exécutez une requête. L'exemple suivant illustre le type d'informations écrites dans le fichier après une requête.

   ```
   2013-11-05 16:41:07 UTC::@:[2955]:LOG:  checkpoint starting: time
   2013-11-05 16:41:07 UTC::@:[2955]:LOG:  checkpoint complete: wrote 1 buffers (0.3%);
    0 transaction log file(s) added, 0 removed, 1 recycled; write=0.000 s, sync=0.003 s,
    total=0.012 s; sync files=1, longest=0.003 s, average=0.003 s
   2013-11-05 16:45:14 UTC:[local]:master@postgres:[8839]:LOG:  statement: SELECT d.datname
    as "Name",
           pg_catalog.pg_get_userbyid(d.datdba) as "Owner",
           pg_catalog.pg_encoding_to_char(d.encoding) as "Encoding",
           d.datcollate as "Collate",
           d.datctype as "Ctype",
           pg_catalog.array_to_string(d.datacl, E'\n') AS "Access privileges"
    FROM pg_catalog.pg_database d
    ORDER BY 1;
   2013-11-05 16:45:
   ```

2. Définissez le paramètre `log_min_duration_statement`. L'exemple suivant illustre les informations écrites dans le fichier `postgres.log` lorsque le paramètre est défini sur `1`.

```
2013-11-05 16:48:56 UTC::@:[2952]:LOG:  received SIGHUP, reloading configuration files
2013-11-05 16:48:56 UTC::@:[2952]:LOG:  parameter "log_min_duration_statement" changed to
 "1"
```

Des informations supplémentaires sont écrites dans le fichier `postgres.log` lorsque vous exécutez une requête dont la durée dépasse celle définie dans le paramètre de durée. L'exemple suivant illustre le type d'informations écrites dans le fichier après une requête.

```
2013-11-05 16:51:10 UTC:[local]:master@postgres:[9193]:LOG:  statement: SELECT
 c2.relname, i.indisprimary, i.indisunique, i.indisclustered, i.indisvalid,
 pg_catalog.pg_get_indexdef(i.indexrelid, 0, true),
   pg_catalog.pg_get_constraintdef(con.oid, true), contype, condeferrable, condeferred,
 c2.reltablespace
 FROM pg_catalog.pg_class c, pg_catalog.pg_class c2, pg_catalog.pg_index i
   LEFT JOIN pg_catalog.pg_constraint con ON (conrelid = i.indrelid AND conindid =
 i.indexrelid AND contype IN ('p','u','x'))
 WHERE c.oid = '1255' AND c.oid = i.indrelid AND i.indexrelid = c2.oid
 ORDER BY i.indisprimary DESC, i.indisunique DESC, c2.relname;
2013-11-05 16:51:10 UTC:[local]:master@postgres:[9193]:LOG:  duration: 3.367 ms
2013-11-05 16:51:10 UTC:[local]:master@postgres:[9193]:LOG:  statement: SELECT
 c.oid::pg_catalog.regclass FROM pg_catalog.pg_class c, pg_catalog.pg_inherits i WHERE
 c.oid=i.inhparent AND i.inhrelid = '1255' ORDER BY inhseqno;
2013-11-05 16:51:10 UTC:[local]:master@postgres:[9193]:LOG:  duration: 1.002 ms
2013-11-05 16:51:10 UTC:[local]:master@postgres:[9193]:LOG:  statement:
 SELECT c.oid::pg_catalog.regclass FROM pg_catalog.pg_class c,
 pg_catalog.pg_inherits i WHERE c.oid=i.inhrelid AND i.inhparent = '1255' ORDER BY
 c.oid::pg_catalog.regclass::pg_catalog.text;
2013-11-05 16:51:18 UTC:[local]:master@postgres:[9193]:LOG:  statement: select proname
 from pg_proc;
2013-11-05 16:51:18 UTC:[local]:master@postgres:[9193]:LOG:  duration: 3.469 ms
```

Publication de journaux PostgreSQL dans CloudWatch Logs

Pour stocker vos enregistrements de journal PostgreSQL dans une solution de stockage hautement durable, vous pouvez utiliser CloudWatch Logs. CloudWatch Logs vous permet également d'effectuer une analyse en temps réel des données de journaux et d'utiliser CloudWatch pour afficher les métriques et créer des alarmes.

Pour utiliser CloudWatch Logs, configurez votre instance de base de données RDS for PostgreSQL de sorte à publier les données de journaux dans un groupe de journaux.

> **Note**
>
> La publication de fichiers journaux dans CloudWatch Logs est uniquement prise en charge pour PostgreSQL version 9.6.6 et versions ultérieures, et pour PostgreSQL version 10.4 et versions ultérieures.

Vous pouvez publier les types de journaux suivants dans CloudWatch Logs pour RDS for PostgreSQL :

- Journal PostgreSQL
- Journal de mise à niveau (non disponible pour Aurora PostgreSQL)

Après avoir terminé la configuration, Amazon RDS publie les événements de journaux dans des flux de journaux au sein d'un groupe de journaux CloudWatch. Par exemple, les données de journaux PostgreSQL sont stockés dans le groupe de journaux `/aws/rds/instance/`*`my_instance`*`/postgresql`. Pour afficher vos journaux, ouvrez la console CloudWatch à l'adresse https://console.aws.amazon.com/cloudwatch/.

Console

Pour publier des journaux PostgreSQL dans CloudWatch Logs à l'aide de la console

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez l'instance de base de données que vous souhaitez modifier, puis choisissez Modifier.
4. Dans la section Exportations des journaux, choisissez les journaux que vous voulez commencer à publier dans CloudWatch Logs.

   La section Exportations des journaux est uniquement disponible pour les versions de PostgreSQL qui prennent en charge la publication dans CloudWatch Logs.
5. Choisissez Continuer, puis Modifier l'instance de base de données sur la page récapitulative.

AWS CLI

Vous pouvez publier des journaux PostgreSQL avec AWS CLI. Vous pouvez appeler la commande `modify-db-instance` avec les paramètres suivants :

- `--db-instance-identifier`
- `--cloudwatch-logs-export-configuration`

> **Note**
>
> Une modification apportée à l'option `--cloudwatch-logs-export-configuration` est toujours appliquée immédiatement à l'instance de base de données. Par conséquent, les options `--apply-immediately` et `--no-apply-immediately` sont sans effet.

Vous pouvez également publier des journaux PostgreSQL en appelant les commandes d'interface de ligne de commande suivantes :

- `create-db-instance`
- `restore-db-instance-from-db-snapshot`
- `restore-db-instance-to-point-in-time`

Exécutez l'une de ces commandes d'interface de ligne de commande avec les options suivantes :

- `--db-instance-identifier`
- `--enable-cloudwatch-logs-exports`
- `--db-instance-class`
- `--engine`

D'autres options peuvent être requises en fonction de la commande d'interface de ligne de commande que vous exécutez.

Example Modification d'une instance pour publier des journaux dans CloudWatch Logs

L'exemple suivant modifie une instance de base de données PostgreSQL existante pour publier les fichiers journaux sur CloudWatch Logs. La valeur `--cloudwatch-logs-export-configuration` n'est pas un objet JSON. La clé pour cet objet est `EnableLogTypes` et sa valeur est un tableau de chaînes avec une combinaison quelconque de `postgresql` et `upgrade`.

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --cloudwatch-logs-export-configuration '{"EnableLogTypes":["postgresql", "upgrade"]}'
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration '{"EnableLogTypes":["postgresql","upgrade"]}'
```

Example Création d'une instance pour publier des journaux dans CloudWatch Logs

L'exemple suivant crée une instance de base de données PostgreSQL et publie les fichiers journaux sur CloudWatch Logs. La valeur `--enable-cloudwatch-logs-exports` est un tableau de chaînes JSON. Les chaînes peuvent être une combinaison quelconque de `postgresql` et `upgrade`.

Pour Linux, macOS ou Unix :

```
aws rds create-db-instance \
    --db-instance-identifier mydbinstance \
    --enable-cloudwatch-logs-exports '["postgresql","upgrade"]' \
    --db-instance-class db.m4.large \
    --engine postgres
```

Pour Windows :

```
aws rds create-db-instance ^
    --db-instance-identifier mydbinstance ^
    --enable-cloudwatch-logs-exports '["postgresql","upgrade"]' ^
    --db-instance-class db.m4.large ^
    --engine postgres
```

API RDS

Vous pouvez publier des journaux PostgreSQL avec l'API RDS. Vous pouvez appeler l'action `ModifyDBInstance` avec les paramètres suivants :

- `DBInstanceIdentifier`
- `CloudwatchLogsExportConfiguration`

> **Note**
>
> Une modification apportée au paramètre `CloudwatchLogsExportConfiguration` est toujours appliquée immédiatement à l'instance de base de données. Par conséquent, le paramètre `ApplyImmediately` est sans effet.

Vous pouvez également publier des journaux PostgreSQL en appelant les opérations d'API RDS suivantes :

- `CreateDBInstance`
- `RestoreDBInstanceFromDBSnapshot`
- `RestoreDBInstanceToPointInTime`

Exécutez l'une de ces opérations d'API RDS avec les paramètres suivants :

- `DBInstanceIdentifier`
- `EnableCloudwatchLogsExports`
- `Engine`
- `DBInstanceClass`

D'autres paramètres peuvent être requis en fonction de l'opération que vous exécutez.

Utilisation de AWS CloudTrail et Amazon RDS

AWS CloudTrail est un service AWS qui vous aide à auditer votre compte AWS. CloudTrail est activé sur votre compte AWS lorsque vous le créez.

Pour obtenir des informations détaillées sur CloudTrail, consultez le AWS CloudTrail User Guide.

Intégration de CloudTrail à Amazon RDS

Toutes les actions Amazon RDS sont enregistrées par CloudTrail. CloudTrail fournit un enregistrement des actions réalisées par un utilisateur, un rôle ou un service AWS dans Amazon RDS.

Événements CloudTrail

CloudTrail capture les appels d'API pour Amazon RDS en tant qu'événements. Un événement représente une demande individuelle émise à partir d'une source quelconque et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. Les événements incluent des appels de la console Amazon RDS et le code des appels vers les API Amazon RDS.

L'activité Amazon RDS est enregistrée dans un événement CloudTrail dans l'Historique des événements. Vous pouvez utiliser la console CloudTrail pour afficher les 90 derniers jours d'activité de l'API et d'événements enregistrés dans une région AWS. Pour de plus amples informations, veuillez consulter Affichage des événements avec l'historique des événements CloudTrail.

Journaux de suivi CloudTrail

Pour un enregistrement continu des événements dans votre compte AWS, y compris les événements pour Amazon RDS, créez un journal de suivi. Un journal de suivi est une configuration qui permet de délivrer des événements à un compartiment Amazon S3 spécifié. CloudTrail délivre généralement des fichiers journaux dans les 15 minutes suivant l'activité du compte.

> **Note**
>
> Si vous ne configurez pas de journal de suivi, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Event history (Historique des événements).

Vous pouvez créer deux types de journaux de suivi pour un compte AWS : un journal de suivi qui s'applique à toutes les régions ou un journal de suivi qui s'applique à une région. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions.

En outre, vous pouvez configurer d'autres services AWS pour analyser plus en profondeur les données d'événement collectées dans les journaux CloudTrail et agir sur celles-ci. Pour plus d'informations, consultez :

- Présentation de la création d'un journal de suivi
- Intégrations et services pris en charge par CloudTrail

- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers journaux CloudTrail de plusieurs régions et Réception de fichiers journaux CloudTrail de plusieurs comptes

Entrées de fichier journal Amazon RDS

Les fichiers journaux CloudTrail contiennent une ou plusieurs entrées de journal. Les fichiers journaux CloudTrail ne sont pas une série ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de journal CloudTrail qui illustre l'action `CreateDBInstance`.

```
{
    "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": "5.6.39",
        "dbInstancePort": 0,
        "optionGroupMemberships": [
            {
                "status": "in-sync",
                "optionGroupName": "default:mysql-5-6"
            }
        ],
        "dBParameterGroups": [
            {
                "dBParameterGroupName": "default.mysql5.6",
```

```
            "parameterApplyStatus": "in-sync"
        }
    ],
    "monitoringInterval": 0,
    "dBInstanceClass": "db.m1.small",
    "readReplicaDBInstanceIdentifiers": [],
    "dBSubnetGroup": {
        "dBSubnetGroupName": "default",
        "dBSubnetGroupDescription": "default",
        "subnets": [
            {
                "subnetAvailabilityZone": {"name": "us-east-1b"},
                "subnetIdentifier": "subnet-cbfff283",
                "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"
}
```


Comme indiqué dans l'élément `userIdentity` de l'exemple précédent, chaque événement ou entrée de journal contient des informations sur la personne qui a généré la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou IAM.
- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré.
- Si la requête a été effectuée par un autre service AWS.

Pour de plus amples informations sur `userIdentity`, veuillez consulter la section Élément userIdentity CloudTrail. Pour plus d'informations sur `CreateDBInstance` et d'autres actions Amazon RDS, consultez Amazon RDS API Reference.

Utilisation de Amazon RDS sur AWS Outposts

Amazon RDS sur AWS Outposts étend Amazon RDS pour les bases de données MySQL et PostgreSQL aux environnements AWS Outposts. AWS Outposts utilise le même matériel que dans les régions AWS publiques pour mettre en place des services AWS, une infrastructure et des modèles d'exploitation sur site. Avec RDS sur outposts, vous pouvez allouer des instances de base de données gérées à proximité des applications métier qui doivent être exécutées sur site. Pour de plus amples informations sur AWS Outposts, veuillez consulter AWS Outposts.

Vous utilisez la même AWS Management Console, AWS CLI, et API RDS pour allouer et gérer des instances de base de données RDS sur outposts sur site comme vous le faites pour des instances de base de données RDS s'exécutant dans le cloud AWS. RDS sur outposts automatise les tâches telles que l'allocation de bases de données, l'application de correctifs pour des systèmes d'exploitation et des bases de données, la sauvegarde et l'archivage à long terme dans Amazon S3.

RDS sur outposts prend en charge les sauvegardes automatiques des instances de bases de données. La connectivité réseau entre votre Outpost et votre région AWS est requise pour sauvegarder et restaurer les instances de bases de données. Tous les instantanés de base de données et tous les journaux de transaction d'un Outpost sont stockés dans votre région AWS. À partir de votre région AWS, vous pouvez restaurer une instance de base de données à partir d'un instantané de base de données sur un autre Outpost. Pour de plus amples informations, veuillez consulter Utilisation des sauvegardes (p. 317).

RDS sur outposts prend en charge la maintenance et les mises à niveau automatiques des instances de bases de données. Pour plus d'informations, consultez Entretien d'une instance de base de données (p. 260).

RDS sur outposts utilise le chiffrement au repos pour les instances et les instantanés de base de données, via votre clé AWS Key Management Service (AWS KMS). Pour de plus amples informations sur le chiffrement au repos, veuillez consulter Chiffrement des ressources Amazon RDS (p. 1522).

Lorsque la connectivité réseau à la région AWS n'est pas disponible, votre instance de base de données continue de s'exécuter localement. Vous ne pouvez pas créer de nouvelles instances de base de données ou effectuer de nouvelles actions sur des instances de base de données existantes. Les sauvegardes automatiques n'ont pas lieu s'il n'y a pas de connectivité. En cas de défaillance d'une instance de base de données, celle-ci n'est pas automatiquement remplacée tant que la connectivité n'est pas restaurée. Nous vous recommandons de restaurer la connectivité réseau dès que possible.

Rubriques

- Prérequis pour Amazon RDS sur AWS Outposts (p. 530)
- Prise en charge de Amazon RDS sur AWS Outposts pour les fonctions Amazon RDS (p. 531)
- Classes d'instances de bases de données prises en charge pour Amazon RDS sur AWS Outposts. (p. 534)
- Création d'instances de bases de données pour Amazon RDS sur AWS Outposts (p. 535)

Prérequis pour Amazon RDS sur AWS Outposts

Les conditions suivantes sont requises pour utiliser Amazon RDS sur AWS Outposts :

- Installez AWS Outposts dans votre centre de données sur site. Pour de plus amples informations sur AWS Outposts, veuillez consulter AWS Outposts.
- Assurez-vous de disposer d'au moins un sous-réseau pour RDS sur outposts. Vous pouvez utiliser le même sous-réseau pour d'autres charges de travail.
- Assurez-vous de disposer d'une connexion réseau fiable entre votre Outpost et une région AWS.

Prise en charge de Amazon RDS sur AWS Outposts pour les fonctions Amazon RDS

Fonction	Pris en charge	Remarques	En savoir plus
Allocation d'instances de base de données	Oui	Vous ne pouvez créer que des instances de bases de données pour RDS pour MySQL et des instances de bases de données RDS pour PostgreSQL. Seuls MySQL 8.0.17 et PostgreSQL version 12.2 sont pris en charge. Actuellement, aucun autre moteur de base de données n'est pris en charge.	Création d'une instance de base de données Amazon RDS (p. 146)
Modification du mot de passe utilisateur principal	Oui	—	Modification d'une instance de base de données Amazon RDS (p. 243)
Affectation d'un nouveau nom à une instance DB	Oui	—	Modification d'une instance de base de données Amazon RDS (p. 243)
Redémarrage d'une instance DB	Oui	—	Redémarrage d'une instance de base de données (p. 272)
Arrêt d'une instance de base de données	Oui	—	Arrêt temporaire d'une instance de bases de données Amazon RDS (p. 239)
Démarrage d'une instance de base de données	Oui	—	Démarrage d'une instance de bases de données Amazon RDS précédemment arrêtée (p. 242)
Déploiements multi-AZ	Non	—	Haute disponibilité (multi-AZ) pour Amazon RDS (p. 43)
Groupes de paramètres DB	Oui	—	Utilisation de groupes de paramètres de base de données (p. 225)
Réplicas en lecture	Non	—	Utilisation des réplicas en lecture (p. 275)

Fonction	Pris en charge	Remarques	En savoir plus
Chiffrement au repos	Oui	RDS sur outposts ne prend pas en charge les instances de base de données non chiffrées.	Chiffrement des ressources Amazon RDS (p. 1522)
Authentification de base de données AWS Identity and Access Management (IAM)	Non	—	Authentification de base de données IAM pour MySQL et PostgreSQL (p. 1554)
Association d'un rôle IAM à une instance de base de données	Non	—	Commande d'interface de ligne de commandeadd-role-to-db-instance et opération d'API RDS AddRoleToDBInstance
Authentification Kerberos	Non	—	Authentification Kerberos (p. 1520)
Balisage de ressources Amazon RDS	Oui	—	Balisage de ressources Amazon RDS (p. 293)
Groupes d'options	Non	—	Utilisation de groupes d'options (p. 209)
Modification de la fenêtre de maintenance	Oui	—	Entretien d'une instance de base de données (p. 260)
Mise à niveau automatique de version mineure	Oui	—	Mise à niveau automatique de la version mineure du moteur (p. 269)
Modification de la fenêtre de sauvegarde	Oui	—	Utilisation des sauvegardes (p. 317) and Modification d'une instance de base de données Amazon RDS (p. 243)
Mise à l'échelle d'instance de base de données	Oui	Pour mettre à l'échelle une instance de base de données, modifiez sa classe d'instance de base de données sur site. La mise à l'échelle du stockage n'est pas prise en charge.	Modification d'une instance de base de données Amazon RDS (p. 243)
Instantanés d'instance de base de données manuels et automatiques	Oui	Les instantanés d'instance de base de données manuels et automatiques sont stockés dans votre région AWS.	Création d'un instantané de base de données (p. 327)

Fonction	Pris en charge	Remarques	En savoir plus
Restauration à partir d'un instantané de base de données	Oui	—	Restauration à partir d'un instantané de base de données (p. 329)
Restauration d'une instance de base de données à partir d'Amazon S3	Non	—	Restauration d'une sauvegarde dans une instance de base de données MySQL Amazon RDS (p. 821)
Exportation de données d'instantané vers Amazon S3	Oui	—	Exportation de données d'instantanés de bases de données vers Amazon S3 (p. 349)
Restauration à un instant dans le passé	Oui	—	Restauration d'une instance de base de données à une date spécifiée (p. 365)
Surveillance améliorée	Non	—	Surveillance améliorée (p. 394)
Surveillance d'Amazon CloudWatch	Non	—	Surveillance avec Amazon CloudWatch (p. 376)
Publication des journaux du moteur de base de données dans CloudWatch Logs	Non	—	Publication des journaux de base de données dans Amazon CloudWatch Logs (p. 493)
Notification d'événement	Oui	—	Utilisation de la notification d'événement Amazon RDS (p. 467)
Amazon RDS Performance Insights	Non	—	Utilisation d'Amazon RDS Performance Insights (p. 410)

Fonction	Pris en charge	Remarques	En savoir plus
Affichage ou téléchargement des journaux de base de données	Non	RDS sur outposts ne prend pas en charge l'affichage des journaux de base de données à l'aide de la console ou la description des journaux de base de données à l'aide de l'interface de ligne de commande ou de l'API RDS. RDS sur outposts ne prend pas en charge le téléchargement des journaux de base de données à l'aide de la console ou le téléchargement des journaux de base de données à l'aide de l'interface de ligne de commande ou de l'API RDS.	Amazon RDS Fichiers journaux de base de données (p. 490)
Amazon RDS Proxy	Non	—	Gestion des connexions avec Amazon RDS Proxy (p. 169)
Procédures stockées pour Amazon RDS pour MySQL	Oui	—	Référence SQL de MySQL sur Amazon RDS (p. 899)
Réplication avec des bases de données externes pour Amazon RDS pour MySQL	Non	—	Réplication avec une instance MySQL ou MariaDB s'exécutant à l'extérieur d'Amazon RDS (p. 863)

Note

RDS sur outposts ne prend pas en charge les cas d'utilisation exigeant que toutes les données restent dans votre centre de données.
RDS sur outposts stocke les sauvegardes et les journaux de base de données dans votre région AWS.

Classes d'instances de bases de données prises en charge pour Amazon RDS sur AWS Outposts.

Amazon RDS sur AWS Outposts prend en charge les classes d'instances de bases de données suivantes :

- Classes d'instances de bases de données à usage général
  - db.m5.24xlarge
  - db.m5.12xlarge
  - db.m5.4xlarge
  - db.m5.2xlarge

  - db.m5.xlarge
  - db.m5.large
- Classes d'instances de bases de données à mémoire optimisée
  - db.r5.24xlarge
  - db.r5.12xlarge
  - db.r5.4xlarge
  - db.r5.2xlarge
  - db.r5.xlarge
  - db.r5.large

Seul le stockage SSD à usage général est pris en charge pour les instances de bases de données RDS sur outposts. Pour plus d'informations sur les classes d'instance DB, consultez Classes d'instances de base de données (p. 6).

Création d'instances de bases de données pour Amazon RDS sur AWS Outposts

La création d'une instance de base de données Amazon RDS sur AWS Outposts ressemble à la création d'une instance de base de données Amazon RDS dans le Cloud AWS. Toutefois, vous devez indiquer un groupe de sous-réseaux de base de données associé à votre Outpost.

Un Amazon VPC peut couvrir toutes les zones de disponibilité d'une région AWS. Vous pouvez étendre n'importe quel VPC de la région AWS à votre Outpost en ajoutant un sous-réseau Outpost. Pour ajouter un sous-réseau Outpost à un VPC, spécifiez l'ARN (Amazon Resource Name) de l'Outpost lorsque vous créez le sous-réseau.

Avant de créer une instance de base de données RDS sur outposts, vous pouvez créer un groupe de sous-réseaux de base de données incluant un sous-réseau associé à votre Outpost. Lorsque vous créez une instance de base de données RDS sur outposts, indiquez ce groupe de sous-réseaux de base de données. Vous pouvez également choisir de créer un nouveau groupe de sous-réseaux de base de données lorsque vous créez votre instance de base de données.

Pour de plus amples informations sur la configuration d'AWS Outposts, veuillez consulter AWS Outposts User Guide.

Console

Pour créer une instance de base de données RDS sur outposts à l'aide de la console

1. Créez un groupe de sous-réseaux de base de données avec un sous-réseau associé à votre Outpost.

   Pour créer un nouveau groupe de sous-réseaux de base de données pour l'Outpost lorsque vous créez votre instance de base de données, ignorez cette étape.

   > **Note**
   >
   > Pour créer un groupe de sous-réseaux de base de données pour le Cloud AWS, vous devez indiquer au moins deux sous-réseaux. Toutefois, pour un groupe de sous-réseaux de base de données Outpost, vous pouvez n'indiquer qu'un seul sous-réseau.

   a. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.

b. Dans le coin supérieur droit de la console Amazon RDS, choisissez la région AWS dans laquelle vous voulez créer le groupe de sous-réseaux de base de données.

c. Sélectionnez Groupes de sous-réseaux, puis Créer un groupe de sous-réseaux DB.

La page Créer un groupe de sous-réseaux DB s'affiche.

d. Définissez les valeurs suivantes pour votre nouveau groupe de sous-réseaux DB :

- Nom : indiquez le nom du groupe de sous-réseaux de base de données.
- Description : saisissez une description pour le groupe de sous-réseaux de base de données.
- VPC : choisissez le VPC pour lequel vous créez le groupe de sous-réseaux de base de données.

e. Pour Zones de disponibilité, choisissez la zone de disponibilité pour votre Outpost.

f. Pour Sous-réseaux, choisissez le sous-réseau pour une utilisation par RDS sur outposts.

Votre groupe de sous-réseaux de base de données ne doit contenir qu'un sous-réseau.

g. Sélectionnez Créer pour créer le groupe de sous-réseaux de base de données.

2. Créez l'instance de base de données et choisissez l'Outpost pour votre instance de base de données.

a. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.

b. Dans le coin supérieur droit de la console Amazon RDS, choisissez la région AWS dans laquelle vous voulez créer l'instance de base de données.

c. Dans la panneau de navigation, choisissez Databases (Bases de données).

d. Choisissez Create database (Créer une base de données).

AWS Management Console détecte les Outposts disponibles que vous avez configurés et présente l'option Sur site dans la section Emplacement de la base de données.

> **Note**
>
> Si vous n'avez pas configuré d'Outpost, la section Emplacement de la base de données n'apparaît pas ou l'option RDS sur outposts n'est pas disponible dans la section Choisir une méthode de création sur site.

e. Sélectionnez les paramètres suivants :

- Database location (Emplacement de la base de données) : On-premises (Sur site)
- Méthode de création sur site : RDS sur outposts
- Outpost : Outpost utilisant le VPC contenant le groupe de sous-réseaux de base de données pour votre instance de base de données. Votre VPC doit être basé sur le service Amazon VPC.
- Virtual Private Cloud (VPC) : VPC contenant le groupe de sous-réseaux de base de données pour votre instance de base de données.
- Groupe de sécurité VPC : Groupe de sécurité Amazon VPC pour votre instance de base de données.
- Groupe de sous-réseaux : Groupe de sous-réseaux de base de données pour votre instance de base de données.

  Vous pouvez sélectionner un groupe de sous-réseaux de base de données existant associé à l'Outpost. Si vous n'avez pas créé de groupe de sous-réseaux de base de données, vous pouvez en créer un pour l'Outpost. Seul un sous-réseau est autorisé dans ce groupe de sous-réseaux de base de données.

f. Pour les sections restantes, spécifiez vos paramètres d’instance de base de données.

Pour de plus amples informations sur chaque paramètre lors de la création d'une instance de base de données, veuillez consulter Paramètres des instances de base de données (p. 151).

g. Choisissez Create database (Créer une base de données).

Si vous choisissez de générer un mot de passe automatiquement, le bouton View credential details (Afficher les informations d'identification) apparaît sur la page Databases (Bases de données).

Pour afficher l'identifiant principal et le mot de passe pour l'instance de base de données, choisissez View credential details (Afficher les informations d'identification).

Pour vous connecter à l'instance de base de données en tant qu'utilisateur principal, utilisez l'identifiant et le mot de passe affichés.

> **Important**
>
> Vous ne pourrez pas afficher le mot de passe de l'utilisateur principal de nouveau. Si vous ne l'enregistrez pas, il sera peut-être nécessaire de le modifier. Pour changer le mot de passe de l'utilisateur principal une fois l'instance de base de données disponible, modifiez l'instance de base de données. Pour de plus amples informations sur la modification d'une instance de base de données, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

h. Pour Databases (Bases de données), choisissez le nom de la nouvelle instance de base de données.

Sur la console RDS, les détails de la nouvelle instance de base de données s'affichent. L'instance de base de données a le statut Creating (Création en cours) jusqu'à ce qu'elle soit créée et prête à l'emploi. Lorsque le statut devient Available (Disponible), vous pouvez vous connecter à l'instance de base de données. En fonction du stockage et de la classe d'instance de base de données alloués, la mise à disposition de la nouvelle instance de base de données peut nécessiter plusieurs minutes.

Une fois l'instance de base de données disponible, vous pouvez la gérer comme vous gérez les instances de bases de données RDS dans le Cloud.

AWS CLI

Pour créer une nouvelle instance de base de données dans un Outpost avec l'AWS CLI, créez d'abord un groupe de sous-réseaux de base de données pour une utilisation par RDS sur outposts en appelant la commande create-db-subnet-group. Pour `--subnet-ids`, spécifiez le groupe de sous-réseaux dans l'Outpost pour une utilisation par RDS sur outposts.

Pour Linux, macOS ou Unix :

```
aws rds create-db-subnet-group \
    --db-subnet-group-name myoutpostdbsubnetgr \
    --db-subnet-group-description "DB subnet group for RDS sur outposts" \
    --subnet-ids subnet-abc123
```

Pour Windows :

```
aws rds create-db-subnet-group ^
    --db-subnet-group-name myoutpostdbsubnetgr ^
    --db-subnet-group-description "DB subnet group for RDS sur outposts" ^
    --subnet-ids subnet-abc123
```

Ensuite, appelez la commande create-db-instance avec les paramètres ci-dessous. Spécifiez une zone de disponibilité pour l'Outpost, un groupe de sécurité Amazon VPC associé à l'Outpost et le groupe de sous-réseaux de base de données que vous avez créé pour l'Outpost. Vous pouvez inclure les options suivantes :

- `--db-instance-identifier`
- `--db-instance-class`
- `--engine`
- `--availability-zone`
- `--db-security-groups`
- `--db-subnet-group-name`
- `--allocated-storage`
- `--master-user-name`
- `--master-user-password`
- `--backup-retention-period`
- `-storage-encrypted`
- `--kms-key-id`

Example

L'exemple suivant créé une instance de base de données MySQL nommée `myoutpostdbinstance`.

Pour Linux, macOS ou Unix :

```
aws rds create-db-instance \
    --db-instance-identifier myoutpostdbinstance \
    --db-instance-class db.m5.large \
    --engine mysql \
    --availability-zone us-east-1d \
    --db-security-groups outpost-sg \
    --db-subnet-group-name myoutpostdbsubnetgr \
    --allocated-storage 100 \
    --master-username masterawsuser \
    --master-user-password masteruserpassword \
    --backup-retention-period 3 \
    --storage-encrypted \
    --kms-key-id mykey
```

Pour Windows :

```
aws rds create-db-instance ^
    --db-instance-identifier myoutpostdbinstance ^
    --db-instance-class db.m5.large ^
    --engine mysql ^
    --availability-zone us-east-1d ^
    --db-security-groups outpost-sg ^
    --db-subnet-group-name myoutpostdbsubnetgr ^
    --allocated-storage 100 ^
    --master-username masterawsuser ^
    --master-user-password masteruserpassword ^
    --backup-retention-period 3 ^
    --storage-encrypted ^
    --kms-key-id mykey
```

Pour créer une instance de base de données PostgreSQL, spécifiez `postgres` pour l'option `--engine`.

Pour de plus amples informations sur chaque paramètre lors de la création d'une instance de base de données, veuillez consulter Paramètres des instances de base de données (p. 151).

API RDS

Pour créer une nouvelle instance de base de données dans un Outpost avec l'API RDS, créez d'abord un groupe de sous-réseaux de base de données pour une utilisation par RDS sur outposts en appelant l'opération CreateDBSubnetGroup. Pour `SubnetIds`, spécifiez le groupe de sous-réseaux dans l'Outpost pour une utilisation par RDS sur outposts.

Ensuite, appelez l'opération CreateDBInstance avec les paramètres ci-dessous. Spécifiez une zone de disponibilité pour l'Outpost, un groupe de sécurité Amazon VPC associé à l'Outpost et le groupe de sous-réseaux de base de données que vous avez créé pour l'Outpost.

- `AllocatedStorage`
- `AvailabilityZone`
- `BackupRetentionPeriod`
- `DBInstanceClass`
- `DBInstanceIdentifier`
- `DBSecurityGroups`
- `DBSubnetGroupName`
- `Engine`
- `MasterUsername`

- `MasterUserPassword`
- `StorageEncrypted`
- `KmsKeyID`

Pour de plus amples informations sur chaque paramètre lors de la création d'une instance de base de données, veuillez consulter Paramètres des instances de base de données (p. 151).

MariaDB sur Amazon RDS

Amazon RDS prend en charge les instances de base de données qui exécutent plusieurs versions de MariaDB. Vous pouvez utiliser les versions majeures suivantes :

- MariaDB 10.4
- MariaDB 10.3
- MariaDB 10.2
- MariaDB 10.1
- MariaDB 10.0

Pour plus d'informations sur la prise en charge des versions mineures, consultez Versions de MariaDB sur Amazon RDS (p. 544).

Vous utilisez d'abord les interfaces ou les outils de gestion Amazon RDS pour créer une instance de base de données Amazon RDS MariaDB. Vous pouvez ensuite utiliser les outils Amazon RDS pour effectuer des actions de gestion de l'instance de base de données, comme reconfigurer ou redimensionner l'instance de base de données, autoriser les connexions à l'instance de base de données, créer et restaurer à partir de sauvegardes ou d'instantanés, créer des secondaires multi-AZ, créer des réplicas en lecture et surveiller les performances de l'instance de base de données. Vous utilisez les applications et les utilitaires MariaDB pour stocker les données de l'instance de base de données et y accéder.

MariaDB est disponible dans toutes les régions AWS. Pour plus d'informations sur les régions AWS, consultez Régions, zones de disponibilité et zones locales (p. 39).

Vous pouvez utiliser Amazon RDS pour les bases de données MariaDB afin de développer des applications conformes à la loi HIPAA. Vous pouvez stocker les informations relatives à la santé, y compris les données de santé protégées (PHI, Protected Health Information), selon les termes d'un accord de partenariat (BAA, Business Associate Agreement) avec AWS. Pour de plus amples informations, veuillez consulter Conformité à la loi HIPAA. Les services AWS concernés par le programme de conformité ont été intégralement évalués par un auditeur tiers et donnent lieu à une certification, une attestation de conformité ou une autorisation d'opérer (ATO, Authorization to operate). Pour de plus amples informations, veuillez consulter Services AWS concernés par le programme de conformité.

Avant de créer votre première instance de base de données, vous devez suivre la procédure décrite dans la section du présent guide relative à la configuration. Pour plus d'informations, consultez Configuration pour Amazon RDS (p. 62).

Tâches courantes de gestion pour MariaDB sur Amazon RDS

Vous trouverez ci-dessous les tâches courantes de gestion que vous exécutez avec une instance de base de données Amazon RDS exécutant MariaDB, avec des liens vers la documentation appropriée relative à chaque tâche.

Type de tâche	Documentation
Classes d'instance, stockage et PIOPS Si vous créez une instance de base de données à des fins de production, vous devez comprendre comment les classes d'instance,	Classes d'instances de base de données (p. 6)

Type de tâche	Documentation
les types de stockage et les IOPS provisionnées fonctionnent dans Amazon RDS.	Types de stockage Amazon RDS (p. 30)
Déploiements multi-AZ Assurez un haut niveau de disponibilité grâce à une réplication de secours synchrone dans une autre zone de disponibilité, au basculement automatique, à la tolérance aux pannes pour les instances de base de données à l'aide de déploiements multi-AZ et aux réplicas en lecture.	Haute disponibilité (multi-AZ) pour Amazon RDS (p. 43)
Amazon Virtual Private Cloud (VPC) Si votre compte AWS possède un VPC par défaut, votre instance de base de données est automatiquement créée dans le VPC par défaut. Si votre compte n'a pas de VPC par défaut et que vous voulez que l'instance de base de données soit dans un VPC, vous devez créer le VPC et les groupes de sous-réseaux avant de créer l'instance de base de données.	Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611) Utilisation d'une instance de base de données dans un VPC (p. 1620)
Groupes de sécurité Par défaut, les instances de bases de données sont créées avec un pare-feu qui empêche d'y accéder. Vous devez donc créer un groupe de sécurité avec les adresses IP correctes et la configuration réseau permettant d'accéder à l'instance de base de données. Le groupe de sécurité que vous créez dépend de la plateforme Amazon EC2 sur laquelle se trouve votre instance de base de données et du fait que vous accédiez ou non à votre instance de base de données depuis une instance Amazon EC2. En général, si votre instance de base de données est sur la plateforme EC2-Classic, vous devez créer un groupe de sécurité de base de données ; si votre instance de base de données est sur la plateforme EC2-VPC, vous devez créer un groupe de sécurité VPC.	Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611) Contrôle d'accès par groupe de sécurité (p. 1590)
Groupes de paramètres Si votre instance de base de données doit nécessiter des paramètres de base de données spécifiques, vous devez créer un groupe de paramètres avant de créer l'instance de base de données.	Utilisation de groupes de paramètres de base de données (p. 225)
Importation et exportation de données Etablir les procédures d'importation ou d'exportation de données.	Importation de données dans une instance de base de données MariaDB (p. 580)
Réplication Vous pouvez décharger le trafic en lecture de votre instance de base de données MariaDB source en créant des réplicas en lecture.	Utilisation des réplicas en lecture (p. 275)
Connexion à votre instance de base de données Connectez-vous à votre instance de base de données à l'aide d'une application client SQL standard.	Connexion à une instance de base de données exécutant le moteur de base de données MariaDB (p. 556)

Type de tâche	Documentation
Sauvegarde et restauration Lorsque vous créez votre instance de base de données, vous pouvez la configurer pour effectuer des sauvegardes automatiques. Vous pouvez également sauvegarder et restaurer vos bases de données manuellement à l'aide des fichiers de sauvegarde complète (fichiers .bak).	Utilisation des sauvegardes (p. 317)
Surveillance Surveillez votre instance de base de données RDS MariaDB à l'aide de métriques RDS Amazon CloudWatch, d'événements et de Surveillance améliorée. Afficher des fichiers journaux pour votre instance de base de données RDS MariaDB.	Affichage des métriques d'instances de base de données (p. 384) Affichage d'événements Amazon RDS (p. 486)
Fichiers journaux Vous pouvez accéder aux fichiers journaux de votre instance de base de données MariaDB.	Amazon RDS Fichiers journaux de base de données (p. 490) Fichiers journaux de base de données MariaDB (p. 494)

Il existe également des tâches d'administration avancées permettant d'utiliser les instances de base de données exécutant MariaDB. Pour plus d'informations, consultez la documentation suivante :

- Paramètres pour MariaDB (p. 584)
- Référence MariaDB sur SQL Amazon RDS (p. 589)

Versions de MariaDB sur Amazon RDS

Les numéros de versions de MariaDB sont organisés selon la version X.Y.Z. Dans la terminologie Amazon RDS, X.Y représente la version majeure et Z le numéro de la version mineure. Pour les implémentations Amazon RDS, un changement de version sera considéré majeur si le numéro de version majeure change. Par exemple, en allant de la version 10.0 à 10.1. Un changement de version sera considéré mineur seulement si le numéro de version mineure change. Par exemple, en allant de la version 10.0.17 à 10.0.24.

Amazon RDS prend actuellement en charge les versions de MariaDB suivantes :

Version majeure	Version mineure
MariaDB 10.4	• 10.4.13 (prise en charge dans toutes les régions AWS) • 10.4.8 (prise en charge dans toutes les régions AWS)
MariaDB 10.3	• 10.3.23 (prise en charge dans toutes les régions AWS) • 10.3.20 (prise en charge dans toutes les régions AWS) • 10.3.13 (prise en charge dans toutes les régions AWS) • 10.3.8 (prise en charge dans toutes les régions AWS)
MariaDB 10.2	• 10.2.21 (prise en charge dans toutes les régions AWS) • 10.2.15 (prise en charge dans toutes les régions AWS) • 10.2.12 (prise en charge dans toutes les régions AWS) • 10.2.11 (prise en charge dans toutes les régions AWS)

Version majeure	Version mineure
MariaDB 10.1	• 10.1.34 (prise en charge dans toutes les régions AWS) • 10.1.31 (prise en charge dans toutes les régions AWS) • 10.1.26 (prise en charge dans toutes les régions AWS) • 10.1.23 (prise en charge dans toutes les régions AWS) • 10.1.19 (prise en charge dans toutes les régions AWS) • 10.1.14 (prise en charge dans toutes les régions AWS, sauf USA Est (Ohio))
MariaDB 10.0	• 10.0.35 (prise en charge dans toutes les régions AWS) • 10.0.34 (prise en charge dans toutes les régions AWS) • 10.0.32 (prise en charge dans toutes les régions AWS) • 10.0.31 (prise en charge dans toutes les régions AWS) • 10.0.28 (prise en charge dans toutes les régions AWS) • 10.0.24 (prise en charge dans toutes les régions AWS) • 10.0.17 (prise en charge dans toutes les régions AWS sauf USA Est (Ohio), Canada (Centre) et Europe (Londres))

Vous pouvez spécifier n'importe quelle version MariaDB actuellement prise en charge lorsque vous créez une instance de base de données. Vous pouvez spécifier la version majeure (par exemple MariaDB 10.2), puis toute version mineure prise en charge pour la version majeure spécifiée. Si aucune version n'est spécifiée, Amazon RDS utilise par défaut une version prise en charge, généralement la plus récente. Si une version majeure est spécifiée, mais qu'une version mineure ne l'est pas, Amazon RDS utilise par défaut une version récente de la version majeure que vous avez spécifiée. Pour afficher la liste des versions prises en charge, ainsi que celles par défaut pour des instances de base de données nouvellement créées, utilisez la commande `describe-db-engine-versions` de l'AWS CLI.

La version par défaut de MariaDB peut varier selon la région AWS. Pour créer une instance de base de données avec une version mineure spécifique, spécifiez la version mineure lors de la création de l'instance de base de données. Vous pouvez déterminer la version secondaire par défaut d'une région AWS à l'aide de la commande AWS CLI suivante :

```
aws rds describe-db-engine-versions --default-only --engine mariadb --engine-version major-
engine-version --region region --query "*[].{Engine:Engine,EngineVersion:EngineVersion}" --
output text
```

Remplacez *`major-engine-version`* par la version majeure du moteur et *`region`* par la région AWS. Par exemple, la commande AWS CLI suivante renvoie la version du moteur mineur MariaDB par défaut pour la version majeure 10.3 et la région AWS USA Ouest (Oregon) (us-west-2) :

```
aws rds describe-db-engine-versions --default-only --engine mariadb --engine-version 10.3
 --region us-west-2 --query '*[].{Engine:Engine,EngineVersion:EngineVersion}' --output text
```

Pour de plus amples informations sur la stratégie d'obsolescence Amazon RDS pour MariaDB, veuillez consulter FAQ Amazon RDS.

Prise en charge des fonctions MariaDB sur Amazon RDS

Les sections suivantes décrivent les fonctions MariaDB prises en charge sur Amazon RDS pour les versions majeures de MariaDB :

Rubriques

- Prise en charge de MariaDB 10.4 sur Amazon RDS (p. 546)
- Prise en charge de MariaDB 10.3 sur Amazon RDS (p. 546)
- Prise en charge de MariaDB 10.2 sur Amazon RDS (p. 547)
- Prise en charge de MariaDB 10.1 sur Amazon RDS (p. 547)
- Prise en charge de MariaDB 10.0 sur Amazon RDS (p. 547)

Pour de plus amples informations sur les versions mineures de Amazon RDS for MariaDB prises en charge, veuillez consulter Versions de MariaDB sur Amazon RDS (p. 544).

Prise en charge de MariaDB 10.4 sur Amazon RDS

Amazon RDS prend en charge les nouvelles fonctions suivantes pour vos instances de base de données exécutant MariaDB version 10.4 ou versions ultérieures :

- Améliorations de la sécurité des comptes utilisateur – Améliorations de l'expiration des mots de passe et du verrouillage des comptes
- Améliorations de l'optimiseur – Fonction Optimizer Trace
- Améliorations InnoDB – Prise en charge de l'opération DROP COLUMN instantanée et extension `VARCHAR` instantanée pour `ROW_FORMAT=DYNAMIC` et `ROW_FORMAT=COMPACT`
- Nouveaux paramètres – Notamment : tcp_nodedelay, tls_version et gtid_cleanup_batch_size

Pour obtenir la liste de toutes les fonctions MariaDB 10.4 et leur documentation, veuillez consulter Changes and Improvements in MariaDB 10.4 (Modifications et améliorations dans MariaDB 10.4) et Release Notes - MariaDB 10.4 Series (Notes de mise à jour - MariaDB 10.4 Series) sur le site web de MariaDB.

Pour obtenir la liste des fonctions non prises en charge, consultez Fonctions non prises en charge (p. 548).

Prise en charge de MariaDB 10.3 sur Amazon RDS

Amazon RDS prend en charge les nouvelles fonctions suivantes pour vos instances de base de données exécutant MariaDB version 10.3 ou ultérieure :

- Compatibilité avec Oracle – analyseur de compatibilité PL/SQL, séquences, INTERSECT et EXCEPT pour compléter UNION, nouvelles déclarations TYPE OF et ROW TYPE OF et colonnes invisibles.
- Traitement de données temporelles – tables gérées par version du système, pour interroger les états passés et présents de la base de données.
- Flexibilité – regroupements définis par l'utilisateur, compression de colonnes indépendante du stockage, et prise en charge du protocole proxy pour relayer l'adresse IP du client au serveur.
- Facilité de gestion – opérations ADD COLUMN instantanées et opérations DDL (Data Definition Language) à échec rapide.

Pour obtenir la liste de toutes les fonctionnalités de MariaDB 10.3 et leur documentation, consultez Changes & Improvements in MariaDB 10.3 (Modifications et améliorations dans MariaDB 10.3) et Release Notes - MariaDB 10.0 Series (Notes de mise à jour - MariaDB 10.0 Series) sur le site web de MariaDB.

Pour obtenir la liste des fonctions non prises en charge, consultez Fonctions non prises en charge (p. 548).

Prise en charge de MariaDB 10.2 sur Amazon RDS

Amazon RDS prend en charge les nouvelles fonctions suivantes pour vos instances de base de données exécutant MariaDB version 10.2 ou ultérieure :

- ALTER USER
- Expressions de table communes
- Compression des événements pour réduire la taille du journal binaire
- CREATE USER — Nouvelles options pour limiter l'utilisation des ressources et TLS/SSL
- EXECUTE IMMEDIATE
- Flashback
- InnoDB — Nouveau moteur de stockage par défaut à la place de XtraDB
- InnoDB — Définissez dynamiquement la taille du pool de mémoires tampons
- Fonctions JSON
- Fonctions de fenêtrage
- WITH

Pour obtenir la liste de toutes les fonctionnalités de MariaDB 10.2 et leur documentation, consultez Changes & Improvements in MariaDB 10.2 (Modifications et améliorations dans MariaDB 10.2) et Release Notes - MariaDB 10.0 Series (Notes de mise à jour - MariaDB 10.0 Series) sur le site web de MariaDB.

Pour obtenir la liste des fonctions non prises en charge, consultez Fonctions non prises en charge (p. 548).

Prise en charge de MariaDB 10.1 sur Amazon RDS

Amazon RDS prend en charge les nouvelles fonctions suivantes pour vos instances de base de données exécutant MariaDB version 10.1 ou ultérieure :

- Réplication parallèle dans l'ordre optimiste
- Compression de page
- Nettoyage des données XtraDB et défragmentation

Pour obtenir la liste de toutes les fonctionnalités de MariaDB 10.1 et leur documentation, consultez Changes & Improvements in MariaDB 10.1 (Modifications et améliorations dans MariaDB 10.1) et Release Notes - MariaDB 10.0 Series (Notes de mise à jour - MariaDB 10.0 Series) sur le site web de MariaDB.

Pour obtenir la liste des fonctions non prises en charge, consultez Fonctions non prises en charge (p. 548).

Prise en charge de MariaDB 10.0 sur Amazon RDS

Pour obtenir la liste de toutes les fonctionnalités de MariaDB 10.0 et leur documentation, consultez Changes & Improvements in MariaDB 10.0 (Modifications et améliorations dans MariaDB 10.0) et Release Notes - MariaDB 10.0 Series (Notes de mise à jour - MariaDB 10.0 Series) sur le site web de MariaDB.

Pour obtenir la liste des fonctions non prises en charge, consultez Fonctions non prises en charge (p. 548).

Fonctions non prises en charge

Les fonctionnalités de MariaDB suivantes ne sont pas prises en charge sur Amazon RDS :

- Plug-in d'authentification – GSSAPI
- Plug-in d'authentification – Socket Unix
- Plug-in de chiffrement AWS Key Management
- Réplication retardée
- Chiffrement au repos MariaDB natif pour XtraDB, InnoDB et Aria.

  Vous pouvez activer le chiffrement au repos pour une instance de base de données MariaDB en suivant les instructions de Chiffrement des ressources Amazon RDS (p. 1522).
- HandlerSocket
- Type de table JSON
- MariaDB ColumnStore
- MariaDB Galera Cluster
- Réplication multi-source
- Moteur de stockage MyRocks
- Plug-in de validation de mot de passe, `simple_password_check` et `cracklib_password_check`
- Filtres de réplication
- Moteur de stockage Spider
- Moteur de stockage Sphinx
- Moteur de stockage TokuDB
- Attributs d'objets spécifiques au moteur de stockage, comme décrit dans Engine-defined New Table/Field/Index Attributes dans la documentation MariaDB.
- Chiffrement de table et d'espace de tables

Afin de livrer une expérience de service géré, Amazon RDS ne fournit pas d'accès de coquille aux instances de base de données et il restreint l'accès à certaines procédures de systèmes et à des tableaux qui nécessitent des privilèges avancés. Amazon RDS prend en charge l'accès aux bases de données sur une instance de base de données qui utilise toute application de client SQL standard. Amazon RDS ne permet pas d'accès d'hôte direct à une instance de base de données via Telnet, Secure Shell (SSH) ou Windows Remote Desktop Connection.

Moteurs de stockage pris en charge pour MariaDB sur Amazon RDS

Même si MariaDB prend en charge plusieurs moteurs de stockage aux capacités diverses, ils ne sont pas tous optimisés pour la récupération et la durabilité des données. InnoDB (pour les versions 10.2 et ultérieures) et XtraDB (pour les versions 10.0 et 10.1) sont les moteurs de stockage recommandés et pris en charge pour les instances de base de données MariaDB sur Amazon RDS. Les fonctions Amazon RDS comme la restauration à un instant dans le passé et l'instantané nécessitent un moteur de stockage récupérable et ne sont pris en charge que pour le moteur de stockage recommandé pour la version

MariaDB. Amazon RDS prend également en charge Aria, même si l'usage de cette dernière peut avoir un impact négatif sur la récupération en cas d'échec d'instance. Cependant, si vous avez besoin d'utiliser des index spatiaux pour gérer les données géographiques sur MariaDB 10.1 ou 10.0, vous devez utiliser Aria, parce que les index spatiaux ne sont pas pris en charge par XtraDB. Sur MariaDB 10.2 et versions suivantes, le moteur de stockage InnoDB prend en charge les index spatiaux.

Les autres moteurs de stockage ne sont pas pris en charge actuellement par Amazon RDS pour MariaDB.

Limites de taille des fichiers MariaDB dans Amazon RDS

Pour les instances de base de données Amazon RDS MariaDB, la limite maximale de stockage alloué restreint la taille d'une table à un maximum de 16 To lors de l'utilisation des espaces de table file-per-table InnoDB. Cette limite restreint également l'espace de table du système à une taille maximum de 16 To. Les espaces de table file-per-table InnoDB (avec des tables chacune dans leur propre espace de table) sont définis par défaut pour les instances de base de données Amazon RDS MariaDB. Pour plus d'informations, consultez Stockage d'instance de base de données Amazon RDS (p. 30).

Selon votre application, l'utilisation des espaces de table file-per-table InnoDB présente des avantages et des inconvénients. Pour déterminer l'approche optimale pour votre application, veuillez consulter File-Per-Table Tablespaces dans la documentation MySQL.

Il est déconseillé d'autoriser les tables à dépasser la taille maximale de fichier. En général, une meilleure pratique consiste à partitionner les données en tables plus petites, ce qui peut améliorer la performance et les temps de récupération.

Une option que vous pouvez utiliser pour diviser une grande table en plus petites consiste à partitionner. Le partitionnement répartit des portions de votre grande table en fichiers distincts en fonction des règles que vous spécifiez. Par exemple, si vous stockez des transactions par date, vous pouvez créer des règles de partitionnement qui répartissent des transactions plus anciennes en fichiers distincts en utilisant le partitionnement. Ensuite, vous pouvez archiver régulièrement les données de transaction historiques qui n'ont pas besoin d'être rapidement utilisables par votre application. Pour de plus amples informations, veuillez consulter Partitionnement dans la documentation MySQL.

Pour déterminer la taille de fichier d'une table

Utilisez la commande SQL suivante pour déterminer si certaines de vos tables sont trop volumineuses et peuvent faire l'objet d'un partitionnement. Pour mettre à jour les statistiques de table, exécutez une commande `ANALYZE TABLE` sur chaque table. Pour de plus amples informations, veuillez consulter Instruction ANALYZE TABLE dans la documentation MySQL.

```
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');
```

Pour activer les espaces de table file-per-table InnoDB

- Pour activer les espaces de table file-per-table d'InnoDB, affectez au paramètre `innodb_file_per_table` la valeur `1` dans le groupe de paramètres relatif à l'instance de base de données.

Pour désactiver les espaces de table file-per-table InnoDB

- Pour désactiver les espaces de table file-per-table d'InnoDB, affectez au paramètre `innodb_file_per_table` la valeur `0` dans le groupe de paramètres relatif à l'instance de base de données.

Pour plus d'informations sur la mise à jour d'un groupe de paramètres, consultez Utilisation de groupes de paramètres de base de données (p. 225).

Après avoir activé ou désactivé les espaces de table file-per-table InnoDB, vous pouvez émettre une commande `ALTER TABLE`. Vous pouvez utiliser cette commande pour déplacer une table de l'espace de table global vers son propre espace de table. Vous pouvez également déplacer une table de son propre espace de table vers l'espace de table global. Voici un exemple.

```
ALTER TABLE table_name ENGINE=InnoDB, ALGORITHM=COPY;
```

Sécurité MariaDB sur Amazon RDS

La sécurité des instances de base de données Amazon RDS MariaDB est gérée à trois niveaux :

- AWS Identity and Access Management contrôle les personnes autorisées à exécuter des actions de gestion Amazon RDS sur les instances de base de données. Lorsque vous vous connectez à AWS à l'aide des informations d'identification IAM, votre compte IAM doit disposer des stratégies IAM qui accordent les autorisations requises pour exécuter les opérations de gestion Amazon RDS. Pour plus d'informations, consultez Identity and Access Management dans Amazon RDS (p. 1536).
- Lorsque vous créez une instance de base de données, vous utilisez un groupe de sécurité VPC ou un groupe de sécurité DB pour contrôler les appareils et les instances Amazon EC2 qui peuvent ouvrir des connexions au point de terminaison et au port de l'instance de base de données. Ces connexions peuvent être effectuées à l'aide du protocole SSL (Secure Socket Layer). En outre, les règles de pare-feu de votre entreprise peuvent contrôler si les appareils en cours d'exécution dans votre entreprise peuvent ouvrir des connexions à l'instance de base de données.
- Une fois qu'une connexion a été ouverte sur une instance de base de données MariaDB, l'authentification de la connexion et les autorisations sont appliquées de la même manière que dans une instance autonome de MariaDB. Les commandes telles que `CREATE USER`, `RENAME USER`, `GRANT`, `REVOKE` et `SET PASSWORD` fonctionnent de la même façon que dans les bases de données autonomes, comme le fait la modification directe des tables du schéma de base de données.

Lorsque vous créez une instance de base de données Amazon RDS, l'utilisateur principal a les privilèges par défaut suivants :

- `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`

  Ce privilège est limité sur les instances de base de données Amazon RDS MariaDB. Il n'accorde pas l'accès aux opérations FLUSH LOGS ou FLUSH TABLES WITH READ LOCK.
- `replication client`
- `replication slave`
- `select`
- `show databases`
- `show view`
- `trigger`
- `update`

Pour plus d'informations sur ces privilèges, consultez Gestion des comptes d'utilisateur dans la documentation MariaDB.

> **Note**
>
> Bien que vous puissiez supprimer l'utilisateur principal sur une instance de base de données, il est déconseillé d'agir ainsi. Pour recréer l'utilisateur maître, utilisez l'API `ModifyDBInstance` ou l'outil de ligne de commande AWS `modify-db-instance` et spécifiez un nouveau mot de passe utilisateur maître avec le paramètre approprié. Si l'utilisateur maître n'existe pas dans l'instance, il est créé avec le mot de passe spécifié.

Pour fournir des services de gestion à chaque instance de base de données, l'utilisateur `rdsadmin` est créé lors de la création de l'instance de base de données. Les tentatives de supprimer, renommer et modifier le mot de passe du compte `rdsadmin`, ou d'en modifier les privilèges, génèrent une erreur.

Pour autoriser la gestion de l'instance de base de données, les commandes standard `kill` et `kill_query` ont fait l'objet de restrictions. Les commandes Amazon RDS `mysql.rds_kill`, `mysql.rds_kill_query` et `mysql.rds_kill_query_id` sont fournies pour être utilisées dans MariaDB et dans MySQL également, de telle sorte que vous puissiez mettre fin aux sessions utilisateur ou aux requêtes sur les instances de base de données.

Utilisation de SSL avec une instance de base de données MariaDB

Amazon RDS prend en charge les connexions SSL avec les instances de base de données exécutant le moteur de base de données MariaDB.

Amazon RDS crée un certificat SSL et l'installe sur l'instance de base de données quand Amazon RDS alloue l'instance. Ces certificats sont signés par une autorité de certification. Le certificat SSL inclut le point de terminaison de l'instance de base de données en tant que nom commun du certificat SSL pour assurer une protection contre les attaques par usurpation.

Pour de plus amples informations sur le téléchargement de certificats, veuillez consulter Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).

MariaDB utilise yaSSL pour les connexions sécurisées dans les versions suivantes :

- Version MariaDB 10.1.26 et versions 10.1 antérieures
- Version MariaDB 10.0.32 et versions 10.0 antérieures

MariaDB utilise OpenSSL pour les connexions sécurisées dans les versions suivantes :

- Versions MariaDB 10.4
- Versions MariaDB 10.3
- Versions MariaDB 10.2
- Version MariaDB 10.1.31 et versions 10.1 ultérieures
- Version MariaDB 10.0.34 et versions 10.0 ultérieures

Amazon RDS pour MariaDB prend en charge les versions 1.0, 1.1 et 1.2 du protocole TLS (Transport Layer Security). Le tableau suivant affiche la prise en charge du protocole TLS pour les versions MySQL.

Version MariaDB	TLS 1.0	TLS 1.1	TLS 1.2
MariaDB 10.4	Pris en charge	Pris en charge	Pris en charge
MariaDB 10.3	Pris en charge	Pris en charge	Pris en charge
MariaDB 10.2	Pris en charge	Pris en charge	Pris en charge
MariaDB 10.1	Pris en charge	Pris en charge pour la version 10.1.31 et les versions 10.1 ultérieures	Pris en charge pour la version 10.1.31 et les versions 10.1 ultérieures
MariaDB 10.0	Pris en charge	Pris en charge pour la version 10.0.34 et les versions 10.0 ultérieures	Pris en charge pour la version 10.0.34 et les versions 10.0 ultérieures

Pour chiffrer les connexions à l'aide du client mysql par défaut, lancez le client mysql à l'aide du paramètre `--ssl-ca` pour référencer la clé publique, comme illustré dans l'exemple suivant.

L'exemple suivant montre comment lancer le client à l'aide du paramètre `--ssl-ca` pour MariaDB 10.2 ou version ultérieure.

```
mysql -h myinstance.c9akciq32.rds-us-east-1.amazonaws.com
--ssl-ca=[full path]rds-combined-ca-bundle.pem --ssl-mode=REQUIRED
```

L'exemple suivant montre comment lancer le client à l'aide du paramètre `--ssl-ca` pour MariaDB 10.1 ou version antérieure.

```
mysql -h myinstance.c9akciq32.rds-us-east-1.amazonaws.com
--ssl-ca=[full path]rds-combined-ca-bundle.pem --ssl-verify-server-cert
```

Vous pouvez exiger des connexions SSL pour des comptes d'utilisateur spécifiques. Par exemple, vous pouvez utiliser l'une des instructions suivantes, selon votre version MariaDB, pour exiger des connexions SSL sur le compte utilisateur `encrypted_user`.

Pour MariaDB 10.2 et version ultérieure, utilisez la déclaration suivante.

```
ALTER USER 'encrypted_user'@'%' REQUIRE SSL;
```

Pour MariaDB 10.1 et version antérieure, utilisez la déclaration suivante.

```
GRANT USAGE ON *.* TO 'encrypted_user'@'%' REQUIRE SSL;
```

Pour plus d'informations sur les connexions SSL avec MariaDB, consultez la page SSL Overview dans la documentation MariaDB.

Préparation du cache

La préparation du cache InnoDB (version 10.2 et suivante) et XtraDB (versions 10.0 et 10.1) peut fournir des gains de performances pour votre instance de base de données MariaDB en enregistrant l'état actuel du pool de mémoires tampons lorsque l'instance de base de données est arrêtée, puis en rechargeant le pool de mémoires tampons à partir des informations enregistrées au démarrage de l'instance de base de données. Cette approche contourne la nécessité de « préparer » le pool de tampons à partir d'une utilisation normale de la base de données et précharge à la place le pool de tampons avec les pages des requêtes courantes connues. Pour plus d'informations sur la préparation du cache, consultez Vidage et restauration du pool de tampons dans la documentation MariaDB.

La préparation du cache est activée par défaut sur les instances de base de données MariaDB 10.2 et ultérieures. Pour l'activer, définissez les paramètres `innodb_buffer_pool_dump_at_shutdown` et `innodb_buffer_pool_load_at_startup` avec la valeur 1 dans le groupe de paramètres de votre instance de base de données. La modification de ces valeurs dans un groupe de paramètres affecte toutes les instances de base de données MariaDB qui utilisent ce groupe de paramètres. Pour activer la préparation du cache pour des instances de base de données MariaDB spécifiques, vous aurez peut-être à créer un groupe de paramètres pour ces instances de base de données. Pour plus d'informations sur les groupes de paramètres, consultez Utilisation de groupes de paramètres de base de données (p. 225).

La préparation du cache fournit principalement une amélioration des performances pour les instances de bases de données qui utilisent le stockage standard. Si vous utilisez le stockage PIOPS, vous ne constatez généralement pas d'amélioration significative des performances.

> **Important**
>
> Si votre instance de base de données MariaDB ne se ferme pas normalement, comme lors d'un basculement, l'état du pool de tampons n'est pas enregistré sur le disque. Dans ce cas, MariaDB charge n'importe quel fichier du pool de tampons disponible au redémarrage de l'instance de base de données. Il n'en résulte aucun dommage, mais le pool de tampons restauré peut ne pas refléter l'état le plus récent du pool de tampons avant le redémarrage. Pour vous assurer d'avoir un état récent du pool de mémoires tampons disponible afin de préparer le cache au démarrage, il est recommandé que vous vidiez régulièrement le pool de mémoires tampons « à la demande ». Vous pouvez vider ou charger le pool de tampons à la demande.
> Vous pouvez créer un événement pour vider le pool de tampons automatiquement et à intervalles réguliers. Par exemple, l'instruction suivante crée un événement nommé `periodic_buffer_pool_dump` qui vide le pool de mémoires tampons toutes les heures.
>
> ```
> CREATE EVENT periodic_buffer_pool_dump
> ```

```
ON SCHEDULE EVERY 1 HOUR
DO CALL mysql.rds_innodb_buffer_pool_dump_now();
```

Pour plus d'informations, consultez Événements dans la documentation MariaDB.

Vidage et chargement du pool de tampons à la demande

Vous pouvez enregistrer et charger le cache à la demande à l'aide des procédures stockées suivantes :

- Pour vider l'état actuel du pool de mémoires tampons sur le disque, appelez la procédure stockée mysql.rds_innodb_buffer_pool_dump_now (p. 920).
- Pour charger l'état enregistré du pool de mémoires tampons à partir du disque, appelez la procédure stockée mysql.rds_innodb_buffer_pool_load_now (p. 920).
- Pour annuler une opération de chargement en cours, appelez la procédure stockée mysql.rds_innodb_buffer_pool_load_abort (p. 920).

Paramètres de base de données pour MariaDB

Par défaut, une instance de base de données MariaDB utilise un groupe de paramètres DB qui est spécifique à une base de données MariaDB. Ce groupe de paramètres contient certains, mais pas la totalité, des paramètres du groupe de paramètres de base de données Amazon RDS du moteur de base de données MySQL. Il contient également un certain nombre de nouveaux paramètres propres à MariaDB. Pour plus d'informations sur les paramètres disponibles pour le moteur de base de données Amazon RDS MariaDB, consultez Paramètres pour MariaDB (p. 584).

Tâches DBA courantes pour MariaDB

Supprimer des sessions ou des requêtes, ignorer des erreurs de réplication, utiliser les espaces de table InnoDB (version 10.2 et suivante) et XtraDB (versions 10.0 et 10.1) pour améliorer les temps de récupération sur incident et gérer l'historique global des statuts sont des tâches DBA courantes que vous pouvez exécuter dans une instance de base de données MariaDB. Vous pouvez gérer ces tâches tout comme dans une instance de base de données MySQL Amazon RDS, comme décrit dans Tâches DBA courantes pour les instances de base de données MySQL (p. 881). Les instructions de récupération sur incident se rapportent ici au moteur InnoDB MySQL, mais s'appliquent aussi bien à une instance MariaDB exécutant InnoDB ou XtraDB.

Fuseau horaire local pour les instances de base de données MariaDB

Par défaut, le fuseau horaire d'une instance de base de données MariaDB RDS est le fuseau UTC (temps universel). Vous pouvez à la place définir le fuseau horaire de votre instance de base de données sur le fuseau horaire local de votre application.

Pour définir le fuseau horaire local d'une instance de base de données, définissez le paramètre `time_zone` du groupe de paramètres de votre instance de base de données avec l'une

des valeurs prises en charge et répertoriées plus bas dans cette section. Lorsque vous définissez le paramètre `time_zone` d'un groupe de paramètres, toutes les instances de base de données et tous les réplicas en lecture qui ont recours à ce groupe de paramètres sont modifiés de façon à utiliser le nouveau fuseau horaire local. Pour plus d'informations sur la définition des paramètres d'un groupe de paramètres, consultez Utilisation de groupes de paramètres de base de données (p. 225).

Une fois que vous avez défini le fuseau horaire local, toutes les nouvelles connexions à la base de données reflètent la modification. Si des connexions à votre base de données sont ouvertes lorsque vous modifiez le fuseau horaire local, la mise à jour du fuseau horaire local n'apparaît pas tant que vous n'avez pas fermé la connexion et n'en avez pas ouvert une nouvelle.

Vous pouvez définir un fuseau horaire local différent pour une instance de base de données et un ou plusieurs de ses réplicas en lecture. Pour ce faire, utilisez un autre groupe de paramètres pour l'instance de base de données et les réplicas, et définissez le paramètre `time_zone` de chaque groupe de paramètres avec un autre fuseau horaire local.

Si la réplication s'effectue entre les régions AWS, l'instance de base de données source et le réplica en lecture utilisent des groupes de paramètres différents (les groupes de paramètres sont propres à chaque région AWS). Pour que chaque instance utilise le même fuseau horaire local, vous devez définir le paramètre `time_zone` dans les groupes de paramètres de l'instance et du réplica en lecture.

Lorsque vous restaurez une instance de base de données à partir d'un instantané de base de données, le fuseau horaire local a la valeur UTC. Vous pouvez mettre à jour le fuseau horaire sur votre fuseau horaire local une fois la restauration terminée. Si vous restaurez une instance de base de données à un instant dans le passé, le fuseau horaire local de l'instance de base de données restaurée est le paramètre de fuseau horaire du groupe de paramètres de l'instance de base de données restaurée.

Vous pouvez définir votre fuseau horaire local avec l'une des valeurs suivantes.

`Africa/Cairo`	`Asia/Bangkok`	`Australia/Darwin`
`Africa/Casablanca`	`Asia/Beirut`	`Australia/Hobart`
`Africa/Harare`	`Asia/Calcutta`	`Australia/Perth`
`Africa/Monrovia`	`Asia/Damascus`	`Australia/Sydney`
`Africa/Nairobi`	`Asia/Dhaka`	`Brazil/East`
`Africa/Tripoli`	`Asia/Irkutsk`	`Canada/Newfoundland`
`Africa/Windhoek`	`Asia/Jerusalem`	`Canada/Saskatchewan`
`America/Araguaina`	`Asia/Kabul`	`Europe/Amsterdam`
`America/Asuncion`	`Asia/Karachi`	`Europe/Athens`
`America/Bogota`	`Asia/Kathmandu`	`Europe/Dublin`
`America/Caracas`	`Asia/Krasnoyarsk`	`Europe/Helsinki`
`America/Chihuahua`	`Asia/Magadan`	`Europe/Istanbul`
`America/Cuiaba`	`Asia/Muscat`	`Europe/Kaliningrad`
`America/Denver`	`Asia/Novosibirsk`	`Europe/Moscow`
`America/Fortaleza`	`Asia/Riyadh`	`Europe/Paris`
`America/Guatemala`	`Asia/Seoul`	`Europe/Prague`

America/Halifax	Asia/Shanghai	Europe/Sarajevo
America/Manaus	Asia/Singapore	Pacific/Auckland
America/Matamoros	Asia/Taipei	Pacific/Fiji
America/Monterrey	Asia/Tehran	Pacific/Guam
America/Montevideo	Asia/Tokyo	Pacific/Honolulu
America/Phoenix	Asia/Ulaanbaatar	Pacific/Samoa
America/Santiago	Asia/Vladivostok	US/Alaska
America/Tijuana	Asia/Yakutsk	US/Central
Asia/Amman	Asia/Yerevan	US/Eastern
Asia/Ashgabat	Atlantic/Azores	US/East-Indiana
Asia/Baghdad	Australia/Adelaide	US/Pacific
Asia/Baku	Australia/Brisbane	UTC

Connexion à une instance de base de données exécutant le moteur de base de données MariaDB

Une fois qu'Amazon RDS a provisionné votre instance de base de données, vous pouvez utiliser n'importe quelle application cliente MariaDB standard pour vous connecter à l'instance. Dans la chaîne de connexion, vous spécifiez l'adresse DNS (système de noms de domaine) du point de terminaison de l'instance de base de données en tant que paramètre hôte. Vous spécifiez également le numéro de port du point de terminaison de l'instance de base de données en tant que paramètre de port.

Vous pouvez utiliser la AWS Management Console, la commande describe-db-instances de l'interface AWS CLI ou l'opération d'API Amazon RDS DescribeDBInstances pour répertorier les détails d'une instance de base de données Amazon RDS, notamment son point de terminaison.

Pour rechercher le point de terminaison d'une instance de base de données MariaDB dans l'AWS Management Console

1. Ouvrez la console RDS et choisissez Bases de données pour afficher une liste de vos instances de bases de données.
2. Choisissez le nom de l'instance de base de données MariaDB pour afficher ses détails.
3. Dans l'onglet Connectivity & security (Connectivité et sécurité), copiez le point de terminaison. Notez également le numéro du port. Vous avez besoin du point de terminaison et du numéro de port pour vous connecter à l'instance de base de données.

Si la valeur d'un point de terminaison est `mariadb-instance1.123456789012.us-east-1.rds.amazonaws.com:3306`, vous spécifiez les valeurs suivantes dans une chaîne de connexion MariaDB :

- Pour un hôte ou nom d'hôte, spécifiez `mariadb-instance1.123456789012.us-east-1.rds.amazonaws.com`
- Pour un port, spécifiez `3306`.

Vous pouvez vous connecter à une instance de base de données MariaDB Amazon RDS en utilisant des outils tels que l'utilitaire de ligne de commande mysql. Pour de plus amples informations sur l'utilisation de l'utilitaire mysql, veuillez consulter Client de ligne de commande mysql dans la documentation MariaDB. Heidi est une application basée sur l'interface utilisateur graphique que vous pouvez utiliser pour la connexion. Pour de plus amples informations, veuillez consulter la page Télécharger Heidi.

Pour se connecter à une instance de base de données hors de son Amazon VPC, l'instance de base de données doit être accessible au public, l'accès doit être accordé en utilisant les règles entrantes du groupe de sécurité de l'instance de base de données et d'autres exigences doivent être respectées. Pour de plus amples informations, veuillez consulter Impossible de se connecter à l'instance de base de données Amazon RDS (p. 1639).

Vous pouvez utiliser le chiffrement SSL sur les connexions à une instance de base de données MariaDB Amazon RDS. Pour plus d'informations, consultez Utilisation de SSL avec une instance de base de données MariaDB (p. 551).

Connexion depuis l'utilitaire mysql

Pour vous connecter à une instance de base de données à l'aide de l'utilitaire mysql, entrez la commande suivante à l'invite de commandes d'un ordinateur client. Vous êtes alors connecté à une base de données sur une instance de base de données MariaDB. Remplacez *<endpoint>* par le nom DNS (point de terminaison) de votre instance de base de données et *<quartermaster>* par le nom d'utilisateur principal que vous avez utilisé. Indiquez le mot de passe principal que vous avez utilisé lorsque vous êtes invité à entrer un mot de passe.

```
mysql -h <endpoint> -P 3306 -u <mymasteruser> -p
```

Après avoir entré le mot de passe pour l'utilisateur, le résultat suivant doit normalement s'afficher.

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 272
Server version: 5.5.5-10.0.17-MariaDB-log MariaDB Server

Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql >
```

Connexion à SSL

Amazon RDS crée un certificat SSL pour votre instance de base de données lorsque l'instance est créée. Si vous activez la vérification du certificat SSL, ce dernier inclut le point de terminaison de l'instance de base de données en tant que nom commun du certificat SSL pour assurer une protection contre les attaques par usurpation. Pour vous connecter à votre instance de base de données en utilisant SSL, suivez les étapes suivantes :

Pour se connecter à une instance de base de données avec SSL en utilisant l'utilitaire mysql

1. Téléchargez un certificat racine valide pour toutes les régions AWS.

   Pour de plus amples informations sur le téléchargement de certificats, veuillez consulter Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).
2. Saisissez la commande suivante dans une invite de commande pour vous connecter à une instance de base de données avec SSL en utilisant l'utilitaire `mysql`. Pour le paramètre `-h`, remplacez le nom DNS pour votre instance de base de données. Pour le paramètre `--ssl-ca`, remplacez le nom de fichier du certificat SSL par le nom approprié.

```
mysql -h mariadb-instance1.123456789012.us-east-1.rds.amazonaws.com --ssl-ca=rds-ca-2015-root.pem -p
```

3. Incluez le paramètre `--ssl-verify-server-cert` afin que la connexion SSL vérifie le point de terminaison de l'instance de base de données par rapport au point de terminaison dans le certificat SSL. Exemples :

```
mysql -h mariadb-instance1.123456789012.us-east-1.rds.amazonaws.com --ssl-ca=rds-ca-2015-root.pem --ssl-verify-server-cert -p
```

4. Entrez le mot de passe de l'utilisateur principal quand vous y êtes invité.

Vous devez visualiser des résultats similaires à ce qui suit.

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 272
Server version: 5.5.5-10.0.17-MariaDB-log MariaDB Server

Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql >
```

Dépannage des connexions à votre instance de base de données MariaDB

Les deux causes les plus courantes d'échec de connexion à une nouvelle instance de base de données sont :

- L'instance de base de données a été créée grâce à un groupe de sécurité qui interdit les connexions depuis l'appareil ou l'instance Amazon EC2 où l'application ou l'utilitaire MariaDB s'exécute. Si l'instance de base de données a été créée à l'intérieur d'un Amazon VPC, elle doit avoir un groupe de sécurité VPC qui autorise les connexions. Pour de plus amples informations, veuillez consulter VPC Amazon Virtual Private Cloud et Amazon RDS (p. 1610).

  Vous pouvez ajouter ou modifier une règle entrante dans le groupe de sécurité. Pour Source, choisissez Mon IP. Cela autorise à accéder à l'instance de base de données à partir de l'adresse IP détectée dans votre navigateur.

  Si l'instance de base de données a été créée à l'extérieur d'un VPC, elle doit avoir un groupe de sécurité de bases de données qui autorise les connexions.
- L'instance de base de données a été créée à l'aide du port par défaut 3306, et votre entreprise dispose de règles de pare-feu bloquant les connexions à ce port depuis les appareils de votre réseau d'entreprise. Pour corriger le problème, recréez l'instance avec un port différent.

Pour de plus amples informations sur les problèmes de connexion, veuillez consulter Impossible de se connecter à l'instance de base de données Amazon RDS (p. 1639).

Mise à jour des applications pour se connecter aux instances de bases de données MariaDB à l'aide des nouveaux certificats SSL/TLS

Le 19 septembre 2019, Amazon RDS a publié de nouveaux certificats de l'autorité de certification (CA) à connecter à vos instances de bases de données RDS à l'aide du protocole Secure Socket Layer ou Transport Layer Security (SSL/TLS). Vous trouverez ci-après des informations sur la mise à jour de vos applications afin d'utiliser les nouveaux certificats.

Cette rubrique peut vous aider à déterminer si vos applications nécessitent une vérification du certificat pour se connecter à vos instances de bases de données.

> **Note**
>
> Certaines applications sont configurées pour se connecter à MariaDB uniquement si la vérification du certificat sur le serveur s'effectue avec succès. Pour ces applications, vous devez mettre à jour les magasins d'approbations des applications clientes afin d'inclure les nouveaux certificats de l'autorité de certification.
> Vous pouvez spécifier les modes SSL suivants : `disabled`, `preferred` et `required`. Lorsque vous utilisez le mode SSL `preferred` et que le certificat d'autorité de certification n'existe pas ou n'est pas à jour, le comportement suivant s'applique :
>
> - Pour MariaDB version 10.2 et versions ultérieures, ainsi que les versions mineures et plus récentes des versions 10.0 et 10.1, la connexion n'utilise plus SSL et s'établit toujours avec succès.
>
> Étant donné que ces versions ultérieures utilisent le protocole OpenSSL, un certificat de serveur expiré n'empêche pas l'établissement des connexions, sauf si le mode SSL `required` est spécifié.
> - Pour les versions mineures plus anciennes de MariaDB 10.0 et 10.1, une erreur est renvoyée.
>
> Étant donné que ces versions plus anciennes utilisent le protocole yaSSL, la vérification du certificat est strictement appliquée et la connexion échoue.
>
> Les versions mineures de MariaDB suivantes utilisent le protocole yaSSL :
> - 10.0.17, 10.0.24, 10.0.28, 10.0.31, 10.0.32
> - 10.1.14, 10.1.19, 10.1.23, 10.1.26

Une fois que vous avez mis à jour les certificats de l'autorité de certification dans les magasins d'approbations des applications clientes, vous pouvez soumettre les certificats de vos instances de bases de données à une rotation. Nous vous recommandons vivement de tester ces procédures dans un environnement de développement ou intermédiaire avant de les implémenter dans vos environnements de production.

Pour de plus amples informations sur la rotation de certificats, veuillez consulter Rotation de votre certificat SSL/TLS (p. 1527). Pour en savoir plus sur le téléchargement de certificats, consultez Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525). Pour de plus amples informations sur l'utilisation des protocoles SSL/TLS avec les instances de bases de données MariaDB, veuillez consulter Utilisation de SSL avec une instance de base de données MariaDB (p. 551).

Rubriques

- Contrôle de la nécessité d'une vérification du certificat du client pour qu'il puisse se connecter (p. 561)
- Mise à jour du magasin d'approbations de votre application (p. 562)

- Exemple de code Java pour l'établissement de connexions SSL (p. 563)

Contrôle de la nécessité d'une vérification du certificat du client pour qu'il puisse se connecter

Vous pouvez vérifier si les clients JDBC et les clients MySQL requièrent une vérification du certificat pour pouvoir se connecter.

JDBC

L'exemple suivant avec MySQL Connector/J 8.0 illustre une façon de vérifier les propriétés de connexion JDBC d'une application afin de déterminer si les connexions nécessitent un certificat valide pour réussir. Pour de plus amples informations sur l'ensemble des options de connexion JDBC pour MySQL, veuillez consulter Configuration Properties dans la documentation MySQL.

Lorsque vous utilisez MySQL Connector/J 8.0, une connexion SSL nécessite la vérification du certificat de l'autorité de certification sur le serveur si vos propriétés de connexion ont `sslMode` défini sur `VERIFY_CA` ou `VERIFY_IDENTITY`, comme illustré dans l'exemple suivant.

```
Properties properties = new Properties();
properties.setProperty("sslMode", "VERIFY_IDENTITY");
properties.put("user", DB_USER);
properties.put("password", DB_PASSWORD);
```

> **Note**
>
> Si vous utilisez MySQL Java Connector v5.1.38 ou version ultérieure, ou MySQL Java Connector v8.0.9 ou version ultérieure, pour vous connecter à vos bases de données, même si vous n'avez pas explicitement configuré vos applications de manière à utiliser SSL/TLS lors de la connexion à vos bases de données, ces pilotes clients utilisent par défaut SSL/TLS. En outre, lors de l'utilisation de SSL/TLS, ils effectuent une vérification partielle du certificat et ne parviennent pas à se connecter si le certificat du serveur de base de données est expiré.

MySQL

Les exemples suivants avec le client MySQL montrent deux façons de vérifier la connexion MySQL d'un script pour déterminer si les connexions nécessitent un certificat valide pour réussir. Pour de plus amples informations sur l'ensemble des options de connexion avec le client MySQL, veuillez consulter Client-Side Configuration for Encrypted Connections dans la documentation MySQL.

Lorsque vous utilisez MySQL 5.7 or MySQL 8.0, une connexion SSL nécessite la vérification du certificat de l'autorité de certification sur le serveur si pour l'option `--ssl-mode`, vous spécifiez `VERIFY_CA` ou `VERIFY_IDENTITY`, comme illustré dans l'exemple suivant.

```
mysql -h mysql-database.rds.amazonaws.com -uadmin -ppassword --ssl-ca=/tmp/ssl-cert.pem --
ssl-mode=VERIFY_CA
```

Lorsque vous utilisez le client MySQL 5.6, une connexion SSL nécessite la vérification du certificat de l'autorité de certification sur le serveur si vous spécifiez l'option `--ssl-verify-server-cert`, comme illustré dans l'exemple suivant.

```
mysql -h mysql-database.rds.amazonaws.com -uadmin -ppassword --ssl-ca=/tmp/ssl-cert.pem --
ssl-verify-server-cert
```

Mise à jour du magasin d'approbations de votre application

Pour de plus amples informations sur la mise à jour du magasin d'approbations pour des applications MySQL, veuillez consulter Using TLS/SSL with MariaDB Connector/J dans la documentation MariaDB.

> **Note**
>
> Lors de la mise à jour du magasin d'approbations, vous pouvez conserver les certificats plus anciens en complément de l'ajout des nouveaux certificats.

Mise à jour du magasin d'approbations de votre application pour JDBC

Vous pouvez mettre à jour le magasin d'approbations pour les applications qui utilisent JDBC dans le cadre de connexions SSL/TLS.

Pour mettre à jour le magasin d'approbations pour les applications JDBC

1. Téléchargez le certificat racine 2019 qui fonctionne pour toutes les régions AWS et placez le fichier dans le répertoire du magasin d'approbations.

   Pour plus d'informations sur le téléchargement du certificat racine, consultez Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).
2. Convertissez le certificat au format .der à l'aide de la commande suivante.

   ```
   openssl x509 -outform der -in rds-ca-2019-root.pem -out rds-ca-2019-root.der
   ```

   Remplacez le nom du fichier par celui du fichier téléchargé.
3. Importez le certificat dans le magasin de clés à l'aide de la commande suivante.

   ```
   keytool -import -alias rds-root -keystore clientkeystore -file rds-ca-2019-root.der
   ```
4. Vérifiez que le magasin de clés a été mis à jour avec succès.

   ```
   keytool -list -v -keystore clientkeystore.jks
   ```

   Entrez le mot de passe du magasin de clés lorsque vous y êtes invité.

   La sortie doit contenir les lignes suivantes :

```
rds-root,date, trustedCertEntry,
Certificate fingerprint (SHA1):
 D4:0D:DB:29:E3:75:0D:FF:A6:71:C3:14:0B:BF:5F:47:8D:1C:80:96
# This fingerprint should match the output from the below command
openssl x509 -fingerprint -in rds-ca-2019-root.pem -noout
```

Si vous utilisez le pilote JDBC MariaDB Connector/J dans une application, définissez les propriétés suivantes dans l'application.

```
System.setProperty("javax.net.ssl.trustStore", certs);
System.setProperty("javax.net.ssl.trustStorePassword", "password");
```

Lorsque vous démarrez l'application, définissez les propriétés suivantes.

```
java -Djavax.net.ssl.trustStore=/path_to_truststore/MyTruststore.jks -
Djavax.net.ssl.trustStorePassword=my_truststore_password com.companyName.MyApplication
```

Exemple de code Java pour l'établissement de connexions SSL

L'exemple de code suivant montre comment configurer la connexion SSL à l'aide de 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

Une fois que vous avez déterminé que vos connexions de base de données utilisent un protocole SSL/TLS et que vous avez mis à jour le magasin d'approbations de votre application, vous pouvez mettre à jour votre base de données de sorte qu'elle utilise les certificats rds-ca-2019. Pour obtenir des instructions, veuillez consulter l'étape 3 dans Mise à jour de votre certificat CA en modifiant votre instance de base de données (p. 1528).

Mise à niveau du moteur de base de données MariaDB

Lorsque Amazon RDS prend en charge une nouvelle version d'un moteur de base de données, vous pouvez mettre à niveau vos instances de bases de données vers cette nouvelle version. Il existe deux types de mises à niveau pour les instances de base de données MariaDB : les mises à niveau de version majeure et les mises à niveau de version mineure.

Les mises à niveau de version majeure peuvent contenir des modifications de base de données qui ne sont pas rétrocompatibles avec les applications existantes. En conséquence, vous devez effectuer manuellement les mises à niveau de version majeure de vos instances de base de données. Vous pouvez lancer une mise à niveau de version majeure en modifiant votre instance de base de données. Cependant, avant d'effectuer une mise à niveau de version majeure, nous vous recommandons de suivre les étapes décrites dans Mises à niveau des versions majeures pour MariaDB (p. 566).

En revanche, une mise à niveau de version mineure contient uniquement des modifications rétrocompatibles avec les applications existantes. Vous pouvez lancer manuellement une mise à niveau de version mineure en modifiant votre instance de base de données. Vous pouvez également activer l'option Mise à niveau automatique des versions mineures lorsque vous créez ou modifiez une instance de base de données. Dans ce cas, votre instance de base de données est automatiquement mise à niveau une fois que Amazon RDS a testé et approuvé la nouvelle version. Pour de plus amples informations sur la mise à niveau, veuillez consulter Mise à niveau d'une version du moteur d'une instance de base de données (p. 267).

Si votre instance de base de données MariaDB utilise des réplicas en lecture, vous devez mettre à niveau tous les réplicas en lecture avant de mettre à niveau l'instance source. Si votre instance de base de données se trouve dans un déploiement Multi-AZ, les deux réplicas, enregistreur et de secours, sont mis à niveau. Votre instance de base de données peut ne pas être disponible tant que la mise à niveau n'est pas terminée.

Pour plus d'informations sur les versions MariaDB prises en charge et la gestion des versions, consultez Versions de MariaDB sur Amazon RDS (p. 544).

Rubriques

- Présentation de la mise à niveau (p. 564)
- Mises à niveau des versions majeures pour MariaDB (p. 566)
- Mise à niveau d'une instance de base de données MariaDB (p. 566)
- Mises à niveau automatiques des versions mineures pour MariaDB (p. 566)

Présentation de la mise à niveau

Lorsque vous utilisez AWS Management Console pour mettre à niveau une instance de base de données, les cibles de mise à niveau valides pour l'instance de base de données sont affichées. Vous pouvez également utiliser la commande AWS CLI suivante pour identifier les cibles de mise à niveau valides pour une instance de base de données :

Pour Linux, macOS ou Unix :

```
aws rds describe-db-engine-versions \
  --engine mariadb \
  --engine-version version-number \
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

Pour Windows :

```
aws rds describe-db-engine-versions ^
  --engine mariadb ^
  --engine-version version-number ^
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

Par exemple, pour identifier les cibles de mise à niveau valides pour une instance de base de données MariaDB version 10.1.19, exécutez la commande AWS CLI suivante :

Pour Linux, macOS ou Unix :

```
aws rds describe-db-engine-versions \
  --engine mariadb \
  --engine-version 10.1.19 \
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

Pour Windows :

```
aws rds describe-db-engine-versions ^
  --engine mariadb ^
  --engine-version 10.1.19 ^
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

Amazon RDS prend deux instantanés de base de données au cours du processus de mise à niveau. Le premier instantané de base de données porte sur l'instance de base de données avant que toute modification de mise à niveau soit apportée. Si la mise à niveau ne fonctionne pas pour vos bases de données, vous pouvez restaurer cet instantané pour créer une instance de base de données exécutant l'ancienne version. Le second instantané de base de données est pris à la fin de la mise à niveau.

> **Note**
>
> Amazon RDS ne prend des instantanés de base de données que si vous avez défini la période de rétention des sauvegardes de votre instance de base de données sur un nombre supérieur à 0. Pour modifier la période de rétention des sauvegardes, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Une fois la mise à niveau terminée, vous ne pouvez pas rétablir la version précédente du moteur de base de données. Si vous souhaitez revenir à la version précédente, restaurez le premier instantané de base de données pris pour créer une nouvelle instance de base de données.

Vous contrôlez à quel moment vous mettez à niveau votre instance de base de données vers une nouvelle version prise en charge par Amazon RDS. Ce niveau de contrôle vous aide à maintenir la compatibilité avec des versions de base de données spécifiques et à tester les nouvelles versions avec votre application avant un déploiement en production. Lorsque vous êtes prêt, vous pouvez effectuer des mises à niveau de version aux moments qui conviennent le mieux à votre planning.

Si votre instance DB utilise la réplication en lecture, vous devez mettre à niveau tous les réplicas en lecture avant de mettre à niveau l'instance source.

Si votre instance de base de données se trouve dans un déploiement multi-AZ, les deux instances de base de données principale et de secours sont mises à niveau. Les instances de base de données principales et de secours sont mises à niveau en même temps, et vous êtes confronté à une panne jusqu'à ce que la mise à niveau soit terminée. La durée de la panne varie selon votre moteur de base de données, la version du moteur et la taille de votre instance de base de données.

Mises à niveau des versions majeures pour MariaDB

Les mises à niveau de versions majeures peuvent contenir des modifications de base de données qui ne sont pas rétrocompatibles avec les applications existantes. En conséquence, Amazon RDS n'applique pas les mise à niveau de version majeure automatiquement. Vous devez modifier manuellement votre instance de base de données. Nous vous recommandons de tester soigneusement toute mise à niveau avant de l'appliquer à vos instances de production.

Amazon RDS prend en charge les mises à niveau sur place suivantes des versions majeures du moteur de base de données MariaDB :

- MariaDB 10.0 vers MariaDB 10.1
- MariaDB 10.1 vers MariaDB 10.2
- MariaDB 10.2 vers MariaDB 10.3
- MariaDB 10.3 vers MariaDB 10.4

Pour effectuer une mise à niveau de version majeure pour une instance de base de données MariaDB version 10.0 sur Amazon RDS vers MariaDB version 10.1 ou ultérieure, procédez d'abord à la mise à niveau vers chaque version majeure : 10.0 vers 10.1, puis 10.1 vers 10.2, 10.2 vers 10.3 et 10.3 vers 10.4.

Si vous utilisez un groupe de paramètres personnalisé et que vous effectuez une mise à niveau de version majeure, vous devez spécifier un groupe de paramètres par défaut pour la nouvelle version du moteur de base de données ou créer votre propre groupe de paramètres personnalisé pour la nouvelle version du moteur de base de données. L'association du nouveau groupe de paramètres avec l'instance de base de données exige un redémarrage de la base de données initié par le client après la mise à niveau. Le statut du groupe de paramètres de l'instance indique `pending-reboot` si l'instance doit être redémarrée pour que les modifications du groupe de paramètres soient appliquées. Il est possible d'afficher le statut du groupe de paramètres d'une instance dans la console AWS ou en utilisant un appel « describe » tel que `describe-db-instances`.

Mise à niveau d'une instance de base de données MariaDB

Pour plus d'informations sur la mise à niveau manuelle ou automatique d'une instance de base de données MariaDB, consultez la section Mise à niveau d'une version du moteur d'une instance de base de données (p. 267).

Mises à niveau automatiques des versions mineures pour MariaDB

Si vous activez l'option Mise à niveau automatique des versions mineures au moment de créer ou modifier une instance de base de données, votre instance de base de données peut être mise à niveau automatiquement.

Pour certaines versions majeures de RDS pour MariaDB dans certaines régions AWS, RDS désigne une version mineure comme version de mise à niveau automatique. Une fois qu'une version mineure a été testée et approuvée par Amazon RDS, la mise à niveau de la version mineure se produit automatiquement pendant votre fenêtre de maintenance. RDS ne définit pas automatiquement les dernières versions mineures publiées comme version de mise à niveau automatique. Avant de désigner une publication de version récente comme version de mise à niveau automatique, RDS prend en compte plusieurs critères, à savoir :

- Problèmes de sécurité connus
- Bogues dans la version de la communauté MySQL
- Stabilité globale du parc depuis la publication de la version mineure

Vous pouvez utiliser la commande AWS CLI et le script suivants pour déterminer la version cible de mise à niveau mineure automatique actuelle pour une version mineure MariaDB spécifiée dans une région AWS spécifique.

```
aws rds describe-db-engine-versions --output=table --engine mariadb --engine-version minor-
version --region region
```

Par exemple, la commande AWS CLI suivante détermine la cible de mise à niveau mineure automatique pour MariaDB version mineure 10.2.11 dans la région AWS USA Est (Ohio) (us-east-2).

```
aws rds describe-db-engine-versions --output=table --engine mariadb --engine-version
 10.2.11 --region us-east-2
```

Votre sortie est similaire à ce qui suit.

```
-----------------------------------------------------------------------------------------------
|                                  DescribeDBEngineVersions
 |
+---------------------------------------------------------------------------------------------
+
||                                     DBEngineVersions
 ||
|+--------------------------------------------------+-------------------------------------
+|
||  DBEngineDescription                             |  MariaDb Community Edition
 ||
||  DBEngineVersionDescription                      |  MariaDB 10.2.11
 ||
||  DBParameterGroupFamily                          |  mariadb10.2
 ||
||  Engine                                          |  mariadb
 ||
||  EngineVersion                                   |  10.2.11
 ||
||  Status                                          |  available
 ||
||  SupportsGlobalDatabases                         |  False
 ||
||  SupportsLogExportsToCloudwatchLogs              |  True
 ||
||  SupportsParallelQuery                           |  False
 ||
||  SupportsReadReplica                             |  True
 ||
|+--------------------------------------------------+-------------------------------------
+|
|||                                   ExportableLogTypes
 |||
```

```
||+-------------------------------------------------------------------------------------------
+||
|||  audit
 |||
|||  error
 |||
|||  general
 |||
|||  slowquery
 |||
||+-------------------------------------------------------------------------------------------
+||
|||                                   ValidUpgradeTarget
 |||
||+-------------+------------------+----------+----------------+--------------------------
+||
||| AutoUpgrade |   Description    | Engine   | EngineVersion  |  IsMajorVersionUpgrade
 |||
||+-------------+------------------+----------+----------------+--------------------------
+||
|||  False      |  MariaDB 10.2.12 |  mariadb |  10.2.12       |  False
 |||
|||  False      |  MariaDB 10.2.15 |  mariadb |  10.2.15       |  False
 |||
|||  True       |  MariaDB 10.2.21 |  mariadb |  10.2.21       |  False
 |||
|||  False      |  MariaDB 10.3.8  |  mariadb |  10.3.8        |  True
 |||
|||  False      |  MariaDB 10.3.20 |  mariadb |  10.3.20       |  True
 |||
|||  False      |  MariaDB 10.3.23 |  mariadb |  10.3.23       |  True
 |||
||+-------------+------------------+----------+----------------+--------------------------
+||
```

Dans cet exemple, la valeur de `AutoUpgrade` est `True` pour MariaDB version 10.2.21. Ainsi, la cible de mise à niveau mineure automatique est MariaDB version 10.2.21, comme mis en évidence dans la sortie.

Une instance de base de données MariaDB est automatiquement mise à niveau pendant votre fenêtre de maintenance si les critères suivants sont réunis :

- L'option Mise à niveau automatique des versions mineures est activée pour l'instance de base de données.
- L'instance de base de données exécute une version mineure du moteur de base de données qui est inférieure à la version mineure de la mise à niveau automatique actuelle.

Pour plus d'informations, consultez Mise à niveau automatique de la version mineure du moteur (p. 269).

Migration des données à partir d'un instantané de base de données MySQL vers une instance de base de données MariaDB

Vous pouvez migrer un instantané de base de données MySQL Amazon RDS vers une nouvelle instance de base de données exécutant MariaDB 10.1 à l'aide de la AWS Management Console, de l'AWS CLI ou de l'API Amazon RDS. Vous devez créer l'instantané de base de données à partir d'une instance de base de données Amazon RDS exécutant MySQL 5.6. Pour savoir comment créer instantané de base de données RDS MySQL, consultez Création d'un instantané de base de données (p. 327).

Après la migration de MySQL vers MariaDB, l'instance de base de données MariaDB sera associée au groupe d'options et au groupe de paramètres de base de données par défaut. Après la restauration de l'instantané de base de données, vous pouvez associer un groupe de paramètres de base de données personnalisé pour la nouvelle instance de base de données. Toutefois, un groupe de paramètres MariaDB a un ensemble différent de variables système configurables. Pour de plus amples informations sur les différences entre les variables système MySQL et MariaDB, veuillez consulter System Variable Differences Between MariaDB 10.1 and MySQL 5.6. Pour en savoir plus sur les groupes de paramètres de base de données, consultez Utilisation de groupes de paramètres de base de données (p. 225). Pour de plus amples informations sur les groupes d'options, veuillez consulter Utilisation de groupes d'options (p. 209).

Incompatibilités entre MariaDB et MySQL

Les incompatibilités entre MySQL et MariaDB incluent les éléments suivants :

- Vous ne pouvez pas migrer un instantané de base de données créé avec MySQL 5.5 vers MariaDB 10.1.
- Vous ne pouvez pas migrer un instantané de base de données créé avec MySQL 5.7 vers MariaDB.
- Vous ne pouvez pas migrer un instantané de base de données créé avec MySQL 8.0 vers MariaDB.
- Vous ne pouvez pas migrer un instantané chiffré.
- Si la base de données MySQL source utilise un hachage SHA256 du mot de passe, vous devez réinitialiser les mots de passe utilisateur qui ont été hachés via SHA256 avant que de vous être connecté à la base de données MariaDB. Le code suivant montre comment réinitialiser un mot de passe qui a été haché via SHA256 :

```
SET old_passwords = 0;
UPDATE mysql.user SET plugin = 'mysql_native_password',
Password = PASSWORD('new_password')
WHERE (User, Host) = ('master_user_name', %);
FLUSH PRIVILEGES;
```

- Si votre compte d'utilisateur principal RDS utilise le hachage de mot de passe SHA-256, le mot de passe doit être réinitialisé à l'aide de la commande `modify-db-instance` RDS de l'AWS CLI, de l'opération de l'API ModifyDBInstance ou d'AWS Management Console. Pour plus d'informations sur la modification d'une instance de base de données , consultez Modification d'une instance de base de données Amazon RDS (p. 243).
- MariaDB ne prend pas en charge le plug-in Memcached ; toutefois, les données utilisées par le plug-in Memcached sont stockées dans les tables InnoDB. Après la migration d'un instantané de base de données MySQL, vous pouvez accéder aux données utilisées par le plug-in Memcached à l'aide de SQL. Pour de plus amples informations sur la base de données innodb_memcache, veuillez consulter la section InnoDB memcached Plugin Internals.

Exécution de la migration

Vous pouvez migrer un instantané de base de données MySQL Amazon RDS vers une nouvelle instance de base de données MariaDB avec la AWS Management Console,à l'aide de l'AWS CLI ou de l'API RDS.

Console

Pour migrer un instantané de base de données MySQL vers une instance de base de données MariaDB

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.

2. Dans le panneau de navigation, choisissez Instantanés, puis sélectionnez l'instantané de base de données MySQL que vous souhaitez migrer.
3. Pour Actions, sélectionnez Migrer l'instantané. La page Migrer la base de données apparaît.
4. Pour Migrate to DB Engine (Migrer au moteur de base de données), choisissez mariadb.
5. Dans la page Migrer la base de données, fournissez des informations supplémentaires dont RDS a besoin pour lancer l'instance de base de données MariaDB.

   - Version du moteur de base de données : choisissez la version du moteur de base de données MariaDB que vous souhaitez utiliser. Pour plus d'informations, consultez Mise à niveau du moteur de base de données MariaDB (p. 564).
   - Classe d'instance de base de données : choisissez une classe d'instance de base de données qui possède le stockage et la capacité requis pour votre base de données. Par exemple, db.r3.large. Pour toutes les applications de production nécessitant des performances d'E/S rapides et cohérentes, nous recommandons d'utiliser le stockage des IOPS provisionnés. Pour plus d'informations, consultez Stockage SSD d'I/O par seconde provisionnées (p. 33). MariaDB 10.1 ne prend pas en charge les classes d'instance de base de données de génération précédente. Pour plus d'informations, consultez Classes d'instances de base de données (p. 6).
   - Déploiement multi-AZ : si vous souhaitez déployer votre instance de base de données dans plusieurs zones de disponibilité, choisissez Oui. Dans le cas contraire, choisissez Non. Pour plus d'informations, consultez Régions, zones de disponibilité et zones locales (p. 39).
   - ID d'instantané de base de données : tapez un nom pour l'identifiant d'instantané de base de données.

     L'identifiant d'instantané de base de données respecte les contraintes suivantes :

     - Il doit contenir entre 1 et 255 caractères alphanumériques ou traits d'union.
     - Le caractère doit être une lettre.
     - Il ne peut pas se terminer par un trait d'union ou contenir deux traits d'union consécutifs.

     Si vous restaurez à partir d'un instantané de base de données manuel partagé, l'identifiant d'instantané de base de données doit être l'Amazon Resource Name (ARN) de l'instantané de base de données partagé.
   - DB Instance Identifier (Identifiant d'instance DB) : tapez un nom pour l'instance de base de données, qui soit unique pour votre compte dans la région AWS où l'instance de base de données résidera. Cet identifiant est utilisé dans les adresses de point de terminaison des instances de votre instance de base de données.

     L'identifiant d'instance de base de données obéit aux contraintes suivantes :

     - Il doit contenir entre 1 et 63 caractères alphanumériques ou traits d'union.
     - Son premier caractère doit être une lettre.
     - Il ne peut pas se terminer par un trait d'union ou contenir deux traits d'union consécutifs.
     - Il doit être unique pour toutes les instances de base de données de votre compte AWS au sein d'une région AWS.
   - Virtual Private Cloud (VPC) : si vous disposez d´un VPC existant, vous pouvez l'utiliser avec votre instance de base de données MariaDB en sélectionnant votre identifiant VPC, par exemple `vpc-a464d1c1`. Pour plus d'informations sur le VPC, consultez VPC Amazon Virtual Private Cloud et Amazon RDS (p. 1610) .

     Sinon, vous pouvez choisir de demander à Amazon RDS de créer un VPC pour vous, en sélectionnant Créer un VPC.

     Vous ne pouvez pas créer des instances MariaDB dans le réseau EC2-Classic.
   - Groupe de sous-réseaux : si vous avez un groupe de sous-réseaux existant, vous pouvez utiliser ce groupe de sous-réseaux avec votre instance de base de données MariaDB en sélectionnant votre identifiant de groupe de sous-réseaux, par exemple `gs-subnet-group1`.

Sinon, vous pouvez choisir de demander à Amazon RDS de créer un groupe de sous-réseaux pour vous en sélectionnant Create a new subnet group.

- Accessibilité publique : choisissez Non pour spécifier que les instances de votre instance de base de données ne sont accessibles que par les ressources à l'intérieur de votre VPC. Choisissez Oui pour spécifier que les instances de votre instance de base de données ne sont accessibles que par les ressources du réseau public. La valeur par défaut est Oui.
- Zone de disponibilité : choisissez la Zone de disponibilité pour héberger l'instance principale de votre instance de base de données MariaDB. Pour que Amazon RDS choisisse une Zone de disponibilité pour vous, sélectionnez Aucune préférence.
- Port de la base de données : tapez le port par défaut à utiliser lors de la connexion aux instances figurant dans l'instance de base de données. La valeur par défaut est `3306`.

  Il se peut que vous soyez derrière un pare-feu d'entreprise qui n'autorise pas l'accès aux ports par défaut, tels que le port par défaut MySQL `3306`. Dans ce cas, fournissez une valeur de port que votre pare-feu d'entreprise autorise.
- Groupe d'options : choisissez le groupe d'options que vous voulez associer à l'instance de base de données. Pour plus d'informations, consultez Utilisation de groupes d'options (p. 209).
- Chiffrement : choisissez Activer le chiffrement pour que votre nouvelle instance de base de données MariaDB soit chiffrée « au repos ». Si vous choisissez Activer le chiffrement, vous devez choisir une clé de chiffrement AWS KMS comme valeur Clé principale.
- Mise à niveau automatique de versions mineures : Sélectionnez Enable auto minor version upgrade (Activer la mise à niveau automatique des versions mineures) pour activer votre instance de base de données de sorte à recevoir automatiquement les mises à niveau de la version mineure préférée du moteur de base de données lorsqu'elles sont disponibles. Amazon RDS effectue les mises à niveau automatiques des versions mineures dans la fenêtre de maintenance. L'option Mise à niveau automatique de versions mineures ne s'applique qu'aux mises à niveau vers les versions mineures du moteur MySQL pour votre instance de base de données MariaDB. Elle ne s'applique pas aux correctifs réguliers appliqués pour maintenir la stabilité du système.

6. Choisissez Migrer.

AWS CLI

Pour migrer les données à partir d'un instantané de base de données MySQL vers une instance de base de données MariaDB, utilisez la commande `restore-db-instance-from-db-snapshot` de l'AWS CLI avec les paramètres suivants :

- --db-instance-identifier – Nom de l'instance de base de données à créer à partir de l'instantané de base de données.
- --db-snapshot-identifier – Identificateur de l'instantané de base de données à partir duquel restaurer.
- --engine – Moteur de base de données à utiliser pour la nouvelle instance.

Example

Pour Linux, macOS ou Unix :

```
aws rds restore-db-instance-from-db-snapshot \
    --db-instance-identifier newmariadbinstance \
    --db-snapshot-identifier mysqlsnapshot \
    --engine mariadb
```

Pour Windows :

```
aws rds restore-db-instance-from-db-snapshot \
```

```
    --db-instance-identifier newmariadbinstance ^
    --db-snapshot-identifier mysqlsnapshot ^
    --engine mariadb
```

API

Pour migrer les données à partir d'un instantané de base de données MySQL vers une instance de base de données MariaDB, appelez l'opération d'API Amazon RDS `RestoreDBInstanceFromDBSnapshot`.

Example

```
https://rds.us-west-2.amazonaws.com/
   ?Action=RestoreDBInstanceFromDBSnapshot
   &DBInstanceIdentifier= newmariadbinstance
   &DBSnapshotIdentifier= mysqlsnapshot
   &Engine= mariadb
   &SignatureMethod=HmacSHA256
   &SignatureVersion=4
   &Version=2013-09-09
   &X-Amz-Algorithm=AWS4-HMAC-SHA256
   &X-Amz-Credential=AKIADQKE4SARGYLE/20140428/us-west-2/rds/aws4_request
   &X-Amz-Date=20140428T232655Z
   &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
   &X-Amz-Signature=78ac761e8c8f54a8c0727f4e67ad0a766fbb0024510b9aa34ea6d1f7df52fe92
```

Utilisation de la réplication MariaDB dans Amazon RDS

Vous utilisez généralement des réplicas en lecture pour configurer la réplication entre instances de base de données Amazon RDS. Pour obtenir des informations générales sur les réplicas en lecture, veuillez consulter Utilisation des réplicas en lecture (p. 275). Pour obtenir des informations spécifiques sur l'utilisation des réplicas en lecture dans Amazon RDS MariaDB, veuillez consulter Utilisation de réplicas en lecture MariaDB (p. 574).

Vous pouvez également configurer la réplication en fonction des coordonnées des journaux binaires pour une instance de base de données MariaDB. Pour les instances MariaDB, vous pouvez également configurer la réplication en fonction des ID de transaction globaux (GTID), qui fournissent une meilleure sécurité en cas d'incident. Pour plus d'informations, consultez Configuration d'une réplication basée sur GTID dans une instance de base de données MariaDB Amazon RDS (p. 577).

Les autres options de réplication disponibles avec Amazon RDS MariaDB sont les suivantes :

- Vous pouvez configurer la réplication entre une instance de base de données MariaDB Amazon RDS et une instance MySQL ou MariaDB externe à Amazon RDS. Pour plus d'informations sur la réplication de configuration avec une source externe, consultez Réplication avec une instance MySQL ou MariaDB s'exécutant à l'extérieur d'Amazon RDS (p. 863).
- Vous pouvez configurer la réplication de sorte à importer des bases de données d'une instance MySQL ou MariaDB extérieure à Amazon RDS, ou à exporter des bases de données vers de telles instances. Pour plus d'informations, consultez Importation de données vers une instance de base de données MySQL ou MariaDB Amazon RDS avec un temps réduit (p. 832) et Exportation de données à partir d'une instance DB MySQL grâce à la réplication (p. 869).

Pour chacune de ces options de réplication, vous pouvez utiliser la réplication basée sur les lignes, basée sur les instructions ou mixte. La réplication basée sur les lignes réplique uniquement les lignes modifiées à la suite d'une instruction SQL. La réplication basée sur les instructions réplique l'ensemble de l'instruction SQL. La réplication mixte utilise la réplication basée sur les instructions chaque fois que possible, mais bascule vers la réplication basée sur les lignes lorsque des instructions SQL présentant un risque pour la réplication basée sur les instructions sont exécutées. La réplication mixte est recommandée dans la plupart des cas. Le format de journalisation binaire de l'instance de base de données détermine si la réplication est basée sur les lignes, basée sur les instructions ou mixte. Pour plus d'informations sur la définition du format de journalisation binaire, consultez la section Format de journalisation binaire (p. 500).

Rubriques

- Utilisation de réplicas en lecture MariaDB (p. 574)
- Configuration d'une réplication basée sur GTID dans une instance de base de données MariaDB Amazon RDS (p. 577)

Utilisation de réplicas en lecture MariaDB

Cette section contient des informations spécifiques sur l'utilisation des réplicas en lecture dans Amazon RDS MariaDB. Pour obtenir des informations générales sur les réplicas en lecture et des instructions pour les utiliser, veuillez consulter Utilisation des réplicas en lecture (p. 275).

Rubriques

- Configuration de réplicas en lecture avec MariaDB (p. 574)
- Mises à jour de réplicas en lecture avec MariaDB (p. 575)
- Déploiements multi-AZ de réplicas en lecture avec MariaDB (p. 575)
- Surveillance des réplicas en lecture MariaDB (p. 575)
- Démarrage et arrêt de la réplication avec des réplicas en lecture MariaDB (p. 576)
- Résolution d'un problème de réplica en lecture MariaDB (p. 576)

Configuration de réplicas en lecture avec MariaDB

Avant qu'une instance de base de données MariaDB puisse servir de source de réplication, vous devez activer les sauvegardes automatiques sur l'instance de base de données source en affectant à la période de rétention des sauvegardes une valeur différente de 0. Cette exigence s'applique également à un réplica en lecture qui serait l'instance de base de données source d'un autre réplica en lecture.

Vous pouvez créer jusqu'à cinq réplicas en lecture à partir d'une seule instance de base de données. Pour que la réplication fonctionne de façon efficace, chaque réplica en lecture doit avoir la même quantité de ressources de calcul et de stockage que l'instance de base de données source. Si vous mettez à l'échelle l'instance de base de données source, faites-le également pour les réplicas en lecture.

Si un réplica en lecture exécute une version de MariaDB, vous pouvez la spécifier comme instance de base de données source pour un autre réplica en lecture. Par exemple, vous pouvez créer ReadReplica1 from MyDBInstance, puis ReadReplica2 à partir de ReadReplica1. Les mises à jour effectuées sur InstanceDB sont répliquées sur ReplicaEnLecture1 puis répliquées de ReplicaEnLecture1 vers ReplicaEnLecture2. Vous ne pouvez pas avoir plus de quatre instances impliquées dans une chaîne de réplication. Par exemple, vous pouvez créer ReadReplica1 à partir de MySourceDBInstance, ReadReplica2 à partir de ReadReplica1, puis ReadReplica3 à partir de ReadReplica2, mais vous ne pouvez pas créer ReadReplica4 à partir de ReadReplica3.

Si vous procédez à la promotion d'un réplica en lecture MariaDB qui réplique à son tour vers d'autres réplicas en lecture, ces réplicas en lecture restent actifs. Considérez un exemple dans lequel InstanceDB1

réplique vers InstanceDB2, et InstanceDB2 réplique vers InstanceDB3. Si vous promouvez InstanceDB2, la réplication d'InstanceDB1 vers InstanceDB2 n'intervient plus, mais InstanceDB2 continue à répliquer vers InstanceDB3.

Pour activer les sauvegardes automatiques sur un réplica en lecture pour Amazon RDS MariaDB, commencez par créer le réplica en lecture, puis modifiez le réplica en lecture pour activer les sauvegardes automatiques.

Vous pouvez exécuter plusieurs actions simultanées de création ou suppression de réplica en lecture faisant référence à la même instance de base de données source, tant que vous restez dans la limite des cinq réplicas en lecture pour l'instance source.

Mises à jour de réplicas en lecture avec MariaDB

Les réplicas en lecture sont conçus pour prendre en charge les requêtes de lecture, mais vous pouvez avoir besoin de mises à jour ponctuelles. A titre d'exemple, vous pouvez avoir besoin d'ajouter un index, pour accélérer les types spécifiques de requêtes accédant au réplica. Vous pouvez autoriser les mises à jour en affectant au paramètre `read_only` la valeur 0 dans le groupe de paramètres de base de données pour le réplica en lecture.

Déploiements multi-AZ de réplicas en lecture avec MariaDB

Vous pouvez créer un réplica en lecture à partir de déploiements d'instance de base de données mono-AZ ou multi-AZ. Vous utilisez des déploiements multi-AZ pour améliorer la durabilité et la disponibilité des données critiques, mais vous ne pouvez pas utiliser une instance secondaire multi-AZ pour servir les requêtes en lecture seule. À la place, vous pouvez créer des réplicas en lecture à partir d'instances de base de données multi-AZ à trafic élevé pour décharger les requêtes en lecture seule. Si l'instance source d'un déploiement multi-AZ bascule vers l'instance secondaire, tous les réplicas en lecture associés se mettent automatiquement à utiliser l'instance secondaire (désormais principale) comme source de réplication. Pour plus d'informations, consultez Haute disponibilité (multi-AZ) pour Amazon RDS (p. 43).

Vous pouvez désormais créer un réplica en lecture en tant qu'instance de base de données multi-AZ. Amazon RDS crée une instance de secours de votre réplica dans une autre zone de disponibilité pour la prise en charge du basculement pour le réplica. La création de votre réplica en lecture en tant qu'instance de base de données multi-AZ est indépendante du fait que la base de données source soit ou non une instance de base de données multi-AZ.

Surveillance des réplicas en lecture MariaDB

Pour les réplicas en lecture MariaDB, vous pouvez surveiller le retard de réplication dans Amazon CloudWatch en consultant la métrique Amazon RDS `ReplicaLag`. La métrique `ReplicaLag` contient la valeur du champ `Seconds_Behind_Master` de la commande `SHOW SLAVE STATUS`.

Les causes courantes du retard de réplication pour MariaDB sont les suivantes :

- Une indisponibilité du réseau.
- L'écriture dans des tables avec des index sur un réplica en lecture. Si le paramètre `read_only` n'a pas pour valeur 0 sur le réplica en lecture, il peut interrompre la réplication.
- Utilisation d'un moteur de stockage non transactionnel tel que MyISAM. La réplication est prise en charge uniquement pour le moteur de stockage InnoDB sur MariaDB 10.2 et versions ultérieures et pour le moteur de stockage XtraDB sur MariaDB 10.1 et versions antérieures.

Lorsque la métrique `ReplicaLag` atteint 0, le réplica a rattrapé l'instance de bases de données source. Si la métrique `ReplicaLag` retourne -1, la réplication n'est actuellement pas active. `ReplicaLag`= -1 est équivalent à `Seconds_Behind_Master` = `NULL`.

Démarrage et arrêt de la réplication avec des réplicas en lecture MariaDB

Vous pouvez arrêter et redémarrer le processus de réplication sur une instance de base de données Amazon RDS en appelant les procédures stockées système mysql.rds_stop_replication (p. 916) et mysql.rds_start_replication (p. 913). Vous pouvez procéder ainsi lors d'une réplication entre deux instances Amazon RDS pour des opérations de longue durée, telles que la création d'un grand index. Vous devez également arrêter et démarrer la réplication lors de l'importation ou de l'exportation de bases de données. Pour de plus amples informations, veuillez consulter Importation de données vers une instance de base de données MySQL ou MariaDB Amazon RDS avec un temps réduit (p. 832) et Exportation de données à partir d'une instance DB MySQL grâce à la réplication (p. 869).

Si la réplication est arrêtée pendant plus de 30 jours consécutifs, manuellement ou en raison d'une erreur de réplication, Amazon RDS met fin à la réplication entre l'instance de base de données source et tous les réplicas en lecture. Cela permet d'éviter l'augmentation des besoins en stockage sur l'instance de bases de données source et d'importants délais de basculement. L'instance de base de données du réplica en lecture est toujours disponible. En revanche, la réplication ne peut pas être reprise, car les journaux binaires requis par le réplica en lecture sont supprimés de l'instance de base de données source une fois la réplication terminée. Vous pouvez créer un nouveau réplica en lecture pour l'instance de base de données source afin de rétablir la réplication.

Résolution d'un problème de réplica en lecture MariaDB

Les technologies de réplication pour MariaDB sont asynchrones. Par conséquent, des augmentations `BinLogDiskUsage` sur l'instance de base de données source et `ReplicaLag` sur le réplica en lecture sont prévisibles. Par exemple, un volume élevé d'opérations d'écriture sur l'instance de bases de données source peut se produire en parallèle. Tandis que les opérations d'écritures sur le réplica en lecture sont sérialisées à l'aide d'un seul thread d'E/S, ce qui peut conduire à un retard entre l'instance source et le réplica. Pour plus d'informations sur les réplicas en lecture seule dans la documentation MariaDB, consultez Présentation de la réplication.

Vous pouvez effectuer plusieurs opérations pour réduire le retard entre les mises à jour d'une instance de base de données source et les mises à jour suivantes appliquées au réplica en lecture, telles que les opérations suivantes :

- Dimensionnement d'un réplica en lecture pour qu'il ait une taille de stockage et une classe d'instance de base de données comparables à celles de l'instance de base de données source.
- Garantie que les réglages des paramètres dans les groupes de paramètres de base de données utilisés par l'instance de base de données source et le réplica en lecture sont compatibles. Pour obtenir plus d'informations et un exemple, reportez-vous à la présentation du paramètre `max_allowed_packet`, plus loin dans cette section.

Amazon RDS surveille l'état de réplication de vos réplicas en lecture et met à jour le champ `Replication State` de l'instance du réplica en lecture avec la valeur `Error` si la réplication s'arrête pour une raison quelconque. Par exemple, dans le cas de requêtes DML exécutées sur votre réplica en lecture qui sont en conflit avec les mises à jour effectuées sur l'instance de base de données source.

Vous pouvez passer en revue les détails de l'erreur associée et déclenchée par le moteur MariaDB, en consultant le champ `Replication Error`. Des événements indiquant l'état du réplica en lecture sont également générés, y compris RDS-EVENT-0045 (p. 474), RDS-EVENT-0046 (p. 474) et RDS-EVENT-0047 (p. 472). Pour plus d'informations sur les événements et l'abonnement aux événements, consultez Utilisation de la notification d'événement Amazon RDS (p. 467). Si un message d'erreur MariaDB est retourné, consultez l'erreur dans la documentation sur les messages d'erreur MariaDB.

Un problème courant susceptible de causer des erreurs de réplication se pose lorsque la valeur du paramètre `max_allowed_packet` d'un réplica en lecture est inférieure à celle du paramètre `max_allowed_packet` de l'instance de base de données source. Le paramètre `max_allowed_packet`

est un paramètre personnalisé que vous pouvez définir dans un groupe de paramètres DB utilisé pour spécifier la taille maximale du code DML qui peut être exécuté sur la base de données. Dans certains cas, la valeur du paramètre `max_allowed_packet` dans le groupe de paramètres de base de données associé à une instance de base de données source est inférieure à la valeur du paramètre `max_allowed_packet` dans le groupe de paramètres de base de données associé au réplica en lecture de la source. Le processus de réplication peut alors générer une erreur (Packet bigger than 'max_allowed_packet' bytes) et arrêter la réplication. Vous pouvez corriger cette erreur en indiquant à la source et au réplica en lecture d'utiliser des groupes de paramètres de base de données avec les mêmes valeurs du paramètre `max_allowed_packet`.

Voici d'autres situations courantes susceptibles de causer des erreurs de réplication :

- Écriture sur les tables d'un réplica en lecture. Si vous créez des index sur un réplica en lecture, le paramètre `read_only` doit être défini sur 0 pour créer les index. Si vous écrivez dans des tables sur le réplica en lecture, cela peut interrompre la réplication.
- Lorsqu'elles utilisent un moteur de stockage non transactionnel tel que MyISAM, les réplicas en lecture nécessitent un moteur de stockage transactionnel. La réplication est prise en charge uniquement pour le moteur de stockage InnoDB sur MariaDB 10.2 et versions ultérieures et pour le moteur de stockage XtraDB sur MariaDB 10.1 et versions antérieures.
- Utilisation de requêtes non déterministes non sécurisées telles que `SYSDATE()`. Pour de plus amples informations, veuillez consulter Détermination d'instructions sécurisées et non sécurisées dans la journalisation binaire.

Si vous décidez que vous pouvez ignorer une erreur en toute sécurité, vous pouvez suivre la procédure décrite dans la section Ignorer une erreur de réplication (p. 881). Dans le cas contraire, vous pouvez supprimer le réplica en lecture et créer une instance à l'aide du même identifiant d'instance de base de données de sorte que le point de terminaison reste le même que celui de votre ancien réplica en lecture. Si une erreur de réplication est corrigée, le champ `Replication State` prend la valeur replicating (réplication en cours).

Pour les instances de base de données MariaDB, dans certains cas, les réplicas en lecture ne peuvent pas être basculés vers l'instance secondaire si des événements de journaux binaires ne sont pas vidés au cours de la panne. Dans ces situations, vous devez supprimer et recréer manuellement les réplicas en lecture. Vous pouvez réduire la probabilité que cela se produise dans MySQL 5.5 en définissant les variables dynamiques suivantes : `sync_binlog=1`, `innodb_flush_log_at_trx_commit=1` et `innodb_support_xa=1`. Ces paramètres peuvent réduire les performances. Testez donc leur impact avant d'implémenter les modifications dans un environnement de production.

Configuration d'une réplication basée sur GTID dans une instance de base de données MariaDB Amazon RDS

Vous pouvez configurer une réplication basée sur GTID depuis une instance MariaDB externe, version 10.0.24 ou ultérieure, dans une instance de base de données MariaDB Amazon RDS. Veillez à suivre ces directives lorsque vous configurez une instance source externe et un réplica sur Amazon RDS :

- Surveillez les événements de basculement de l'instance de base de données MariaDB Amazon RDS qui constitue votre réplica. En cas de basculement, l'instance de base de données qui est votre réplica peut alors être recréée sur un nouvel hôte avec une autre adresse réseau. Pour plus d'informations sur la surveillance des événements de basculement, consultez Utilisation de la notification d'événement Amazon RDS (p. 467).
- Tenez à jour les journaux binaires sur votre instance source jusqu'à ce que vous ayez vérifié qu'ils ont été appliqués au réplica. Cela garantit que vous pouvez restaurer votre instance source en cas de défaillance.

- Activez les sauvegardes automatiques sur votre instance de base de données MariaDB sur Amazon RDS. L'activation des sauvegardes automatiques garantit que vous pouvez restaurer votre réplica sur un instant donné si vous devez resynchroniser votre maître et votre réplica. Pour plus d'informations sur les sauvegardes et la restauration à un instant dans le passé, consultez Sauvegarde et restauration d'une instance de base de données Amazon RDS (p. 317).

  Note

  Les autorisations requises pour démarrer la réplication sur une instance de base de données MariaDB Amazon RDS sont restreintes et ne sont pas disponibles pour votre utilisateur principal Amazon RDS. Pour cette raison, vous devez utiliser les commandes Amazon RDS mysql.rds_set_external_master_gtid (p. 589) et mysql.rds_start_replication (p. 913) pour configurer la réplication entre votre base de données active et votre base de données MariaDB Amazon RDS.

Pour commencer la réplication entre une instance source externe et une instance de base de données MariaDB sur Amazon RDS, appliquez la procédure suivante.

Pour démarrer la réplication

1. Passez l'instance de base de données source MariaDB en lecture seule :

```
mysql> FLUSH TABLES WITH READ LOCK;
mysql> SET GLOBAL read_only = ON;
```

2. Obtenez le GTID actuel de l'instance MariaDB externe. Vous pouvez faire cela en utilisant `mysql` ou l'éditeur de requête de votre choix pour exécuter `SELECT @@gtid_current_pos;`.

   Le GTID est formaté comme suit : `<domain-id>-<server-id>-<sequence-id>`. Un GTID type ressemble un peu à ceci : **`0-1234510749-1728`**. Pour plus d'informations sur les GTID et leurs composants, consultez ID de transaction globaux dans la documentation MariaDB.

3. Copiez la base de données de l'instance externe MariaDB vers l'instance de base de données MariaDB Amazon RDS à l'aide de `mysqldump`. Pour les bases de données très volumineuses, il se peut que vous vouliez utiliser la procédure décrite dans Importation de données vers une instance de base de données MySQL ou MariaDB Amazon RDS avec un temps réduit (p. 832).

   Note

   Veillez bien à ce qu'il n'y ait pas d'espace entre l'option `-p` et le mot de passe saisi.

   Pour Linux, macOS ou Unix :

```
mysqldump \
    --databases <database_name> \
    --single-transaction \
    --compress \
    --order-by-primary \
    -u <local_user> \
    -p<local_password> | mysql \
        --host=hostname \
        --port=3306 \
        -u <RDS_user_name> \
        -p <RDS_password>
```

   Pour Windows :

```
mysqldump ^
    --databases <database_name> ^
```

```
    --single-transaction ^
    --compress ^
    --order-by-primary \
    -u <local_user> \
    -p<local_password> | mysql ^
        --host=hostname ^
        --port=3306 ^
        -u <RDS_user_name> ^
        -p <RDS_password>
```

Utilisez les options `--host`, `--user (-u)`, `--port` et `-p` de la commande `mysql` pour spécifier le nom d'hôte, le nom d'utilisateur, le port et le mot de passe afin de vous connecter à votre instance de base de données MariaDB Amazon RDS. Le nom d'hôte est le nom DNS du point de terminaison de l'instance de base de données MariaDB Amazon RDS. Par exemple, `myinstance.123456789012.us-east-1.rds.amazonaws.com`. Vous pouvez trouver la valeur du point de terminaison dans les détails de l'instance dans Amazon RDS Management Console.

4. Transformez l'instance source MariaDB en instance accessible de nouveau en écriture :

```
mysql> SET GLOBAL read_only = OFF;
mysql> UNLOCK TABLES;
```

5. Dans Amazon RDS Management Console, ajoutez l'adresse IP du serveur qui héberge la base de données MariaDB externe au groupe de sécurité VPC de l'instance de base de données MariaDB Amazon RDS. Pour plus d'informations sur la modification d'un groupe de sécurité VPC, accédez à Groupes de sécurité pour votre VPC dans le Guide de l'utilisateur Amazon Virtual Private Cloud.

   L'adresse IP peut changer lorsque les conditions suivantes sont réunies :

   - Vous utilisez une adresse IP publique pour la communication entre l'instance source externe et l'instance de base de données.
   - L'instance source externe a été arrêtée et redémarrée.

   Si ces conditions sont réunies, vérifiez l'adresse IP avant de l'ajouter.

   Il se peut que vous ayez également besoin de configurer votre réseau local pour autoriser les connexions à partir de l'adresse IP de votre instance de base de données MariaDB Amazon RDS, de telle sorte qu'elle puisse communiquer avec votre instance MariaDB externe. Pour obtenir l'adresse IP de l'instance de base de données MariaDB Amazon RDS, utilisez la commande `host` :

```
host <RDS_MariaDB_DB_host_name>
```

   Le nom d'hôte est le nom DNS du point de terminaison de l'instance de base de données MariaDB Amazon RDS.

6. A l'aide du client de votre choix, connectez-vous à l'instance MariaDB externe et créez un utilisateur MariaDB à utiliser pour la réplication. Ce compte est utilisé exclusivement pour la réplication et doit être limité à votre domaine pour améliorer la sécurité. Voici un exemple :

```
CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY '<password>';
```

7. Pour l'instance MariaDB externe, attribuez les privilèges `REPLICATION CLIENT` et `REPLICATION SLAVE` à votre utilisateur de réplication. Par exemple, pour accorder les privilèges `REPLICATION CLIENT` et `REPLICATION SLAVE` sur toutes les bases de données à l'utilisateur « `repl_user` » de votre domaine, émettez la commande suivante :

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.*
   TO 'repl_user'@'mydomain.com'
```

```
   IDENTIFIED BY '<password>';
```

8. Transformez l'instance de base de données MariaDB Amazon RDS en réplica. Connectez-vous à l'instance de base de données MariaDB Amazon RDS comme utilisateur principal et identifiez la base de données MariaDB externe comme instance source de réplication à l'aide de la commande mysql.rds_set_external_master_gtid (p. 589). Utilisez le GTID que vous avez déterminé à l'étape 2. Voici un exemple :

```
CALL mysql.rds_set_external_master_gtid ('mymasterserver.mydomain.com', 3306,
    'repl_user', '<password>', '<GTID>', 0);
```

9. Sur l'instance de base de données MariaDB Amazon RDS, émettez la commande mysql.rds_start_replication (p. 913) pour démarrer la réplication :

```
CALL mysql.rds_start_replication;
```

Importation de données dans une instance de base de données MariaDB

Vous trouverez ci-après plus d'informations sur d'autres méthodes d'importation de vos données MariaDB dans une instance de base de données Amazon RDS exécutant MariaDB.

Pour procéder à une importation initiale de données dans une instance de base de données MariaDB, vous pouvez utiliser les procédures documentées dans Restauration d'une sauvegarde dans une instance de base de données MySQL Amazon RDS (p. 821), comme suit :

- Pour déplacer des données d'une instance de base de données MySQL Amazon RDS, une instance MariaDB ou MySQL dans Amazon Elastic Compute Cloud (Amazon EC2) dans le même VPC que votre instance de base de données MariaDB Amazon RDS, ou une petite instance sur site de MariaDB ou de MySQL, vous pouvez utiliser la procédure documentée dans Importation de données à partir d'une base de données MySQL ou MariaDB vers une instance de base de données MySQL ou MariaDB Amazon RDS (p. 830).
- Pour déplacer des données depuis une instance sur site de grande taille ou de production de MariaDB ou MySQL, vous pouvez utiliser la procédure documentée dans Importation de données vers une instance de base de données MySQL ou MariaDB Amazon RDS avec un temps réduit (p. 832).
- Pour déplacer des données d'une instance de MariaDB ou de MySQL qui est dans EC2 vers un VPC autre que votre instance de base de données MariaDB Amazon RDS, ou pour déplacer des données de toute source de données pouvant sortir des fichiers texte délimités, vous pouvez utiliser la procédure documentée dans Importation de données à partir d'une source vers une instance de base de données MySQL ou MariaDB (p. 846).

Vous pouvez également utiliser AWS Database Migration Service (AWS DMS) pour importer des données vers une instance de base de données Amazon RDS. AWS DMS peut migrer les bases de données sans interruption et, pour de nombreux moteurs de bases de données, poursuivre la réplication en cours jusqu'à ce que vous soyez prêt à basculer sur la base de données cible. Avec AWS DMS, vous pouvez migrer vers MariaDB à partir du même moteur de base de données ou d'un autre moteur de base de données. Si vous migrez à partir d'un moteur de base de données différent, vous pouvez utiliser l'AWS Schema Conversion Tool pour migrer des objets de schéma qui ne sont pas migrés par AWS DMS. Pour plus d'informations sur AWS DMS, consultez Qu'est-ce que AWS Database Migration Service

Vous pouvez configurer la réplication dans une instance de base de données MariaDB Amazon RDS à l'aide des identificateurs de transaction globaux (GTID) de MariaDB si l'instance externe est MariaDB 10.0.2 ou une version ultérieure, ou qui utilise des coordonnées des journaux binaires pour les

instances MySQL ou MariaDB sur les versions antérieures à 10.0.24. Veuillez noter que les GTID MariaDB sont implémentés différemment que les GTID MySQL, qui ne sont pas pris en charge par Amazon RDS.

Pour configurer la réplication dans une instance de base de données MariaDB, vous pouvez utiliser les procédures suivantes :

- Pour configurer la réplication dans une instance de base de données MariaDB depuis une instance MySQL externe ou une instance MariaDB exécutant une version antérieure à 10.0.24, vous pouvez utiliser la procédure documentée dans Réplication avec une instance MySQL ou MariaDB s'exécutant à l'extérieur d'Amazon RDS (p. 863).
- Pour configurer la réplication dans une instance de base de données MariaDB depuis une instance MySQL externe ou une instance MariaDB exécutant la version 10.0.24, ou une version ultérieure, vous pouvez utiliser la procédure documentée dans Configuration d'une réplication basée sur GTID dans une instance de base de données MariaDB Amazon RDS (p. 577).

> **Note**
>
> La base de données système mysql contient les informations d'authentification et d'autorisation requises pour se connecter à l'instance de base de données et accéder aux données. La suppression, la modification, le renommage ou la troncation de tables, de données ou d'autres contenus de la base de données mysql de votre instance de base de données peut entraîner des erreurs et rendre inaccessibles l'instance de base de données et vos données. Si cela se produit, l'instance de base de données peut être restaurée depuis un instantané en utilisant la commande `restore-db-instance-from-db-snapshot` de l'AWS CLI ou récupérée en utilisant les commandes `restore-db-instance-to-point-in-time`.

Options pour le moteur de base de données MariaDB

Cette annexe décrit les options, ou fonctions supplémentaires, disponibles pour les instances Amazon RDS exécutant le moteur de base de données MariaDB. Pour activer ces options, vous les ajoutez à un groupe d'options personnalisé, puis associer ce dernier à votre instance de base de données. Pour plus d'informations sur l'utilisation de groupes d'options, consultez Utilisation de groupes d'options (p. 209).

Amazon RDS prend en charge les options suivantes pour MariaDB :

ID d'option	Versions du moteur
`MARIADB_AUDIT_PLUGIN`	MariaDB 10.0.24 et version ultérieure

Prise en charge du plug-in d'audit MariaDB

Amazon RDS prend en charge l'utilisation du plug-in d'audit MariaDB sur les instances de base de données MariaDB. Le plug-in d'audit MariaDB enregistre l'activité de la base de données, telle que les utilisateurs qui se connectent à la base de données, les requêtes exécutées sur la base de données et plus encore. L'enregistrement de l'activité de la base de données est stocké dans un fichier journal.

Paramètres de l'option du plug-in d'audit

Amazon RDS prend en charge les paramètres suivants pour l'option de plug-in d'audit MariaDB.

Paramètre d'option	Valeurs valides	Valeur par défaut	Description
SERVER_AUDIT_FILE_PATH	/rdsdbdata/log/audit/	/rdsdbdata/log/audit/	Emplacement du fichier journal. Le fichier journal contient l'enregistrement de l'activité spécifiée dans SERVER_AUDIT_EVENTS. Pour plus d'informations, consultez Liste et affichage des fichiers journaux de base de données (p. 491) et Fichiers journaux de base de données MariaDB (p. 494).
SERVER_AUDIT_FILE_ROTATE_SIZE	1–1 000 000 000	1 000 000	Taille en octets qui, lorsqu'elle est atteinte, entraîne la rotation du fichier. Pour plus d'informations, consultez Taille des fichiers journaux (p. 499).
SERVER_AUDIT_FILE_ROTATIONS	0–100	9	Nombre de rotations de journaux à enregistrer. Pour plus d'informations, consultez Taille des fichiers journaux (p. 499) et Téléchargement d'un fichier journal de base de données (p. 491).
SERVER_AUDIT_EVENTS	CONNECT, QUERY, TABLE, QUERY_DDL, QUERY_DML, QUERY_DCL	CONNECT, QUERY	Types d'activités à enregistrer dans le journal. L'installation du plug-in d'audit MariaDB est elle-même enregistrée. • CONNECT : Permet d'enregistrer les connexions à la base de données, réussies ou non, et les déconnexions de la base de données. • QUERY : Permet d'enregistrer le texte de toutes les requêtes exécutées sur la base de données. • TABLE : Permet d'enregistrer les tables affectées par des requêtes lorsque des requêtes sont exécutées sur la base de données. • QUERY_DDL : semblable à l'événement QUERY, mais renvoie uniquement les requêtes en langage de définition de données (DDL) (CREATE, ALTER, etc.). • QUERY_DML : semblable à l'événement QUERY, mais renvoie uniquement les requêtes en langage de manipulation de données (DML) (INSERT, UPDATE, SELECT, etc.). • QUERY_DCL : semblable à l'événement QUERY, mais renvoie uniquement les requêtes en langage de contrôle de données (DCL) (GRANT, REVOKE, etc.).
SERVER_AUDIT_INCL_USERS	Plusieurs valeurs séparées par des virgules	Aucune	Incluez uniquement l'activité des utilisateurs spécifiés. Par défaut, l'activité est enregistrée pour tous les utilisateurs. Si un utilisateur est spécifié dans SERVER_AUDIT_EXCL_USERS et SERVER_AUDIT_INCL_USERS, l'activité est alors enregistrée pour l'utilisateur.
SERVER_AUDIT_EXCL_USERS	Plusieurs valeurs séparées par des virgules	Aucune	Excluez l'activité des utilisateurs spécifiés. Par défaut, l'activité est enregistrée pour tous les utilisateurs. Si un utilisateur est spécifié dans SERVER_AUDIT_EXCL_USERS et

Paramètre d'option	Valeurs valides	Valeur par défaut	Description
			`SERVER_AUDIT_INCL_USERS`, l'activité est alors enregistrée pour l'utilisateur. L'utilisateur `rdsadmin` interroge la base de données par seconde pour vérifier l'intégrité de la base de données. En fonction de vos autres paramètres, cette activité peut éventuellement provoquer un accroissement considérable et rapide de la taille de votre fichier journal. Si vous n'avez pas besoin d'enregistrer cette activité, ajoutez l'utilisateur `rdsadmin` à la liste `SERVER_AUDIT_EXCL_USERS`. Note L'activité `CONNECT` est toujours enregistrée pour tous les utilisateurs, même si l'utilisateur est spécifié pour ce paramètre d'option.
`SERVER_AUDIT_LOGGING`	`ON`	`ON`	La journalisation est active. La seule valeur valide est `ON`. Amazon RDS ne prend pas en charge la désactivation de la journalisation. Si vous souhaitez désactiver la journalisation, supprimez le plug-in d'audit MariaDB. Pour plus d'informations, consultez Suppression du plug-in d'audit MariaDB (p. 584).
`SERVER_AUDIT_QUERY_LIMIT`	0–2147483647	1024	Limite de longueur de la chaîne de requête dans un enregistrement.

Ajout du plug-in d'audit MariaDB

Le processus général pour ajouter le plug-in d'audit MariaDB à une instance de base de données est le suivant :

1. Créer un groupe d'options ou copier ou modifier un groupe existant.
2. Ajouter l'option au groupe d'options.
3. Associer un groupe d'options à une instance de base de données.

Une fois que vous ajoutez le plug-in d'audit MariaDB, vous n'avez pas besoin de redémarrer votre instance de base de données. Dès que le groupe d'options est actif, l'audit commence immédiatement.

Pour ajouter le plug-in d'audit MariaDB

1. Déterminez le groupe d'options que vous voulez utiliser. Vous pouvez créer un groupe d'options ou utiliser un groupe d'options existant. Si vous souhaitez utiliser un groupe d'options existant, passez à l'étape suivante. Sinon, créez un groupe d'options de base de données personnalisé. Choisissez mariadb pour Moteur, puis 10.0 ou la version ultérieure pour Version majeure du moteur. Pour plus d'informations, consultez Création d'un groupe d'options (p. 212).
2. Ajoutez l'option MARIADB_AUDIT_PLUGIN pour le groupe d'options et configurez les paramètres de l'option. Pour plus d'informations sur l'ajout d'options, consultez Ajout d'une option à un groupe

d'options (p. 214). Pour plus d'informations sur chaque paramètre, consultez Paramètres de l'option du plug-in d'audit (p. 581).

3. Appliquez le groupe d'options à une instance de base de données nouvelle ou existante.
   - Pour une nouvelle instance de base de données, vous appliquez le groupe d'options lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).
   - Pour une instance de base de données existante, vous appliquez le groupe d'options en modifiant l'instance de base de données et en attachant le nouveau groupe d'options. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Affichage et téléchargement du journal du plug-in d'audit MariaDB

Une fois que vous activez le plug-in d'audit MariaDB, vous accéder aux résultats dans les fichiers journaux de la même manière que tous les autres fichiers journaux texte. Les fichiers journaux d'audit se trouvent dans `/rdsdbdata/log/audit/`. Pour plus d'informations sur l'affichage du fichier journal dans la console, consultez Liste et affichage des fichiers journaux de base de données (p. 491). Pour plus d'informations sur le téléchargement du fichier journal, consultez Téléchargement d'un fichier journal de base de données (p. 491).

Modification des paramètres de plug-in d'audit MariaDB

Une fois que vous activez le plug-in d'audit MariaDB, vous pouvez modifier ses paramètres. Pour plus d'informations sur la modification des paramètres d'options, consultez Modification d'un paramètre d'option (p. 219). Pour plus d'informations sur chaque paramètre, consultez Paramètres de l'option du plug-in d'audit (p. 581).

Suppression du plug-in d'audit MariaDB

Amazon RDS ne prend pas en charge la désactivation de la journalisation du plug-in d'audit MariaDB. Toutefois, vous pouvez supprimer le plug-in dans une instance de base de données. Lorsque vous supprimez le plug-in d'audit MariaDB, l'instance de base de données est automatiquement redémarrée pour cesser l'audit.

Pour supprimer le plug-in d'audit MariaDB d'une instance de base de données, effectuez l'une des actions suivantes :

- Supprimez l'option de plug-in d'audit MariaDB du groupe d'options auquel elle appartient. Ce changement affecte toutes les instances de bases de données qui utilisent le groupe d'options. Pour de plus amples informations, veuillez consulter Suppression d'une option d'un groupe d'options (p. 222)
- Modifiez l'instance de base de données et spécifiez un groupe d'options différent qui n'inclut pas le plug-in. Ce changement affecte une seule instance de base de données. Vous pouvez spécifier le groupe d'options (vide) par défaut, ou un groupe d'options personnalisées différent. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Paramètres pour MariaDB

Par défaut, une instance de base de données MariaDB utilise un groupe de paramètres DB qui est spécifique à une base de données MariaDB. Ce groupe de paramètres contient certains, mais pas la totalité, des paramètres du groupe de paramètres de base de données Amazon RDS du moteur de base de données MySQL. Il contient également un certain nombre de nouveaux paramètres propres à MariaDB. Pour de plus amples informations sur l'utilisation des groupes de paramètres et sur la définition des paramètres, veuillez consulter Utilisation de groupes de paramètres de base de données (p. 225).

Les paramètres MySQL suivants ne sont pas disponibles dans les groupes de paramètres DB spécifiques à MariaDB :

- 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

Pour de plus amples informations sur les paramètres MySQL, veuillez consulter la documentation MySQL.

Les groupes de paramètres DB spécifiques à MariaDB contiennent également les paramètres modifiables suivants qui sont applicables à MariaDB uniquement. Les plages acceptables pour tous les paramètres modifiables sont les mêmes que celles spécifiées dans la documentation MariaDB, sauf indication contraire. Les paramètres MariaDB Amazon RDS sont définis sur les valeurs par défaut du moteur de stockage que vous avez sélectionné.

- aria_block_size
- aria_checkpoint_interval
- aria_checkpoint_log_activity
- aria_force_start_after_recovery_failures
- aria_group_commit
- aria_group_commit_interval
- aria_log_dir_path
- aria_log_file_size
- aria_log_purge_type
- aria_max_sort_file_size
- aria_page_checksum
- aria_pagecache_age_threshold
- aria_pagecache_division_limit
- aria_recover

  Amazon RDS MariaDB prend en charge les valeurs de NORMAL, OFF et QUICK, mais pas FORCE ou BACKUP.
- aria_repair_threads
- aria_sort_buffer_size
- aria_stats_method
- aria_sync_log_dir
- binlog_annotate_row_events
- binlog_commit_wait_count
- binlog_commit_wait_usec
- binlog_row_image (MariaDB version 10.1 et ultérieure)
- deadlock_search_depth_long
- deadlock_search_depth_short
- deadlock_timeout_long
- deadlock_timeout_short
- explicit_defaults_for_timestamp (MariaDB version 10.1 et ultérieure)
- extra_max_connections
- extra_port

- commentaire
- feedback_send_retry_wait
- feedback_send_timeout
- feedback_url
- feedback_user_info
- gtid_domain_id
- gtid_strict_mode
- histogram_size
- histogram_type
- innodb_adaptive_hash_index_partitions
- innodb_background_scrub_data_check_interval (MariaDB version 10.1 et ultérieure)
- innodb_background_scrub_data_compressed (MariaDB version 10.1 et ultérieure)
- innodb_background_scrub_data_interval (MariaDB version 10.1 et ultérieure)
- innodb_background_scrub_data_uncompressed (MariaDB version 10.1 et ultérieure)
- innodb_buf_dump_status_frequency (MariaDB version 10.1 et ultérieure)
- innodb_buffer_pool_populate
- innodb_cleaner_lsn_age_factor
- innodb_compression_algorithm (MariaDB version 10.1 et ultérieure)
- innodb_corrupt_table_action
- innodb_defragment (MariaDB version 10.1 et ultérieure)
- innodb_defragment_fill_factor (MariaDB version 10.1 et ultérieure)
- innodb_defragment_fill_factor_n_recs (MariaDB version 10.1 et ultérieure)
- innodb_defragment_frequency (MariaDB version 10.1 et ultérieure)
- innodb_defragment_n_pages (MariaDB version 10.1 et ultérieure)
- innodb_defragment_stats_accuracy (MariaDB version 10.1 et ultérieure)
- innodb_empty_free_List_algorithm
- innodb_fake_changes
- innodb_fatal_semaphore_wait_threshold (MariaDB version 10.1 et ultérieure)
- innodb_foreground_preflush
- innodb_idle_flush_pct (MariaDB version 10.1 et ultérieure)
- innodb_immediate_scrub_data_uncompressed (MariaDB version 10.1 et ultérieure)
- innodb_instrument_semaphores (MariaDB version 10.1 et ultérieure)
- innodb_locking_fake_changes
- innodb_log_arch_dir
- innodb_log_arch_expire_sec
- innodb_log_archive
- innodb_log_block_size
- innodb_log_checksum_algorithm
- innodb_max_bitmap_file_size
- innodb_max_changed_pages
- innodb_prefix_index_cluster_optimization (MariaDB version 10.1 et ultérieure)
- innodb_sched_priority_cleaner
- innodb_scrub_log (MariaDB version 10.1 et ultérieure)
- innodb_scrub_log_speed (MariaDB version 10.1 et ultérieure)
- innodb_show_locks_held

- innodb_show_verbose_locks
- innodb_simulate_comp_failures
- innodb_stats_modified_counter
- innodb_stats_traditional
- innodb_use_atomic_writes
- innodb_use_fallocate
- innodb_use_global_flush_log_at_trx_commit
- innodb_use_stacktrace
- innodb_use_trim (MariaDB version 10.1 et ultérieure)
- join_buffer_space_limit
- join_cache_level
- key_cache_file_hash_size
- key_cache_segments
- max_digest_length (MariaDB version 10.1 et ultérieure)
- max_statement_time (MariaDB version 10.1 et ultérieure)
- mysql56_temporal_format (MariaDB version 10.1 et ultérieure)
- progress_report_time
- query_cache_strip_comments
- replicate_annotate_row_events
- replicate_do_db
- replicate_do_table
- replicate_events_marked_for_skip
- replicate_ignore_db
- replicate_ignore_table
- replicate_wild_ignore_table
- slave_domain_parallel_threads
- slave_parallel_max_queued
- slave_parallel_mode (MariaDB version 10.1 et ultérieure)
- slave_parallel_threads
- slave_run_triggers_for_rbr (MariaDB version 10.1 et ultérieure)
- sql_error_log_filename
- sql_error_log_rate
- sql_error_log_rotate
- sql_error_log_rotations
- sql_error_log_size_limit
- thread_handling
- thread_pool_idle_timeout
- thread_pool_max_threads
- thread_pool_min_threads
- thread_pool_oversubscribe
- thread_pool_size
- thread_pool_stall_limit
- transaction_write_set_extraction
- use_stat_tables
- userstat

Pour plus d'informations sur les paramètres MariaDB, consultez la documentation MariaDB.

Référence MariaDB sur SQL Amazon RDS

Cette annexe décrit les procédures stockées système disponibles pour les instances Amazon RDS exécutant le moteur de base de données MariaDB.

Vous pouvez utiliser les procédures stockées système disponibles pour les instances de base de données MySQL Amazon RDS pour les instances de base de données MariaDB également. Ces procédures stockées sont documentées dans Référence SQL de MySQL sur Amazon RDS (p. 899). Les instances de base de données MariaDB prennent en charge toutes les procédures stockées, à l'exception de `mysql.rds_set_source_delay`.

En outre, les procédures stockées système suivantes sont prises en charge uniquement pour les instances de base de données Amazon RDS exécutant MariaDB :

- mysql.rds_set_external_master_gtid (p. 589)
- mysql.rds_kill_query_id (p. 591)

mysql.rds_set_external_master_gtid

Configure la réplication basée sur GTID d'une instance MariaDB s'exécutant à l'extérieur de Amazon RDS vers une instance de base de données MariaDB Amazon RDS. Cette procédure stockée est prise en charge uniquement lorsque l'instance MariaDB externe est à la version 10.0.24 ou supérieure. Lors de la configuration d'une réplication où une ou les deux instances ne prennent pas en charge les identificateurs de transaction globaux (GTID) MariaDB, utilisez mysql.rds_set_external_master (p. 901).

L'utilisation de GTID pour la réplication fournit des fonctions de sécurité en cas d'incident non proposées par une réplication de journal binaire. Nous la recommandons donc dans les situations où les instances de réplication assurent une prise en charge.

Syntaxe

```
CALL mysql.rds_set_external_master_gtid(
  host_name
  , host_port
  , replication_user_name
  , replication_user_password
  , gtid
  , ssl_encryption
);
```

Paramètres

host_name

String. Nom d'hôte ou adresse IP de l'instance MariaDB s'exécutant à l'extérieur de Amazon RDS et qui deviendra l'instance source.

host_port

Entier : Port utilisé par l'instance MariaDB s'exécutant à l'extérieur de Amazon RDS pour une configuration comme instance source. Si votre configuration réseau inclut une réplication de port SSH qui convertit le numéro de port, spécifiez le numéro de port qui est exposé par SSH.

replication_user_name

String. L'ID d'un utilisateur avec les autorisations `REPLICATION SLAVE` de l'instance de base de données MariaDB à configurer comme réplica en lecture.

replication_user_password

String. Mot de passe de l'ID utilisateur spécifié dans `replication_user_name`.

gtid

String. L'ID de transaction global sur l'instance source à partir de laquelle la réplication doit démarrer.

Vous pouvez utiliser `@@gtid_current_pos` pour obtenir le GTID actuel si l'instance source a été verrouillée pendant que vous configurez la réplication, afin que le journal binaire ne change pas entre les moments où vous obtenez le GTID et celui où la réplication démarre.

Sinon, si vous utilisez `mysqldump` version 10.0.13, ou ultérieure, pour remplir l'instance de réplica avant de démarrer la réplication, vous pouvez obtenir la position GTID dans le résultat en utilisant les options `--master-data` ou `--dump-slave`. Si vous n'utilisez pas `mysqldump` version 10.0.13 ou ultérieure, vous pouvez exécuter le `SHOW MASTER STATUS` ou les mêmes options `mysqldump` pour obtenir la position et le nom du fichier journal binaire, puis les convertir dans un GTID en exécutant `BINLOG_GTID_POS` sur l'instance MariaDB :

```
SELECT BINLOG_GTID_POS('<binary log file name>', <binary log file position>);
```

Pour plus d'informations sur l'implémentation MariaDB de GTID, accédez à ID de transaction global dans la documentation MariaDB.

ssl_encryption

Valeur indiquant si le chiffrement Secure Socket Layer (SSL) est utilisé sur la connexion de réplication. 1 spécifie d'utiliser le chiffrement SSL, 0 spécifie de ne pas utiliser le chiffrement. La valeur par défaut est 0.

Note

L'option `MASTER_SSL_VERIFY_SERVER_CERT` n'est pas prise en charge. Cette option est définie sur 0, ce qui signifie que la connexion est chiffrée, mais que les certificats ne sont pas vérifiés.

Notes d'utilisation

La procédure `mysql.rds_set_external_master_gtid` doit être exécutée par l'utilisateur maître. Elle doit être exécutée sur l'instance de base de données MariaDB que vous configurez comme le réplica d'une instance MariaDB s'exécutant à l'extérieur de Amazon RDS. Avant d'exécuter `mysql.rds_set_external_master_gtid`, vous devez avoir configuré l'instance de MariaDB s'exécutant en dehors de Amazon RDS comme instance source. Pour plus d'informations, consultez Importation de données dans une instance de base de données MariaDB (p. 580).

Warning

N'utilisez pas `mysql.rds_set_external_master_gtid` pour gérer la réplication entre deux instances de base de données Amazon RDS. N'utilisez la procédure que lors de la réplication avec une instance MariaDB s'exécutant à l'extérieur de RDS. Pour plus d'informations sur la gestion de la réplication entre les instances de base de données Amazon RDS, consultez Utilisation des réplicas en lecture (p. 275).

Après avoir appelé `mysql.rds_set_external_master_gtid` pour configurer une instance de base de données Amazon RDS comme réplica en lecture, vous pouvez appeler

mysql.rds_start_replication (p. 913) sur le réplica pour démarrer le processus de réplication. Vous pouvez appeler mysql.rds_reset_external_master (p. 909) pour supprimer la configuration du réplica en lecture.

Quand la procédure `mysql.rds_set_external_master_gtid` est appelée, Amazon RDS enregistre l'heure, l'utilisateur et une action de « set master » dans les tables `mysql.rds_history` et `mysql.rds_replication_status`.

Exemples

Lorsqu'il est exécuté sur une instance de base de données MariaDB, l'exemple suivant la configure comme le réplica d'une instance de MariaDB s'exécutant à l'extérieur de Amazon RDS.

```
call mysql.rds_set_external_master_gtid
 ('Sourcedb.some.com',3306,'ReplicationUser','SomePassW0rd','0-123-456',0);
```

mysql.rds_kill_query_id

Termine une requête s'exécutant sur le serveur MariaDB.

Syntaxe

```
CALL mysql.rds_kill_query_id(queryID);
```

Paramètres

queryID

Entier : L'identité de la requête à terminer.

Notes d'utilisation

Pour arrêter une requête s'exécutant sur le serveur MariaDB, utilisez la procédure `mysql.rds_kill_query_id` et transmettez-lui l'ID de cette requête. Pour obtenir l'ID de requête, interrogez Information Schema PROCESSLIST Table de MariaDB, comme indiqué ci-après :

```
SELECT USER, HOST, COMMAND, TIME, STATE, INFO, QUERY_ID FROM
                INFORMATION_SCHEMA.PROCESSLIST WHERE USER = '<user name>';
```

La connexion au serveur MariaDB est conservée.

Voir aussi

- mysql.rds_kill (p. 923)
- mysql.rds_kill_query (p. 924)

Exemples

L'exemple suivant termine une requête avec un ID de requête 230040 :

```
call mysql.rds_kill_query_id(230040);
```

Microsoft SQL Server sur Amazon RDS

Amazon RDS prend en charge les instances de bases de données exécutant plusieurs versions et éditions de Microsoft SQL Server. La version prise en charge la plus récente de chaque version majeure est indiquée ci-dessous. Pour obtenir la liste complètes des versions, éditions et versions de moteur RDS prises en charge, consultez Versions de Microsoft SQL Server sur Amazon RDS (p. 600).

- SQL Server 2019 CU5 15.00.4043.16, publié par KB4552255 le 22 juin 2020.
- SQL Server 2017 CU20 14.00.3294.2, publié par KB4541283 le 16 juin 2020.
- SQL Server 2016 SP2 CU13 13.00.5820.21, publié par KB4549825 le 16 juin 2020.
- SQL Server 2014 SP3 CU4 12.00.6329.1, publié sous la référence KB4500181 le 29 juillet 2019.
- SQL Server 2012 SP4 GDR 11.0.7493.4, publié sous la référence KB4532098 le 11 février 2020.
- SQL Server 2008 : il n'est plus possible d'allouer de nouvelles instances dans aucune région. Amazon RDS migre activement les instances existantes à partir de cette version.

Pour plus d'informations sur les licences SQL Server;, consultez Gestion des licences Microsoft SQL Server sur Amazon RDS (p. 617). Pour plus d'informations sur les builds SQL Server, consultez l'article du support Microsoft sur les dernières builds SQL Server.

Avec Amazon RDS, vous pouvez créer des instances de bases de données et des Snapshots DB, des restaurations à un moment donné, ainsi que des sauvegardes automatiques ou manuelles. Les instances de bases de données exécutant SQL Server peuvent être utilisées dans un VPC. Vous pouvez également utiliser Secure Sockets Layer (SSL) pour vous connecter à une instance de base de données exécutant SQL Server et vous servir du chiffrement transparent des données (TDE) pour chiffrer les données au repos. Amazon RDS prend actuellement en charge les déploiements multi-AZ pour SQL Server utilisant la mise en miroir de bases de données SQL Server (DBM) ou les groupes de disponibilité (AG) Always On comme solution de basculement à haute disponibilité.

Pour offrir une expérience de service géré, Amazon RDS ne fournit pas l'accès par l'interpréteur de commandes aux instances de base de données. Il restreint l'accès à certaines procédures système et tables qui requièrent des privilèges avancés. Amazon RDS prend en charge l'accès aux bases de données sur une instance de base de données à l'aide de toute application cliente SQL standard, telle que Microsoft SQL Server Management Studio. Amazon RDS n'autorise pas l'accès direct des hôtes à une instance de base de données via Telnet, Secure Shell (SSH) ni une connexion Bureau à distance Windows. Lorsque vous créez une instance de base de données, le rôle db_owner est attribué à l'utilisateur principal pour toutes les bases de données utilisateur sur cette instance, et cet utilisateur dispose de toutes les autorisations au niveau de la base de données, sauf celles qui sont utilisées pour les sauvegardes. Amazon RDS gère les sauvegardes pour vous.

Avant de créer votre première instance de base de données, vous devez suivre la procédure décrite dans la section du présent guide relative à la configuration. Pour plus d'informations, consultez Configuration pour Amazon RDS (p. 62).

Tâches courantes de gestion pour Microsoft SQL Server sur Amazon RDS

Vous trouverez ci-dessous les tâches courantes de gestion que vous exécutez avec une instance de base de données Amazon RDS SQL Server, avec des liens vers la documentation appropriée relative à chaque tâche.

Type de tâche	Documentation
Classes d'instance, stockage et PIOPS Si vous créez une instance de base de données à des fins de production, vous devez comprendre comment les classes d'instance, les types de stockage et les IOPS provisionnées fonctionnent dans Amazon RDS.	Prise en charge de la classe d'instance de base de données pour Microsoft SQL Server (p. 597) Types de stockage Amazon RDS (p. 30)
Déploiements multi-AZ Une instance de base de données de production doit utiliser des déploiements multi-AZ. Les déploiements multi-AZ améliorent la disponibilité, la durabilité des données et la tolérance aux pannes pour les instances de bases de données. Les déploiements multi-AZ pour SQL Server sont implémentés à l'aide de la technologie de mise en miroir de bases de données (DBM) ou de la technologie de groupes de disponibilité (AG) native de SQL Server.	Haute disponibilité (multi-AZ) pour Amazon RDS (p. 43) Déploiements multi-AZ à l'aide de la mise en miroir de bases de données ou des groupes de disponibilité AlwaysOn Microsoft SQL Server (p. 606)
Amazon Virtual Private Cloud (VPC) Si votre compte AWS possède un VPC par défaut, votre instance de base de données est automatiquement créée dans le VPC par défaut. Si votre compte n'a pas de VPC par défaut et que vous voulez que l'instance de base de données soit dans un VPC, vous devez créer le VPC et les groupes de sous-réseaux avant de créer l'instance de base de données.	Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611) Utilisation d'une instance de base de données dans un VPC (p. 1620)
Groupes de sécurité Par défaut, les instances de bases de données sont créées avec un pare-feu qui empêche d'y accéder. Vous devez donc créer un groupe de sécurité avec les adresses IP correctes et la configuration réseau permettant d'accéder à l'instance de base de données. Le groupe de sécurité que vous créez dépend de la plateforme Amazon EC2 sur laquelle se trouve votre instance de base de données et du fait que vous accédiez ou non à votre instance de base de données depuis une instance Amazon EC2. En général, si votre instance de base de données est sur la plateforme EC2-Classic, vous devez créer un groupe de sécurité de base de données ; si votre instance de base de données est sur la plateforme EC2-VPC, vous devez créer un groupe de sécurité VPC.	Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611) Contrôle d'accès par groupe de sécurité (p. 1590)
Groupes de paramètres	Utilisation de groupes de paramètres de base de données (p. 225)

Type de tâche	Documentation
Si votre instance de base de données doit nécessiter des paramètres de base de données spécifiques, vous devez créer un groupe de paramètres avant de créer l'instance de base de données.	
Groupes d'options Si votre instance de base de données doit nécessiter des options de base de données spécifiques, vous devez créer un groupe d'options avant de créer l'instance de base de données.	Options pour le moteur de base de données Microsoft SQL Server (p. 699)
Connexion à votre instance de base de données Après avoir créé un groupe de sécurité et l'avoir associé à une instance de base de données, vous pouvez vous connecter à l'instance de base de données en utilisant une application cliente SQL standard quelconque telle que Microsoft SQL Server Management Studio.	Connexion à une instance de base de données exécutant le moteur de base de données Microsoft SQL Server (p. 618)
Sauvegarde et restauration Lorsque vous créez votre instance de base de données, vous pouvez la configurer pour effectuer des sauvegardes automatiques. Vous pouvez également sauvegarder et restaurer vos bases de données manuellement à l'aide des fichiers de sauvegarde complète (fichiers .bak).	Utilisation des sauvegardes (p. 317) Importation et exportation de bases de données SQL Server (p. 634)
Surveillance Vous pouvez surveiller votre instance de base de données SQL Server en utilisant les métriques CloudWatch Amazon RDS, les événements et la supervision améliorée.	Affichage des métriques d'instances de base de données (p. 384) Affichage d'événements Amazon RDS (p. 486)
Les fichiers journaux Vous pouvez accéder aux fichiers journaux de votre instance de base de données SQL Server.	Amazon RDS Fichiers journaux de base de données (p. 490) Fichiers journaux de base de données Microsoft SQL Server (p. 503)

L'utilisation d'instances de bases de données SQL Server implique également des tâches d'administration avancées. Pour de plus amples informations, veuillez consulter la documentation suivante :

- Tâches DBA courantes pour Microsoft SQL Server (p. 759).
- Utilisation de l'authentification Windows avec une instance de base de données d'instance de base de données (p. 676)
- Accès à la base de données tempdb (p. 760)

Limites propres aux instances de bases de données Microsoft SQL Server

L'implémentation Amazon RDS de Microsoft SQL Server sur une instance de base de données comporte certaines restrictions que vous devez connaître :

- Le nombre maximum de bases de données prises en charge sur une instance de base de données dépend du type de classe d'instance et du mode de disponibilité : Mono-AZ, mise en miroir de bases de données (DBM) multi-AZ ou groupes de disponibilité (AG) multi-AZ. Les bases de données système Microsoft SQL Server ne sont pas prises en compte dans cette limite.

  Le tableau suivant montre le nombre maximum de bases de données prises en charge pour chacun des types de classe d'instance et des modes de disponibilité. Utilisez ce tableau pour déterminer si vous pouvez passer d'un type de classe d'instance ou d'un mode de disponibilité à un autre. La modification de votre instance de base de données source échoue si celle-ci comporte plus de bases de données que ce qui est pris en charge par le type de classe d'instance ou le mode de disponibilité cible. Vous pouvez voir le statut de votre demande dans le panneau Événements.

Type de classe d'instance	Mono-AZ	Multi-AZ avec DBM	Multi-AZ avec AG AlwaysOn
db.*.micro to db.*.medium	30	S/O	S/O
db.*.large	30	30	30
db.*.xlarge vers db.*.16xlarge	100	50	75
db.*.24xlarge	100	50	100

  * représente les différents types de classes d'instances.

  Par exemple, supposons que votre instance de base de données s'exécute sur un type de classe d'instance db.*.16xlarge avec une seule zone de disponibilité (mono-AZ) et qu'elle comporte 76 bases de données. Vous modifiez l'instance de base de données à mettre à niveau pour quelle utilise des groupes de disponibilité (AG) AlwaysOn multi-AZ. Cette mise à niveau échoue, car votre instance de base de données contient plus de bases de données que ce que votre configuration cible peut prendre en charge. Par contre, si vous mettez à niveau votre type de classe d'instance vers db.*.24xlarge, la modification réussit.

  Si la mise à niveau échoue, des événements et des messages similaires à ce qui suit s'affichent :

  - Unable to modify database instance class. The instance has 76 databases, but after conversion it would only support 75. (Impossible de modifier la classe d'instance de base de données. L'instance comporte 76 bases de données, mais après la conversion, elle n'en prendrait en charge que 75).
  - Unable to convert the DB instance to Multi-AZ: The instance has 76 databases, but after conversion it would only support 75. (Impossible de convertir la classe d'instance de base de données en multi-AZ : L'instance comporte 76 bases de données, mais après la conversion, elle n'en prendrait en charge que 75).

  Si la restauration à un instant donné ou la restauration d'instantané échoue, des événements et des messages similaires à ce qui suit s'affichent :

  - Database instance put into incompatible-restore. The instance has 76 databases, but after conversion it would only support 75. (L'instance de base de données a été restaurée de façon incompatible. L'instance comporte 76 bases de données, mais après la conversion, elle n'en prendrait en charge que 75).
- Certains ports sont réservés à Amazon RDS et vous ne pouvez pas les utiliser lorsque vous créez une instance de base de données.
- Les connexions client à partir d'adresse IP dans la plage 169.254.0.0/16 ne sont pas autorisées. Il s'agit d'une plage d'adresses IP privées automatiques (APIPA, Automatic Private IP Addressing Range), qui est utilisée pour l'adressage de liens locaux.

- SQL Server Standard Edition n'utilisera qu'un sous-ensemble des processeurs disponibles si l'instance de base de données dispose de davantage de processeurs que les limites logicielles (24 cœurs, 4 sockets et 128 Go de RAM). Exemples : les classes d'instances db.m5.24xlarge et db.r5.24xlarge.
- Amazon RDS pour SQL Server ne prend pas en charge l'importation de données dans la base de données msdb.
- Vous ne pouvez pas renommer les bases de données sur une instance de base de données dans un déploiement multi-AZ SQL Server.
- La taille de stockage maximale pour les instances de bases de données SQL Server est la suivante :
  - Stockage à usage général (SSD) – 16 Tio pour toutes les éditions
  - Stockage sur volumes d'IOPS provisionnés – 16 Tio pour toutes les éditions
  - Stockage magnétique – 1 Tio pour toutes les éditions

  Si vous disposez d'un scénario exigeant un important volume de stockage, vous pouvez utiliser le partitionnement sur plusieurs instances de bases de données pour contourner la limite. Cette approche nécessite une logique de routage dépendant des données dans les applications qui se connectent au système partitionné. Vous pouvez utiliser une infrastructure de partitionnement existante ou écrire du code personnalisé pour activer le partitionnement. Si vous utilisez une infrastructure existante, elle ne peut installer aucun composant sur le même serveur que l'instance de base de données.
- La taille de stockage minimale pour les instances de bases de données SQL Server est la suivante :
  - Stockage à usage général (SSD) – 20 Gio pour les éditions Enterprise, Standard, Web et Express
  - Stockage sur volumes d'IOPS provisionnés – 20 Gio pour les éditions Enterprise et Standard, 100 Gio pour les éditions Web et Express
  - Stockage magnétique – 200 Gio pour les éditions Enterprise et Standard, 20 Gio pour les éditions Web et Express
- Amazon RDS ne prend pas en charge l'exécution de ces services sur le même serveur que votre instance de base de données RDS :
  - Data Quality Services
  - Master Data Services

  Pour utiliser ces fonctions, nous vous recommandons d'installer SQL Server sur une instance Amazon EC2 ou d'utiliser une instance SQL Server sur site. L'instance EC2 ou SQL Server tient alors lieu de serveur Master Data Services pour votre instance de base de données SQL Server sur Amazon RDS. Vous pouvez installer SQL Server sur une instance Amazon EC2 avec stockage Amazon EBS, conformément aux stratégies de gestion des licences de Microsoft.
- Du fait de limitations dans Microsoft SQL Server, une restauration à un moment donné avant une exécution réussie de `DROP DATABASE` peut ne pas refléter l'état de cette base de données à ce moment précis. Par exemple, la base de données supprimée est généralement restaurée à l'état qui était le sien jusqu'à 5 minutes avant l'exécution de la commande `DROP DATABASE`. Ce type de restauration signifie que vous ne pouvez pas restaurer les transactions effectuées pendant ces quelques minutes sur votre base de données supprimée. Pour contourner ce problème, vous pouvez réémettre la commande `DROP DATABASE` après que l'opération de restauration est terminée. La suppression d'une base de données supprime les journaux de transaction pour cette base de données.
- Pour SQL Server, vous créez vos bases de données après avoir créé votre instance de base de données. Les noms de base de données suivent les règles de dénomination SQL Server habituelles, avec les différences suivantes :
  - Les noms de base de données ne peuvent pas commencer par `rdsadmin`.
  - Ils ne peuvent pas commencer ni se terminer par un espace ou une tabulation.
  - Ils ne peuvent contenir aucun caractère qui crée une nouvelle ligne.
  - Ils ne peuvent pas contenir de guillemet simple (`'`).

Prise en charge de la classe d'instance de base de données pour Microsoft SQL Server

Les capacités de calcul et de mémoire d'une instance de base de données sont déterminées par sa classe d'instance de base de données. La classe d'instance de bases de données dont vous avez besoin varie selon vos exigences en mémoire et en puissance de traitement. Pour de plus amples informations, veuillez consulter Classes d'instances de base de données (p. 6).

Voici la liste des classes d'instances de bases de données prises en charge pour Microsoft SQL Server à titre d'information. Pour consulter la liste actualisée, accédez à la console RDS : https://console.aws.amazon.com/rds/.

Edition SQL Server	Prise en charge 2019	Prise en charge 2017 et 2016	Prise en charge 2014 et 2012
Enterprise Edition	db.t3.xlarge–db.t3.2xlarge db.r5.xlarge–db.r5.24xlarge db.m5.xlarge–db.m5.24xlarge db.x1.16xlarge–db.x1.32xlarge db.x1e.xlarge–db.x1e.32xlarge db.z1d.xlarge–db.z1d.12xlarge	db.t3.xlarge–db.t3.2xlarge db.r3.xlarge–db.r3.8xlarge db.r4.xlarge–db.r4.16xlarge db.r5.xlarge–db.r5.24xlarge db.m4.xlarge–db.m4.16xlarge db.m5.xlarge–db.m5.24xlarge db.x1.16xlarge–db.x1.32xlarge db.x1e.xlarge–db.x1e.32xlarge db.z1d.xlarge–db.z1d.12xlarge	db.t3.xlarge–db.t3.2xlarge db.r3.xlarge–db.r3.8xlarge db.r4.xlarge–db.r4.8xlarge db.r5.xlarge–db.r5.24xlarge db.m4.xlarge–db.m4.10xlarge db.m5.xlarge–db.m5.24xlarge db.x1.16xlarge–db.x1.32xlarge
Standard Edition	db.t3.xlarge–db.t3.2xlarge db.r5.large–db.r5.24xlarge db.m5.large–db.m5.24xlarge db.x1.16xlarge–db.x1.32xlarge db.x1e.xlarge–db.x1e.32xlarge db.z1d.large–db.z1d.12xlarge	db.t3.xlarge–db.t3.2xlarge db.r4.large–db.r4.16xlarge db.r5.large–db.r5.24xlarge db.m4.large–db.m4.16xlarge db.m5.large–db.m5.24xlarge db.x1.16xlarge–db.x1.32xlarge db.x1e.xlarge–db.x1e.32xlarge db.z1d.large–db.z1d.12xlarge	db.t3.xlarge–db.t3.2xlarge db.r3.large–db.r3.8xlarge db.r4.large–db.r4.8xlarge db.r5.large–db.r5.24xlarge db.m3.medium–db.m3.2xlarge db.m4.large–db.m4.10xlarge db.m5.large–db.m5.24xlarge db.x1.16xlarge–db.x1.32xlarge
Web Edition	db.t3.small–db.t3.2xlarge db.r5.large–db.r5.4xlarge db.m5.large–db.m5.4xlarge db.z1d.large–db.z1d.3xlarge	db.t2.small–db.t2.medium db.t3.small–db.t3.2xlarge db.r4.large–db.r4.2xlarge db.r5.large–db.r5.4xlarge	db.t2.small–db.t2.medium db.t3.small–db.t3.2xlarge db.r3.large–db.r3.2xlarge db.r4.large–db.r4.2xlarge

Edition SQL Server	Prise en charge 2019	Prise en charge 2017 et 2016	Prise en charge 2014 et 2012
		db.m4.large–db.m4.4xlarge db.m5.large–db.m5.4xlarge db.z1d.large–db.z1d.3xlarge	db.r5.large–db.r5.4xlarge db.m3.medium–db.m3.2xlarge db.m4.large–db.m4.4xlarge db.m5.large–db.m5.4xlarge
Express Edition	db.t3.small–db.t3.xlarge	db.t2.micro–db.t2.medium db.t3.small–db.t3.xlarge	db.t2.micro–db.t2.medium db.t3.small–db.t3.xlarge

Sécurité de Microsoft SQL Server

Le moteur de base de données Microsoft SQL Server utilise une sécurité basée sur les rôles. Le nom utilisateur maître que vous utilisez lorsque vous créez une instance de base de données est un ID de connexion d'authentification SQL Server qui est un membre des rôles serveur fixes `processadmin`, `public` et `setupadmin`.

Tout utilisateur qui créé une base de données est affecté au rôle db_owner pour cette base de données et possède toutes les autorisations de niveau base de données, sauf celles utilisées pour les sauvegardes. Amazon RDS gère les sauvegardes à votre place.

Les rôles de niveau serveur suivants ne sont pas disponibles actuellement dans Amazon RDS :

- bulkadmin
- dbcreator
- diskadmin
- securityadmin
- serveradmin
- sysadmin

Les autorisations de niveau serveur suivantes ne sont pas disponibles sur les instances de bases de données SQL Server :

- ALTER ANY CREDENTIAL
- ALTER ANY EVENT NOTIFICATION
- ALTER ANY EVENT SESSION
- ALTER RESOURCES
- ALTER SETTINGS (vous pouvez utiliser les opérations d'API de groupe de paramètres de base de données pour modifier des paramètres. Pour de plus amples informations, veuillez consulter Utilisation de groupes de paramètres de base de données (p. 225))
- AUTHENTICATE SERVER
- CONTROL_SERVER
- CREATE DDL EVENT NOTIFICATION
- CREATE ENDPOINT
- CREATE TRACE EVENT NOTIFICATION

- EXTERNAL ACCESS ASSEMBLY
- SHUTDOWN (Vous pouvez utiliser l'option de redémarrage RDS à la place)
- UNSAFE ASSEMBLY
- ALTER ANY AVAILABILITY GROUP (SQL Server 2012 uniquement)
- CREATE ANY AVAILABILITY GROUP (SQL Server 2012 uniquement)

Prise en charge du programme de conformité pour les instances de bases de données Microsoft SQL Server

Les services AWS concernés par le programme de conformité ont été intégralement évalués par un auditeur tiers et donnent lieu à une certification, une attestation de conformité ou une autorisation d'opérer (ATO, Authorization to operate). Pour de plus amples informations, veuillez consulter Services AWS concernés par le programme de conformité.

Prise en charge de la loi HIPAA pour les instances de bases de données Microsoft SQL Server

Vous pouvez utiliser Amazon RDS pour les bases de données Microsoft SQL Server afin de développer des applications conformes à la loi HIPAA. Vous pouvez stocker les informations relatives à la santé, y compris les données de santé protégées (PHI, Protected Health Information), selon les termes d'un accord de partenariat (BAA, Business Associate Agreement) avec AWS. Pour de plus amples informations, veuillez consulter Conformité à la loi HIPAA.

Amazon RDS pour SQL Server prend en charge la loi HIPAA pour les versions et éditions suivantes :

- SQL Server 2017 Enterprise, Standard et Web Editions
- SQL Server 2016 Enterprise, Standard et Web Editions
- SQL Server 2014 Enterprise, Standard et Web Editions
- SQL Server 2012 Enterprise, Standard et Web Editions

Pour activer la prise en charge de la loi HIPAA sur votre instance de base de données, installez les trois composants suivants.

Composant	Détails
Audit	Pour configurer l'audit, définissez le paramètre `rds.sqlserver_audit` sur la valeur `fedramp_hipaa`. Si votre instance de base de données n'utilise pas déjà un groupe de paramètres de base de données personnalisé, vous devez créer un groupe de paramètres personnalisé et l'attacher à votre instance de base de données avant de pouvoir modifier le paramètre `rds.sqlserver_audit`. Pour de plus amples informations, veuillez consulter Utilisation de groupes de paramètres de base de données (p. 225).
Chiffrement de transport	Pour configurer le chiffrement de transport, forcez toutes les connexions à votre instance de base de données pour qu'elles utilisent le protocole SSL (Secure Sockets Layer). Pour de plus amples informations, veuillez consulter Forcer les connexions à votre instance de base de données pour utiliser SSL (p. 669).

Composant	Détails
Chiffrement au repos	Pour configurer le chiffrement au repos, vous disposez de deux options : 1. Si vous exécutez Enterprise Edition, vous pouvez choisir d'utiliser le chiffrement transparent des données (TDE, Transparent Data Encryption) pour obtenir le chiffrement au repos. Pour de plus amples informations, veuillez consulter Prise en charge de Transparent Data Encryption dans SQL Server (p. 704). 2. Vous pouvez configurer le chiffrement au repos à l'aide des clés de chiffrement AWS Key Management Service (AWS KMS). Pour de plus amples informations, veuillez consulter Chiffrement des ressources Amazon RDS (p. 1522).

Prise en charge SSL d'instances de bases de données Microsoft SQL Server

Vous pouvez utiliser SSL pour chiffrer les connexions entre vos applications et vos instances de bases de données Amazon RDS exécutant Microsoft SQL Server. Vous pouvez également forcer toutes les connexions à votre instance de base de données à utiliser SSL. Si vous forcez les connexions à utiliser SSL, cette opération s'exécute en toute transparence pour le client qui n'a rien à faire pour utiliser SSL.

SSL est pris en charge dans toutes les régions AWS et pour toutes les éditions SQL Server prises en charge. Pour plus d'informations, consultez Utilisation de SSL avec une instance DB Microsoft SQL Server (p. 669).

Versions de Microsoft SQL Server sur Amazon RDS

Vous pouvez spécifier n'importe quelle version de Microsoft SQL Server actuellement prise en charge lorsque vous créez une instance de base de données. Vous pouvez spécifier la version majeure de Microsoft SQL Server (par exemple, Microsoft SQL Server 14.00), puis toute version mineure prise en charge pour la version majeure spécifiée. Si aucune version n'est spécifiée, Amazon RDS utilise par défaut une version prise en charge, généralement la plus récente. Si une version majeure est spécifiée, mais qu'une version mineure ne l'est pas, Amazon RDS utilise par défaut une version récente de la version majeure que vous avez spécifiée.

Le tableau suivant indique les versions prises en charge pour toutes les éditions et toutes les régions AWS, sauf indication contraire. Vous pouvez également utiliser la commande AWS CLI `describe-db-engine-versions` pour afficher la liste des versions prises en charge, ainsi que les versions par défaut des instances de base de données nouvellement créées.

Versions SQL Server prises en charge dans RDS

Version majeure	Version mineure	API RDS **`EngineVersion`** et interface de ligne de commande **`engine-version`**
SQL Server 2019	15.00.4043.16 (CU5)	`15.00.4043.16.v1`
SQL Server 2017	14.00.3294.2 (CU20)	`14.00.3294.2.v1`
	14.00.3281.6 (CU19)	`14.00.3281.6.v1`
	14.00.3223.3 (CU16)	`14.00.3223.3.v1`

Version majeure	Version mineure	API RDS **`EngineVersion`** et interface de ligne de commande **`engine-version`**

	14.00.3192.2 (CU15 GDR)
	14.00.3049.1 (mise à jour du correctif CU13)
	14.00.3035.2 (CU9 GDR)
	14.00.3015.40 (CU3)
	14.00.1000.169 (RTM)
		`14.00.3192.2.v1`
		`14.00.3049.1.v1`
		`14.00.3035.2.v1`
		`14.00.3015.40.v1`
		`14.00.1000.169.v1`

SQL Server 2016	13.00.5820.21 (SP2 CU13)
	13.00.5598.27 (SP2 CU11)
	13.00.5426.0 (SP2 CU8)
	13.00.5366.0 (SP2)
	13.00.5292.0 (CU6)
	13.00.5216.0 (CU3)
	13.00.4522.0 (mise à jour de sécurité SP1 CU10)
	13.00.4466.4 (SP1 CU7)
	13.00.4451.0 (SP1 CU5)
	13.00.4422.0 (SP1 CU2)
	13.00.2164.0 (RTM CU2)
		`13.00.5820.21.v1`
		`13.00.5598.27.v1`
		`13.00.5426.0.v1`
		`13.00.5366.0.v1`
		`13.00.5292.0.v1`
		`13.00.5216.0.v1`
		`13.00.4522.0.v1`
		`13.00.4466.4.v1`
		`13.00.4451.0.v1`
		`13.00.4422.0.v1`
		`13.00.2164.0.v1`

SQL Server 2014	12.00.6329.1 (SP3 CU4)
	12.00.6293.0 (SP3 CU3)
	12.00.5571.0 (SP2 CU10)
	12.00.5546.0 (SP2 CU5)
	12.00.5000.0 (SP2)
		`12.00.6329.1.v1`
		`12.00.6293.0.v1`
		`12.00.5571.0.v1`
		`12.00.5546.0.v1`
		`12.00.5000.0.v1`

SQL Server 2012	11.00.7493.4 (SP4 GDR)
	11.00.7462.6 (SP4 GDR)
	11.00.6594.0 (SP3 CU8)
	11.00.6020.0 (SP3)
	11.00.5058.0 (SP2), sauf pour USA Est (Ohio), Canada (Centre) et Europe (Londres)
		`11.00.7493.4.v1`
		`11.00.7462.6.v1`
		`11.00.6594.0.v1`
		`11.00.6020.0.v1`
		`11.00.5058.0.v1`

Gestion des versions dans Amazon RDS

Amazon RDS comprend une gestion flexible des versions qui vous permet de contrôler quand et comment votre instance de base de données est corrigée ou mise à niveau. Cela vous permet d'effectuer les opérations suivantes pour votre moteur de base de données :

- Conserver la compatibilité avec les versions correctives du moteur de base de données.
- Tester les nouvelles versions correctives pour vérifier qu'elles fonctionnent avec votre application avant de les déployer en production.
- Planifier et effectuer des mises à niveau de version pour répondre à vos contrats de niveau de service et à vos exigences en termes de temps.

Application de correctifs de moteur Microsoft SQL Server dans Amazon RDS

Amazon RDS ajoute régulièrement des correctifs de base de données Microsoft SQL Server officiels à une version de moteur de base de données spécifique à Amazon RDS. Pour de plus amples informations sur les correctifs Microsoft SQL Server de chaque version de moteur de base de données, veuillez consulter Versions et fonctions prises en charge sur Amazon RDS.

Actuellement, vous devez effectuer manuellement toutes les mises à niveau de moteur sur votre instance de base de données. Pour plus d'informations, consultez Mise à niveau du moteur de base de données Microsoft SQL Server (p. 629).

Calendrier d'obsolescence pour les versions de moteur majeures de Microsoft SQL Server sur Amazon RDS

Le tableau suivant affiche le calendrier planifié de l'obsolescence des versions de moteur majeures de Microsoft SQL Server.

Date	Informations
12 juillet 2019	L'équipe Amazon RDS a rendu obsolète la prise en charge de Microsoft SQL Server 2008 I Microsoft SQL Server 2008 R2 sont migrées vers SQL Server 2012 (dernière version mineu Pour éviter une mise à niveau automatique depuis Microsoft SQL Server 2008 R2, vous po convient. Pour plus d'informations, consultez Mise à niveau d'une version du moteur d'une
25 avril 2019	Avant fin avril 2019, vous ne pourrez plus créer de nouvelles instances de base de donnée SQL Server 2008 R2.

Fonctionnalités de Microsoft SQL Server sur Amazon RDS

Les versions SQL Server prises en charge sur Amazon RDS incluent les fonctionnalités suivantes.

Fonctionnalités de Microsoft SQL Server 2019

SQL Server 2019 inclut un grand nombre de nouvelles fonctions, par exemple :

- Récupération accélérée de base de données (ADR) : réduction du temps de récupération après un redémarrage ou une restauration de transaction longue durée.
- Traitement intelligent des requêtes (IQP) :
  - Rétroaction d'octroi de mémoire en mode ligne : correction automatique des octrois excessifs entraînant un gaspillage de mémoire et une réduction de la concurrence.
  - Mode batch sur rowstore : permet l'exécution du mode batch pour les charges de travail d'analyse sans nécessiter d'index columnstore.
  - Compilation différée des variables de table : amélioration de la qualité du plan et des performances globales des requêtes faisant référence aux variables de table.
- Performances intelligentes :
  - Option d'index `OPTIMIZE_FOR_SEQUENTIAL_KEY` : amélioration du débit des insertions à forte concurrence dans les index.
  - Amélioration de l'évolutivité des points de contrôle indirects : aide les bases de données présentant des fortes charges de travail DML.
  - Mises à jour d'espace libre simultané (PFS) : permet la gestion en tant que verrou partagé plutôt qu'en tant que verrou exclusif.
- Surveillance des améliorations :
  - Type d'attente `WAIT_ON_SYNC_STATISTICS_REFRESH` : affiche le temps accumulé au niveau de l'instance consacré aux opérations d'actualisation des statistiques synchrones.
  - Configurations définies par base de données : inclure `LIGHTWEIGHT_QUERY_PROFILING` et `LAST_QUERY_PLAN_STATS`.
  - Fonctions de gestion dynamique (DMF) : inclure `sys.dm_exec_query_plan_stats` et `sys.dm_db_page_info`.
- Avertissements de troncature verbeux : le message d'erreur de troncation des données inclut par défaut les noms de table et de colonne et la valeur tronquée.
- Création d'index en ligne pouvant être interrompus : dans SQL Server 2017, seule la reconstruction d'index en ligne pouvant être interrompus est prise en charge.

Pour la liste complète des fonctions SQL Server 2019, veuillez consulter What's new in SQL Server 2019 (15.x) dans la documentation Microsoft.

Pour obtenir la liste des fonctions non prises en charge, consultez Fonctions non prises en charge et fonctions avec prise en charge limitée (p. 606).

Fonctionnalités de Microsoft SQL Server 2017

SQL Server 2017 inclut un grand nombre de nouvelles fonctions, par exemple :

- Traitement des requêtes adaptives
- Correction de plan automatique
- GraphDB
- Reconstructions d'index pouvant être interrompues

Pour la liste complète des fonctions SQL Server 2017, veuillez consulter What's new in SQL Server 2017 dans la documentation Microsoft.

Pour obtenir la liste des fonctions non prises en charge, consultez Fonctions non prises en charge et fonctions avec prise en charge limitée (p. 606).

Fonctionnalités de Microsoft SQL Server 2016

Amazon RDS prend en charge les fonctions suivantes de SQL Server 2016 :

- Toujours chiffré
- JSON
- Analytique opérationnelle
- Magasin de requêtes
- Tables temporelles

Pour la liste complète des fonctions SQL Server 2016, veuillez consulter What's new in SQL Server 2016 dans la documentation Microsoft.

Fonctionnalités de Microsoft SQL Server 2014

En plus des fonctions prises en charge de SQL Server 2012, Amazon RDS prend en charge le nouvel optimiseur de requête disponible dans SQL Server 2014, ainsi que la fonction de durabilité retardée.

Pour obtenir la liste des fonctions non prises en charge, consultez Fonctions non prises en charge et fonctions avec prise en charge limitée (p. 606).

SQL Server 2014 prend en charge tous les paramètres de SQL Server 2012 et utilise les mêmes valeurs par défaut. SQL Server 2014 inclut un nouveau paramètre, total de contrôle de sauvegarde par défaut. Pour de plus amples informations, veuillez consulter Comment activer l'option CHECKSUM si les utilitaires de sauvegarde n'exposent pas cette option dans la documentation de Microsoft.

Fonctionnalités de Microsoft SQL Server 2012

En plus des fonctions prises en charge de SQL Server 2008 R2, Amazon RDS prend en charge les fonctions SQL Server 2012 suivantes :

- Index columnstore (Enterprise Edition)
- Types de données Online Index Create, Rebuild and Drop for XML, varchar(max), nvarchar(max) et varbinary(max) (Enterprise Edition)
- Rôles serveur flexibles
- Service Broker est pris en charge, mais pas les points de terminaison Service Broker
- Bases de données partiellement contenues
- Séquences
- Transparent Data Encryption (Enterprise Edition uniquement)
- Instruction THROW
- Types spatiaux nouveaux et améliorés
- Support UTF-16
- Autorisation niveau serveur ALTER ANY SERVER ROLE

Pour plus d'informations sur SQL Server 2012, consultez Fonctions prises en charge par les éditions de SQL Server 2012 dans la documentation Microsoft.

Pour obtenir la liste des fonctions non prises en charge, consultez Fonctions non prises en charge et fonctions avec prise en charge limitée (p. 606).

Certains paramètres SQL Server ont changé dans SQL Server 2012.

- Les paramètres suivants ont été supprimés de SQL Server 2012 : `awe enabled`, `precompute rank` et `sql mail xps`. Ces paramètres n'étaient pas modifiables sans les instances de bases de données SQL Server et leur suppression ne doit avoir aucun impact sur votre utilisation de SQL Server.
- Un nouveau paramètre `contained database authentication` dans SQL Server 2012 prend en charge les bases de données à relation contenant-contenu partielle. Lorsque vous activez ce paramètre puis que vous créez une base de données à relation contenant-contenu partielle, le nom utilisateur et le mot de passe d'un utilisateur autorisé sont stockés dans la base de données à relation contenant-contenu partielle et non dans la base de données principale. Pour de plus amples informations sur les bases de données à relation contenant-contenu partielle, veuillez consulter Bases de données à relation contenant-contenu dans la documentation Microsoft.

Microsoft SQL Server 2008 R2 obsolète sur Amazon RDS

Nous commençons à mettre à niveau toutes les instances existantes qui utilisent encore SQL Server 2012 R2 vers la dernière version mineure de SQL Server 2012. Pour plus d'informations, consultez Gestion des versions dans Amazon RDS (p. 602).

Pour de plus amples informations sur SQL Server 2008 R2, veuillez consulter Fonctionnalités prises en charge par les éditions de SQL Server 2008 R2 dans la documentation Microsoft.

Prise en charge de la capture de données modifiées (CDC) pour les instances de base de données Microsoft SQL Server

Amazon RDS prend en charge la capture de données modifiées (CDC) pour vos instances de base de données s'exécutant sur Microsoft SQL Server. La fonction de capture de données modifiées capture les modifications apportées aux données de vos tables et stocke les métadonnées correspondant à chaque modification afin que vous puissiez y accéder ultérieurement. Pour de plus amples informations, veuillez consulter Modifier la capture de données dans la documentation de Microsoft.

Amazon RDS prend en charge la fonction CDC pour les versions et éditions suivantes de SQL Server :

- Microsoft SQL Server Enterprise Edition (toutes les versions)
- Microsoft SQL Server Standard Edition :
  - 2019
  - 2017
  - 2016 version 13.00.4422.0 SP1 CU2 ou ultérieure

Pour utiliser la fonction CDC avec vos instances de base de données Amazon RDS, vous devez activer ou désactiver CDC au niveau de la base de données à l'aide des procédures stockées fournies par RDS. Une fois cette opération effectuée, tout utilisateur ayant le rôle `db_owner` pour cette base de données peut utiliser les procédures stockées Microsoft natives sur cette base de données. Pour de plus amples informations, veuillez consulter Utilisation de la capture de données modifiées (p. 772).

Vous pouvez utiliser CDC et AWS Database Migration Service pour activer la réplication continue à partir des instances de base de données SQL Server.

Fonctions non prises en charge et fonctions avec prise en charge limitée

Les fonctions Microsoft SQL Server suivantes ne sont pas prises en charge sur Amazon RDS :

- Sauvegarde dans Microsoft Azure Blob Storage
- Extension du pool de mémoires tampons
- Data Quality Services
- Copie des journaux de transaction de base de données
- Messagerie de base de données
- Procédures stockées étendues, y compris xp_cmdshell
- Support FILESTREAM
- Tables de fichiers
- Machine Learning and R Services (exige un accès de système d'exploitation pour l'installer)
- Plans de maintenance
- Performance Data Collector
- Gestion basée sur la stratégie
- PolyBase
- Réplication
- Resource Governor
- Déclencheurs de niveau serveur
- Points de terminaison Service Broker
- Stretch Database
- Points de terminaison T-SQL (toutes les opérations utilisant CREATE ENDPOINT sont indisponibles)
- WCF Data Services

Les fonctions Microsoft SQL Server suivantes ont une prise en charge limitée sur Amazon RDS :

- Requêtes distribuées/Serveurs liés. Pour de plus amples informations, veuillez consulter Implémentation de serveurs liés avec Amazon RDS pour Microsoft SQL Server.

Déploiements multi-AZ à l'aide de la mise en miroir de bases de données ou des groupes de disponibilité AlwaysOn Microsoft SQL Server

Amazon RDS prend en charge les déploiements multi-AZ pour les instances de bases de données exécutant Microsoft SQL Server à l'aide de la mise en miroir de bases de données (DBM) ou des groupes de disponibilité (AG) AlwaysOn. Les déploiements multi-AZ améliorent la disponibilité, la durabilité des donnés et la tolérance aux pannes pour les instances de bases de données. En cas de maintenance de base de données programmée ou d'interruption non programmée du service, Amazon RDS bascule automatiquement vers le réplica secondaire à jour afin que les opérations de base de données puissent reprendre rapidement, sans intervention manuelle. Les instances principales et secondaires utilisent le même point de terminaison, dont l'adresse réseau physique est transférée vers le réplica secondaire passif dans le cadre du processus de basculement. Vous n'avez pas à reconfigurer votre application lorsqu'un basculement se produit.

Amazon RDS gère le basculement en surveillant activement votre déploiement multi-AZ et en initiant un basculement en cas de problème avec l'élément principal. Le basculement ne se produit pas, sauf si les instances principales et de secours sont complètement synchronisées. Amazon RDS maintient activement votre déploiement Multi-AZ en réparant automatiquement les instances de base de données défectueuses et en rétablissant une réplication synchrone. Vous n'avez rien à faire. Amazon RDS gère automatiquement les instances principales, les instances témoin et les instances de secours. Lorsque vous configurez déploiements multi-AZ SQL Server, RDS configure des instances secondaires passives pour toutes les bases de données de l'instance.

Pour plus d'informations, consultez Déploiements multi-AZ pour Microsoft SQL Server (p. 664).

Utilisation de Transparent Data Encryption pour chiffrer les données au repos

Amazon RDS prend en charge Microsoft SQL Server Transparent Data Encryption (TDE), qui chiffre en toute transparence les données stockées. Amazon RDS utilise des groupes d'options pour activer et configurer ces fonctions. Pour plus d'informations sur l'option TDE, consultez Prise en charge de Transparent Data Encryption dans SQL Server (p. 704).

Fonctions et procédures stockées Amazon RDS pour Microsoft SQL Server

Le tableau suivant répertorie les fonctions Amazon RDS et les procédures stockées qui aident à automatiser les tâches SQL Server.

Fonctions et procédures stockées SQL Server

Type de tâche	Procédure ou fonction	Utilisation
Tâches administratives	`rds_drop_database`	Suppression d'une base de données Microsoft SQL Server (p. 770)
	`rds_failover_time`	Détermination de l'heure du dernier basculement (p. 769)
	`rds_modify_db_name`	Modification du nom d'une base de données Microsoft SQL Server dans un déploiement Multi-AZ (p. 771)
	`rds_read_error_log`	Affichage des journaux des erreurs et des agents (p. 777)
	`rds_set_configuration`	Définit diverses configurations d'instance de base de données : • Capture de données modifiées (CDC) pour les instances multi-AZ (p. 774) • Configuration de la période de rétention pour les fichiers de trace et de vidage (p. 777) • Compression des fichiers de sauvegarde (p. 650)
	`rds_set_database_online`	Passage d'une base de données Microsoft SQL Server de l'état OFFLINE à l'état ONLINE (p. 772)

Type de tâche	Procédure ou fonction	Utilisation
	`rds_show_configuration`	Affiche les valeurs définies à l'aide de `rds_set_configuration` : • Capture de données modifiées (CDC) pour les instances multi-AZ (p. 774) • Configuration de la période de rétention pour les fichiers de trace et de vidage (p. 777)
	`rds_shrink_tempdbfile`	Réduction de la base de données tempdb (p. 761)
Capture des données de modification (CDC)	`rds_cdc_disable_db`	Désactivation CDC (p. 772)
	`rds_cdc_enable_db`	Activation de la CDC (p. 772)
Sauvegarde et restauration natives	`rds_backup_database`	Sauvegarde d'une base de données (p. 640)
	`rds_cancel_task`	Annulation d'une tâche (p. 647)
	`rds_finish_restore`	Finalisation d'une restauration de base de données (p. 647)
	`rds_restore_database`	Restauration d'une base de données (p. 642)
	`rds_restore_log`	Restauration d'un journal (p. 645)
Transfert de fichiers Amazon S3	`rds_delete_from_filesystem`	Suppression des fichiers sur l'instance RDS (p. 695)
	`rds_download_from_s3`	Téléchargement des fichiers d'un compartiment Amazon S3 vers une instance de base de données SQL Server (p. 693)
	`rds_gather_file_details`	Liste des fichiers sur l'instance de base de données RDS (p. 695)
	`rds_upload_to_s3`	Téléchargement des fichiers depuis une instance de base de données SQL Server vers un compartiment Amazon S3 (p. 694)
Microsoft Distributed Transaction Coordinator (MSDTC)	`rds_msdtc_transaction_tracing`	Utilisation du suivi des transactions (p. 756)
SQL Server Audit	`rds_fn_get_audit_file`	Consultation des journaux d'audit (p. 710)

Type de tâche	Procédure ou fonction	Utilisation
Microsoft Business Intelligence (MSBI)	`rds_msbi_task`	SQL Server Analysis Services (SSAS) : • Déploiement de projets SSAS sur Amazon RDS (p. 718) • Ajout d'un utilisateur de domaine en tant qu'administrateur de base de données (p. 721) • Sauvegarde d'une base de données SSAS (p. 721) • Restauration d'une base de données SSAS (p. 722) SQL Server Integration Services (SSIS) : • Autorisations administratives sur SSISDB (p. 731) • Déploiement d'un projet SSIS (p. 732) SQL Server Reporting Services (SSRS) : • Octroi de l'accès aux utilisateurs du domaine (p. 744) • Révocation des autorisations de niveau système (p. 745)
	`rds_fn_task_status`	Affiche l'état des tâches MSBI : • SSAS : Surveillance de l'état d'une tâche de déploiement (p. 719) • SSIS : Surveillance de l'état d'une tâche de déploiement (p. 733) • SSRS : Surveillance du statut d'une tâche (p. 745)
SSIS	`rds_drop_ssis_database`	Suppression de la base de données SSISDB (p. 738)
	`rds_sqlagent_proxy`	Création d'un proxy SSIS (p. 734)
SSRS	`rds_drop_ssrs_databases`	Suppression des bases de données SSRS (p. 747)

Fuseau horaire local pour les instances de bases de données Microsoft SQL Server

Le fuseau horaire d'une instance de base de données Amazon RDS qui exécute Microsoft SQL Server est défini par défaut. La valeur par défaut actuelle est UTC (temps universel coordonné). Vous pouvez définir le fuseau horaire de votre instance de base de données à un fuseau horaire local, correspondant à celui de vos applications.

Vous définissez le fuseau horaire lorsque vous créez votre instance de base de données. Vous pouvez créer votre instance de base de données en utilisant la AWS Management Console, l'action d'API Amazon RDS CreateDBInstance ou la commande AWS CLI create-db-instance.

Si votre instance de base de données fait partie d'un déploiement multi-AZ (utilisant la mise en miroir de bases de données ou les groupes de disponibilité SQL Server), lorsque vous basculez, votre fuseau horaire demeure celui que vous avez défini. Pour plus d'informations, consultez Déploiements multi-AZ

à l'aide de la mise en miroir de bases de données ou des groupes de disponibilité AlwaysOn Microsoft SQL Server (p. 606).

Lorsque vous demandez une restauration à un moment donné, vous spécifiez l'heure de restauration. L'heure est affichée dans votre fuseau horaire local. Pour plus d'informations, consultez Restauration d'une instance de base de données à une date spécifiée (p. 365).

Ci-après les restrictions affectant la définition du fuseau horaire local sur votre instance de base de données :

- Vous ne pouvez pas modifier le fuseau horaire d'une instance de base de données SQL Server existante.
- Vous ne pouvez pas restaurer un instantané à partir d'une instance de base de données dans un fuseau horaire dans une instance de base de données d'un autre fuseau horaire.
- Nous vous recommandons vivement de ne pas restaurer de fichier de sauvegarde d'un fuseau horaire dans un autre fuseau horaire. Si vous restaurez un fichier de sauvegarde d'un fuseau horaire dans un autre fuseau horaire, vous devez auditer vos requêtes et vos applications afin de déterminer les effets du changement de fuseau horaire. Pour plus d'informations, consultez Importation et exportation de bases de données SQL Server (p. 634).

Fuseaux horaires pris en charge

Vous pouvez définir votre fuseau horaire local avec l'une des valeurs du tableau suivant.

Fuseaux horaires pris en charge pour Amazon RDS sur SQL Server

Fuseau horaire	Décalage horaire standard	Description	Remarques
Heure normale d'Afghanistan	(UTC+04:30)	Kaboul	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale de l'Alaska	(UTC–09:00)	Alaska	
Heure normale Aléoutiennes	(UTC–10:00)	Îles Aléoutiennes	
Heure normale de l'Altaï	(UTC+07:00)	Barnaul, Gorno-Altaysk	
Heure normale arabe	(UTC+03:00)	Koweït, Riyad	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale des Emirats Arabe Unis	(UTC+04:00)	Abou Dhabi, Mascate	
Heure normale Arabie saoudite	(UTC+03:00)	Bagdad	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale d'Argentine	(UTC–03:00)	Ville de Buenos Aires	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale d'Astrakhan	(UTC+04:00)	Astrakhan, Oulianovsk	

Fuseau horaire	Décalage horaire standard	Description	Remarques
Heure normale de l'Atlantique	(UTC–04:00)	Heure de l'Atlantique (Canada)	
Heure normale de l'Australie centrale	(UTC+09:30)	Darwin	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale de l'Australie centrale	(UTC+08:45)	Eucla	
Heure normale de l'Australie orientale	(UTC+10:00)	Canberra, Melbourne, Sydney	
Heure normale d'Azerbaïdjan	(UTC+04:00)	Bakou	
Heure normale des Açores	(UTC–01:00)	Açores	
Heure normale de Bahia	(UTC–03:00)	Salvador	
Heure normale du Bangladesh	(UTC+06:00)	Dacca	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale de Biélorussie	(UTC+03:00)	Minsk	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale de Bougainville	(UTC+11:00)	Île de Bougainville	
Heure normale du Canada central	(UTC–06:00)	Saskatchewan	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale du Cap-Vert	(UTC–01:00)	Cap-Vert	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale du Caucase	(UTC+04:00)	Erevan	
Heure normale de l'Australie centrale	(UTC+09:30)	Adélaïde	
Heure normale de l'Amérique centrale	(UTC–06:00)	Amérique centrale	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale de l'Asie centrale	(UTC+06:00)	Astana	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale du Brésil central	(UTC–04:00)	Cuiabá	
Heure normale de l'Europe centrale	(UTC+01:00)	Belgrade, Bratislava, Budapest, Ljubljana, Prague	

Fuseau horaire	Décalage horaire standard	Description	Remarques
Heure normale de l'Europe centrale	(UTC+01:00)	Sarajevo, Skopje, Varsovie, Zagreb	
Heure normale du Pacifique central	(UTC+11:00)	Îles Salomon, Nouvelle-Calédonie	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale du Centre	(UTC–06:00)	Heure centrale (États-Unis et Canada)	
Heure normale du Centre (Mexique)	(UTC–06:00)	Guadalajara, Mexico, Monterrey	
Heure normale des îles Chatham	(UTC+12:45)	Îles Chatham	
Heure normale de Chine	(UTC+08:00)	Pékin, Chongqing, Hong-Kong, Urumqi	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale de Cuba	(UTC–05:00)	La Havane	
Heure normale de la ligne de changement de date	(UTC–12:00)	Ligne de changement de date internationale Ouest	Ce fuseau horaire ne respecte pas l'heure d'été.
E. Heure normale d'Afrique	(UTC+03:00)	Nairobi	Ce fuseau horaire ne respecte pas l'heure d'été.
E. normale de l'Australie centrale	(UTC+10:00)	Brisbane	Ce fuseau horaire ne respecte pas l'heure d'été.
E. Heure normale d'Europe	(UTC+02:00)	Chi#inău	
E. Heure normale d'Amérique du Sud	(UTC–03:00)	Brasilia	
Heure normale de l'île de Pâques	(UTC–06:00)	Île de Pâques	
Heure normale de l'Est	(UTC–05:00)	Heure de l'Est (États-Unis et Canada)	
Heure normale de l'Est (Mexique)	(UTC–05:00)	Chetumal	
Heure normale de l’Égypte	(UTC+02:00)	Le Caire	
Heure normale d'Iekaterinbourg	(UTC+05:00)	Iekaterinbourg	
Heure normale des Fidji	(UTC+12:00)	Fidji	
Heure normale de l’Europe de l’Est	(UTC+02:00)	Helsinki, Kiev, Riga, Sofia, Tallinn, Vilnius	

Fuseau horaire	Décalage horaire standard	Description	Remarques
Heure normale de Géorgie	(UTC+04:00)	Tbilisi	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale GMT	(UTC)	Dublin, Edimbourg, Lisbonne, Londres	Ce fuseau horaire n'est pas le même que l'heure moyenne de Greenwich (GMT). Ce fuseau horaire respecte l'heure d'été.
Heure normale du Groenland	(UTC–03:00)	Groenland	
Heure normale de Greenwich	(UTC)	Monrovia, Reykjavik	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale GTB	(UTC+02:00)	Athènes, Bucarest	
Heure normale d'Haïti	(UTC–05:00)	Haïti	
Heure normale de Hawaï	(UTC–10:00)	Hawaii	
Heure normale d'Inde	(UTC+05:30)	Chennai, Calcutta, Mumbai, New Delhi	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale de l’Iran	(UTC+03:30)	Téhéran	
Heure normale d'Israël	(UTC+02:00)	Jérusalem	
Heure normale de Jordanie	(UTC+02:00)	Amman	
Heure normale de Kaliningrad	(UTC+02:00)	Kaliningrad	
Heure normale du Kamtchatka	(UTC+12:00)	Petropavlovsk-Kamchatsky – Ancienne	
Heure normale de Corée	(UTC+09:00)	Séoul	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale de Libye	(UTC+02:00)	Tripoli	
Heure normale des îles de la Ligne	(UTC+14:00)	Île Christmas	
Heure normale de l’île Lord Howe	(UTC+10:30)	Île Lord Howe	
Heure normale de Magadan	(UTC+11:00)	Magadan	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale en Magallanes	(UTC–03:00)	Punta Arenas	
Heure normale des Marquises	(UTC–09:30)	Îles Marquises	

Fuseau horaire	Décalage horaire standard	Description	Remarques
Heure normale de Maurice	(UTC+04:00)	Port Louis	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale du Moyen-Orient	(UTC+02:00)	Beyrouth	
Heure normale de Montevideo	(UTC–03:00)	Montevideo	
Heure normale du Maroc	(UTC+01:00)	Casablanca	
Heure normale des Rocheuses	(UTC–07:00)	Heure des Rocheuses (États-Unis et Canada)	
Heure normale des Rocheuses (Mexique)	(UTC–07:00)	Chihuahua, La Paz, Mazatlán	
Heure normale du Myanmar	(UTC+06:30)	Yangon (Rangoun)	Ce fuseau horaire ne respecte pas l'heure d'été.
Virginie Heure normale de l'Asie centrale	(UTC+07:00)	Novossibirsk	
Heure normale de Namibie	(UTC+02:00)	Windhoek	
Heure normale du Népal	(UTC+05:45)	Katmandou	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale de Nouvelle-Zélande	(UTC+12:00)	Auckland, Wellington	
Heure normale de Terre-Neuve	(UTC–03:30)	Terre-Neuve	
Heure normale de l’île Norfolk	(UTC+11:00)	Île Norfolk	
Heure normale de l'Asie du Nord-Est	(UTC+08:00)	Irkoutsk	
Heure normale de l'Asie du Nord	(UTC+07:00)	Krasnoïarsk	
Heure normale de la Corée du Nord	(UTC+09:00)	Pyongyang	
Heure normale d’Omsk	(UTC+06:00)	Omsk	
Heure normale du Pacifique	(UTC–03:00)	Santiago	
Heure normale du Pacifique	(UTC–08:00)	Heure du Pacifique (États-Unis et Canada)	
Heure normale du Pacifique (Mexique)	(UTC–08:00)	Basse-Californie	

Fuseau horaire	Décalage horaire standard	Description	Remarques
Heure normale du Pakistan	(UTC+05:00)	Islamabad, Karachi	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale du Paraguay	(UTC–04:00)	Asunción	
Heure normale Romance	(UTC+01:00)	Bruxelles, Copenhague, Madrid, Paris	
Fuseau horaire 10 Russie	(UTC+11:00)	Chokurdakh	
Fuseau horaire 11 Russie	(UTC+12:00)	Anadyr, Petropavlovsk-Kamchatsky	
Fuseau horaire 3 Russie	(UTC+04:00)	Izhevsk, Samara	
Heure normale de Russie	(UTC+03:00)	Moscou, Saint-Pétersbourg, Volgograd	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale de l'Est AS	(UTC–03:00)	Cayenne, Fortaleza	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale du Pacifique	(UTC–05:00)	Bogota, Lima, Quito, Rio Branco	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale de l'Ouest AS	(UTC–04:00)	Georgetown, La Paz, Manaus, San Juan	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale Saint-Pierre	(UTC–03:00)	Saint-Pierre-et-Miquelon	
Heure normale de Sakhaline	(UTC+11:00)	Sakhaline	
Heure normale des Samoa	(UTC+13:00)	Samoa	
Heure normale de Sao Tomé	(UTC+01:00)	Sao Tomé	
Heure normale de Saratov	(UTC+04:00)	Saratov	
Heure normale de l'Asie du Sud-Est	(UTC+07:00)	Bangkok, Hanoï, Djakarta	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale de Singapour	(UTC+08:00)	Kuala Lumpur, Singapour	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale d'Afrique du Sud	(UTC+02:00)	Harare, Pretoria	Ce fuseau horaire ne respecte pas l'heure d'été.

Fuseau horaire	Décalage horaire standard	Description	Remarques
Heure normale du Sri Lanka	(UTC+05:30)	Sri Jayawardenepura	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale du Soudan	(UTC+02:00)	Khartoum	
Heure normale de Syrie	(UTC+02:00)	Damas	
Heure normale de Taipei	(UTC+08:00)	Taipei	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale de Tasmanie	(UTC+10:00)	Hobart	
Heure normale du Tocantins	(UTC–03:00)	Araguaina	
Heure normale de Tokyo	(UTC+09:00)	Osaka, Sapporo, Tokyo	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale de Tomsk	(UTC+07:00)	Tomsk	
Heure normale des Tonga	(UTC+13:00)	Nuku'alofa	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale de la Transbaïkalie	(UTC+09:00)	Tchita	
Heure normale de Turquie	(UTC+03:00)	Istanbul	
Heure normale des îles Turques-et-Caïques	(UTC–05:00)	Turques-et-Caïques	
Heure normale d'Oulan-Bator	(UTC+08:00)	Oulan-Bator	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale de l'Est	(UTC–05:00)	Indiana (Est)	
Heure normale des Rocheuses	(UTC–07:00)	Arizona	Ce fuseau horaire ne respecte pas l'heure d'été.
UTC	UTC	Temps universel coordonné	Ce fuseau horaire ne respecte pas l'heure d'été.
UTC–02	(UTC–02:00)	Temps universel coordonné–02	Ce fuseau horaire ne respecte pas l'heure d'été.
UTC–08	(UTC–08:00)	Temps universel coordonné–08	
UTC–09	(UTC–09:00)	Temps universel coordonné–09	

Fuseau horaire	Décalage horaire standard	Description	Remarques
UTC–11	(UTC–11:00)	Temps universel coordonné–11	Ce fuseau horaire ne respecte pas l'heure d'été.
UTC+12	(UTC+12:00)	Temps universel coordonné+12	Ce fuseau horaire ne respecte pas l'heure d'été.
UTC+13	(UTC+13:00)	Temps universel coordonné+13	
Heure normale du Venezuela	(UTC–04:00)	Caracas	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale de Vladivostok	(UTC+10:00)	Vladivostok	
Heure normale de Volgograd	(UTC+04:00)	Volgograd	
W. normale de l'Australie centrale	(UTC+08:00)	Perth	Ce fuseau horaire ne respecte pas l'heure d'été.
W. Heure normale d'Afrique centrale	(UTC+01:00)	Afrique centrale de l'Ouest	Ce fuseau horaire ne respecte pas l'heure d'été.
W. Heure normale d'Europe	(UTC+01:00)	Amsterdam, Berlin, Berne, Rome, Stockholm, Vienne	
W. Heure normale de Mongolie	(UTC+07:00)	Hovd	
Heure normale de l'Asie de l’Est	(UTC+05:00)	Achgabat, Tachkent	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale de Cisjordanie	(UTC+02:00)	Gaza, Hébron	
Heure normale du Pacifique Ouest	(UTC+10:00)	Guam, Port Moresby	Ce fuseau horaire ne respecte pas l'heure d'été.
Heure normale de Iakoutsk	(UTC+09:00)	Iakoutsk	

Gestion des licences Microsoft SQL Server sur Amazon RDS

Lorsque vous définissez une instance de base de données Amazon RDS pour Microsoft SQL Server, la licence logicielle est incluse.

Cela signifie que vous n'avez pas besoin d'acheter séparément des licences SQL Server. AWS gère la licence du logiciel de base de données SQL Server. Amazon RDS comprend la licence de logiciel, les ressources matérielles sous-jacentes et les capacités de gestion Amazon RDS.

Amazon RDS prend en charge les éditions Microsoft SQL Server suivantes :

- Enterprise
- Standard
- Web
- Express

> Note
>
> La gestion des licences pour SQL Server Web Edition prend en charge uniquement les pages Web, les sites Web, les applications Web et les services Web bénéficiant d'un accès public et Internet. Ce niveau de prise en charge est obligatoire pour la conformité avec les droits d'utilisation de Microsoft. Pour de plus amples informations, veuillez consulter Conditions de service AWS.

Amazon RDS prend en charge les déploiements Multi-AZ pour les instances de bases de données exécutant Microsoft SQL Server à l'aide de la mise en miroir de bases de données SQL Server ou des groupes de disponibilité AlwaysOn. Il n'y a aucune exigence de licence supplémentaire pour les déploiements multi-AZ. Pour plus d'informations, consultez Déploiements multi-AZ pour Microsoft SQL Server (p. 664).

Restauration des instances de bases de données résiliées faute de licence

Amazon RDS prend des instantanés des instances de base de données résiliées faute de licence. Si votre instance est résiliée en raison de problèmes de licences, vous pouvez la restaurer depuis l'instantané vers une nouvelle instance de base de données. Les nouvelles instances de base de données incluent une licence.

Pour plus d'informations, consultez Restauration des instances de bases de données résiliées faute de licence (p. 771).

Développement et test

En raison des exigences concernant les licences, nous ne pouvons pas fournir l'édition SQL Server Developer dans Amazon RDS. Vous pouvez utiliser l'édition Express à des fins de développement, des tests et pour répondre à des besoins autre que la production. Toutefois, si vous avez besoin des fonctions complètes d'une installation de niveau entreprise de SQL Server pour le développement, vous pouvez télécharger et installer l'édition SQL Server Developer (et d'autres produits MSDN) sur Amazon EC2. Aucune infrastructure dédiée n'est requise pour l'édition Développeur. En utilisant votre propre, vous pouvez également accéder à d'autres fonctions de programmabilité qui ne sont pas accessibles dans Amazon RDS. Pour plus d'informations sur la différence entre les éditions SQL Server, consultez Editions and supported features of SQL Server 2017 (Éditions et fonctions prises en charge de SQL Server 2017) dans la documentation de Microsoft.

Connexion à une instance de base de données exécutant le moteur de base de données Microsoft SQL Server

Après qu'Amazon RDS a provisionné votre instance de base de données, vous pouvez utiliser n'importe quelle application cliente SQL standard pour vous connecter à l'instance de base de données. Dans cette

rubrique, vous vous connectez à votre instance de base de données à l'aide de Microsoft SQL Server Management Studio (SSMS) ou de SQL Workbench/J.

Pour obtenir un exemple qui vous explique le processus de création et de connexion à un exemple d'instance de base de données, consultez Création d'une instance de base de données Microsoft SQL Server et connexion à une instance de base de données (p. 76).

Connexion à votre instance de base de données avec Microsoft SQL Server Management Studio

Au cours de cette procédure, vous vous connectez à votre exemple d'instance de base de données à l'aide de Microsoft SQL Server Management Studio (SSMS). Pour télécharger une version autonome de cet utilitaire, veuillez consulter Télécharger SQL Server Management Studio (SSMS) dans la documentation Microsoft.

Pour vous connecter à une instance de base de données à l'aide de SSMS

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le coin supérieur droit de la console Amazon RDS, choisissez la région AWS de votre instance de base de données.
3. Trouvez le numéro de port et le nom DNS (Domain Name System) pour votre instance de base de données :
   a. Ouvrez la console RDS et choisissez Bases de données pour afficher une liste de vos instances de bases de données.
   b. Choisissez le nom de l'instance de base de données SQL Server pour afficher ses détails.
   c. Dans l'onglet Connectivity & security (Connectivité et sécurité), copiez le point de terminaison. Notez également le numéro du port. Vous avez besoin du point de terminaison et du numéro de port pour vous connecter à l'instance de base de données.

4. Démarrez SQL Server Management Studio.

   La boîte de dialogue Connect to Server (Se connecter à un serveur) s'affiche.

5. Fournissez les informations relatives à votre instance de base de données :

   a. Pour Server type (Type de serveur), choisissez Database Engine (Moteur de base de données).

   b. Pour Server name (Nom du serveur), saisissez le nom DNS et le numéro de port de votre instance de base de données, séparés par une virgule.

      Important

      Remplacez les deux-points entre le nom DNS et le numéro de port par une virgule.

      Par exemple, le nom du serveur doit se présenter comme suit.

```
database-2.cg034itsfake.us-east-1.rds.amazonaws.com,1433
```

   c. Pour Authentication, choisissez Authentication SQL Server.

   d. Pour Login (Connexion), saisissez le nom d'utilisateur principal de votre instance de base de données.

   e. Pour Password (Mot de passe), saisissez le mot de passe de votre instance de base de données.

6. Choisissez Connexion.

   Après quelques instants, SSMS se connecte à votre instance de base de données. Si vous ne pouvez pas vous connecter à votre instance de base de données, consultez Considérations relatives aux groupes de sécurité (p. 624) et Résolution des problèmes de connexion à votre instance de base de données SQL Server (p. 624).

7. Votre instance de base de données SQL Server est fournie avec les bases de données système intégrées standard de SQL Server (`master`, `model`, `msdb` et `tempdb`). Pour explorer les bases de données système, effectuez les opérations suivantes :

   a. Dans SSMS, dans le menu View (Afficher), choisissez Object Explorer (Navigateur d'objet).

   b. Développez votre instance de base de données, développez Databases (Bases de données), puis System Databases (Bases de données système).

8. Votre instance de base de données SQL Server est également accompagnée d'une base de données nommée `rdsadmin`. Amazon RDS utilise cette base de données pour stocker les objets dont il se sert pour gérer votre base de données. La base de données `rdsadmin` inclut également des procédures stockées que vous pouvez exécuter pour effectuer des tâches avancées. Pour plus d'informations, consultez Tâches DBA courantes pour Microsoft SQL Server (p. 759).
9. Vous pouvez maintenant commencer à créer vos propres bases de données et à exécuter des requêtes sur votre instance de base de données et vos bases de données comme d'habitude. Pour exécuter une requête de test sur votre instance de base de données, procédez comme suit :
   a. Dans SSMS, dans le menu Fichier, pointez sur Nouveau, puis choisissez Query with Current Connection (Requête avec la connexion actuelle).
   b. Entrez la requête SQL suivante.

```
select @@VERSION
```

   c. Exécutez la requête. SSMS renvoie la version SQL Server de votre instance de base de données Amazon RDS.

Connexion à votre instance de base de données avec SQL Workbench/J

Cet exemple montre comment se connecter à une instance de base de données exécutant le moteur de base de données Microsoft SQL Server en utilisant l'outil de base de données SQL Workbench/J. Pour télécharger SQL Workbench/J, consultez SQL Workbench/J.

SQL Workbench/J utilise JDBC pour se connecter à votre instance de base de données. Vous avez également besoin du pilote JDBC pour SQL Server. Pour télécharger ce pilote, consultez Microsoft JDBC Drivers 4.1 (Preview) and 4.0 for SQL Server.

Se connecter à une instance de base de données à l'aide de SQL Workbench/J

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le coin supérieur droit de la console Amazon RDS, choisissez la région AWS de votre instance de base de données.
3. Trouvez le numéro de port et le nom DNS pour votre instance de base de données :
   a. Ouvrez la console RDS et choisissez Bases de données pour afficher une liste de vos instances de base de données.
   b. Choisissez le nom de votre instance de base de données SQL Server pour en afficher les détails.

   c. Dans l'onglet Connectivité, copiez le point de terminaison. Notez également le port utilisé par l'instance de base de données.
4. Ouvrez SQL Workbench/J. La boîte de dialogue Select Connection Profile (Sélectionner le profil de connexion) s'affiche, comme illustré ci-dessous.

5. Dans la première case en haut de la boîte de dialogue, saisissez un nom pour le profil.
6. Pour Driver (Pilote), sélectionnez **`SQL JDBC 4.0`**.
7. Pour URL, saisissez **`jdbc:sqlserver://`**, puis le point de terminaison de votre instance de base de données. Par exemple, la valeur de l'URL pourrait être la suivante.

```
jdbc:sqlserver://sqlsvr-pdz.abcd12340.us-west-2.rds.amazonaws.com:1433
```

8. Pour Nom d'utilisateur, saisissez le nom d'utilisateur principal de votre instance de base de données.
9. Pour Mot de passe, saisissez le mot de passe pour l'utilisateur principal.
10. Choisissez l'icône d'enregistrement dans la barre d'outils de la boîte de dialogue, comme illustré ci-dessous.

11. Choisissez OK. Après quelques instants, SQL Workbench/J se connecte à votre instance de base de données. Si vous ne pouvez pas vous connecter à votre instance de base de données, consultez Considérations relatives aux groupes de sécurité (p. 624) et Résolution des problèmes de connexion à votre instance de base de données SQL Server (p. 624).
12. Dans le volet de requête, saisissez la requête SQL suivante.

```
select @@VERSION
```

13. Choisissez l'icône `Execute` dans la barre d'outils, comme illustré ci-dessous.

La requête renvoie les informations de version pour votre instance de base de données, comme illustré ci-dessous.

```
Microsoft SQL Server 2012 - 11.0.2100.60 (X64)
```

Considérations relatives aux groupes de sécurité

Pour vous connecter à votre instance de base de données, cette dernière doit être associée à un groupe de sécurité. Ce groupe de sécurité contient les adresses IP et la configuration réseau que vous utilisez pour accéder à l'instance de base de données. Vous avez peut-être associé votre instance de base de données à un groupe de sécurité correspondant lorsque vous avez créé votre instance de base de données. Si vous avez attribué un groupe de sécurité non configuré par défaut lors de la création de votre instance de base de données, le pare-feu de celle-ci bloque les connexions.

Dans certains cas, vous devrez peut-être créer un groupe de sécurité pour autoriser l'accès. Le type du groupe de sécurité à créer dépendra de la plateforme Amazon EC2 sur laquelle se trouve votre instance de base de données. Pour déterminer votre plateforme, consultez Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611). En général, si votre instance de base de données se trouve sur la plateforme EC2-Classic, vous créez un groupe de sécurité de base de données. Si votre instance de base de données se trouve sur la plateforme VPC, vous créez un groupe de sécurité VPC.

Pour obtenir des instructions sur la création d'un nouveau groupe de sécurité, consultez Contrôle d'accès par groupe de sécurité (p. 1590). Pour accéder à une rubrique qui décrit le processus de configuration des règles pour votre groupe de sécurité VPC, veuillez consulter Didacticiel : créer un Amazon VPC à utiliser avec une instance de base de données (p. 1629).

Une fois le groupe de sécurité créé, modifiez votre instance de base de données pour l'associer au groupe de sécurité. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Vous pouvez améliorer la sécurité en utilisant SSL pour chiffrer les connexions à votre instance de base de données. Pour plus d'informations, consultez Utilisation de SSL avec une instance DB Microsoft SQL Server (p. 669).

Résolution des problèmes de connexion à votre instance de base de données SQL Server

Le tableau ci-dessous répertorie les messages d'erreur qui peuvent survenir lors d'une tentative de connexion à votre instance de base de données SQL Server. Pour de plus amples informations sur les problèmes de connexion, veuillez consulter Impossible de se connecter à l'instance de base de données Amazon RDS (p. 1639).

Problème	Suggestions de dépannage
Could not open a connection to SQL Server – Microsoft SQL Server, Error: 53	Vérifiez que vous avez spécifié le nom de serveur correct. Pour Server name (Nom du serveur), saisissez le nom DNS et le numéro de port de votre exemple d'instance de base de données, séparés par une virgule. **Important** Si le nom DNS et le numéro de port sont séparés par deux-points, remplacez ces derniers par une virgule. Votre nom de serveur doit ressembler à l'exemple suivant. `sample-instance.cg034itsfake.us-east-1.rds.amazonaws.com,1433`
No connection could be made because the target machine actively refused it – Microsoft SQL Server, Error: 10061	Vous avez pu atteindre l'instance de base de données, mais la connexion a été refusée. Ce problème est souvent dû au fait que le nom d'utilisateur ou le mot de passe spécifié est incorrect. Vérifiez le nom d'utilisateur et le mot de passe, puis réessayez.

Problème	Suggestions de dépannage
A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible... The wait operation timed out – Microsoft SQL Server, Error: 258	Les règles d'accès appliquées par votre pare-feu local et les adresses IP autorisées à accéder à votre instance de base de données ne correspondent peut-être pas. Le problème est probablement lié aux règles entrantes de votre groupe de sécurité.
	Votre instance de base de données doit être accessible au public. Pour s'y connecter depuis l'extérieur du VPC, une adresse IP publique doit être attribuée à l'instance.

Mise à jour des applications pour se connecter aux instances de bases de données Microsoft SQL Server à l'aide des nouveaux certificats SSL/TLS

Le 19 septembre 2019, Amazon RDS a publié de nouveaux certificats de l'autorité de certification (CA) à connecter à vos instances de bases de données RDS à l'aide du protocole Secure Socket Layer ou Transport Layer Security (SSL/TLS). Vous trouverez ci-après des informations sur la mise à jour de vos applications afin d'utiliser les nouveaux certificats.

Cette rubrique peut vous aider à déterminer si des applications clientes utilisent un protocole SSL/TLS pour se connecter à vos instances de bases de données. Si tel est le cas, il vous est alors possible de vérifier si ces applications nécessitent une vérification du certificat pour se connecter.

> Note
>
> Certaines applications sont configurées pour se connecter aux instances de bases de données SQL Server uniquement si la vérification du certificat sur le serveur s'effectue avec succès. Pour ces applications, vous devez mettre à jour les magasins d'approbations des applications clientes afin d'inclure les nouveaux certificats de l'autorité de certification.

Une fois que vous avez mis à jour les certificats de l'autorité de certification dans les magasins d'approbations des applications clientes, vous pouvez soumettre les certificats de vos instances de bases de données à une rotation. Nous vous recommandons vivement de tester ces procédures dans un environnement de développement ou intermédiaire avant de les implémenter dans vos environnements de production.

Pour de plus amples informations sur la rotation de certificats, veuillez consulter Rotation de votre certificat SSL/TLS (p. 1527). Pour en savoir plus sur le téléchargement de certificats, consultez Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525). Pour de plus amples informations sur l'utilisation des protocoles SSL/TLS avec les instances de bases de données Microsoft SQL Server, veuillez consulter Utilisation de SSL avec une instance DB Microsoft SQL Server (p. 669).

Rubriques

- Contrôle de la connexion des applications aux instances de bases de données Microsoft SQL Server avec un protocole SSL (p. 626)
- Contrôle de la nécessité d'une vérification du certificat du client pour qu'il puisse se connecter (p. 626)
- Mise à jour du magasin d'approbations de votre application (p. 628)

Contrôle de la connexion des applications aux instances de bases de données Microsoft SQL Server avec un protocole SSL

Dans la configuration de l'instance de base de données, vérifiez la valeur du paramètre `rds.force_ssl`. Par défaut, le paramètre `rds.force_ssl` a pour valeur 0 (désactivé). Si le paramètre `rds.force_ssl` est défini sur 1 (activé), les clients doivent utiliser le protocole SSL/TLS pour se connecter. Pour plus d'informations sur les groupes de paramètres, consultez Utilisation de groupes de paramètres de base de données (p. 225). Vous pouvez également trouver le réglage de ce paramètre dans le DMV `sys.dm_server_registry`.

Exécutez la requête suivante afin d'obtenir l'option de chiffrement actuelle pour toutes les connexion ouvertes à une instance de base de données. La colonne `ENCRYPT_OPTION` renvoie `TRUE` si la connexion est chiffrée.

```
select SESSION_ID,
    ENCRYPT_OPTION,
    NET_TRANSPORT,
    AUTH_SCHEME
    from SYS.DM_EXEC_CONNECTIONS
```

Cette requête affiche uniquement les connexions actuelles. Elle n'indique pas si les applications qui se sont connectées et déconnectées par le passé ont utilisé un protocole SDSL.

Contrôle de la nécessité d'une vérification du certificat du client pour qu'il puisse se connecter

Vous pouvez vérifier si différents types de clients requièrent une vérification du certificat pour pouvoir se connecter.

> **Note**
>
> Si vous utilisez des connecteurs autres que ceux répertoriés, veuillez consulter la documentation spécifique au connecteur pour des informations sur leur façon d'appliquer des connexions chiffrées. Pour de plus amples informations, veuillez consulter Modules de connexion pour les bases de données Microsoft SQL dans la documentation Microsoft SQL Server.

SQL Server Management Studio

Vérifiez si le chiffrement est appliqué pour les connexions SQL Server Management Studio :

1. Lancez SQL Server Management Studio.
2. Pour Connect to server (Se connecter au serveur), entrez les informations de serveur, le mot de passe et le nom d'utilisateur de connexion.
3. Choisissez Options.
4. Vérifiez si Encrypt connection (Chiffrer la connexion) est sélectionné sur la page de connexion.

Pour plus d'informations sur SQL Server Management Studio, consultez Utilisation de SQL Server Management Studio.

sqlcmd

Les exemples suivants avec le client `sqlcmd` montrent comment vérifier la connexion SQL Server d'un script pour déterminer si les connexions nécessitent un certificat valide pour réussir. Pour de plus amples informations, veuillez consulter, Connexion avec sqlcmd dans la documentation Microsoft SQL Server.

Lorsque vous utilisez `sqlcmd`, une connexion SSL nécessite la vérification du certificat de serveur si vous spécifiez l'argument de commande `-N`, comme illustré dans l'exemple suivant.

```
$ sqlcmd -N -S dbinstance.rds.amazon.com -d ExampleDB
```

> **Note**
>
> Si `sqlcmd` est invoqué avec l'option `-C`, il approuve le certificat de serveur, même s'il ne correspond pas au magasin d'approbations côté client.

ADO.NET

Dans l'exemple suivant, l'application se connecte à l'aide d'un protocole SSL et le certificat de serveur doit être vérifié.

```
using SQLC = Microsoft.Data.SqlClient;

...

    static public void Main()
    {
        using (var connection = new SQLC.SqlConnection(
            "Server=tcp:dbinstance.rds.amazon.com;" +
            "Database=ExampleDB;User ID=LOGIN_NAME;" +
            "Password=YOUR_PASSWORD;" +
            "Encrypt=True;TrustServerCertificate=False;"
            ))
        {
            connection.Open();
            ...
        }
```

Java

Dans l'exemple suivant, l'application se connecte à l'aide d'un protocole SSL et le certificat de serveur doit être vérifié.

```
String connectionUrl =
    "jdbc:sqlserver://dbinstance.rds.amazon.com;" +
    "databaseName=ExampleDB;integratedSecurity=true;" +
    "encrypt=true;trustServerCertificate=false";
```

Pour activer le chiffrement SSL pour des clients qui se connectent en utilisant JDBC, vous devrez peut-être ajouter le certificat Amazon RDS au magasin de certificats de l'autorité de certification Java. Pour obtenir des instructions, veuillez consulter Configuration du client pour le chiffrement dans la documentation

Microsoft SQL Server. Vous pouvez également fournir directement le nom du fichier du certificat de l'autorité de certification approuvé en ajoutant `trustStore=`*`path-to-certificate-trust-store-file`* à la chaîne de connexion.

> **Note**
>
> Si vous utilisez `TrustServerCertificate=true` (ou son équivalent) dans la chaîne de connexion, le processus de connexion ignore la validation de la chaîne d'approbation. Dans ce cas, l'application se connecte, même lorsque le certificat ne peut pas être vérifié. Utiliser `TrustServerCertificate=false` applique la validation du certificat, en plus d'être une bonne pratique.

Mise à jour du magasin d'approbations de votre application

Vous pouvez mettre à jour le magasin d'approbations pour les applications qui utilisent Microsoft SQL Server. Pour obtenir des instructions, consultez Chiffrement de connexions spécifiques (p. 670). Veuillez également consulter Configuration du client pour le chiffrement dans la documentation Microsoft SQL Server.

Si vous utilisez un système d'exploitation différent de Microsoft Windows, veuillez consulter la documentation de distribution de logiciels pour l'implémentation de protocoles SSL/TLS afin d'obtenir des informations sur l'ajout d'un nouveau certificat racine de l'autorité de certification. Par exemple, OpenSSL et GnuTLS sont des options populaires. Utilisez la méthode d'implémentation pour ajouter une approbation au certificat racine RDS de l'autorité de certification. Microsoft fournit des instructions afin de configurer des certificats sur certains systèmes.

> **Note**
>
> Lors de la mise à jour du magasin d'approbations, vous pouvez conserver les certificats plus anciens en complément de l'ajout des nouveaux certificats.

Mise à jour du magasin d'approbations de votre application pour JDBC

Vous pouvez mettre à jour le magasin d'approbations pour les applications qui utilisent JDBC dans le cadre de connexions SSL/TLS.

Pour mettre à jour le magasin d'approbations pour les applications JDBC

1. Téléchargez le certificat racine 2019 qui fonctionne pour toutes les régions AWS et placez le fichier dans le répertoire du magasin d'approbations.

   Pour plus d'informations sur le téléchargement du certificat racine, consultez Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).
2. Convertissez le certificat au format .der à l'aide de la commande suivante.

   ```
   openssl x509 -outform der -in rds-ca-2019-root.pem -out rds-ca-2019-root.der
   ```

   Remplacez le nom du fichier par celui du fichier téléchargé.
3. Importez le certificat dans le magasin de clés à l'aide de la commande suivante.

```
keytool -import -alias rds-root -keystore clientkeystore -file rds-ca-2019-root.der
```

4. Vérifiez que le magasin de clés a été mis à jour avec succès.

```
keytool -list -v -keystore clientkeystore.jks
```

Entrez le mot de passe du magasin de clés lorsque vous y êtes invité.

La sortie doit contenir les lignes suivantes :

```
rds-root,date, trustedCertEntry,
Certificate fingerprint (SHA1):
 D4:0D:DB:29:E3:75:0D:FF:A6:71:C3:14:0B:BF:5F:47:8D:1C:80:96
# This fingerprint should match the output from the below command
openssl x509 -fingerprint -in rds-ca-2019-root.pem -noout
```

Important

Une fois que vous avez déterminé que vos connexions de base de données utilisent un protocole SSL/TLS et que vous avez mis à jour le magasin d'approbations de votre application, vous pouvez mettre à jour votre base de données de sorte qu'elle utilise les certificats rds-ca-2019. Pour obtenir des instructions, veuillez consulter l'étape 3 dans Mise à jour de votre certificat CA en modifiant votre instance de base de données (p. 1528).

Mise à niveau du moteur de base de données Microsoft SQL Server

Lorsque Amazon RDS prend en charge une nouvelle version d'un moteur de base de données, vous pouvez mettre à niveau vos instances de base de données vers cette nouvelle version. Il existe deux types de mises à niveau pour les instances de base de données SQL Server : les mises à niveau de version majeure et les mises à niveau de version mineure.

Les mises à niveau de version majeure peuvent contenir des modifications de base de données qui ne sont pas rétrocompatibles avec les applications existantes. En conséquence, vous devez effectuer manuellement les mises à niveau de version majeure de vos instances de base de données. Vous pouvez lancer une mise à niveau de version majeure en modifiant votre instance de base de données. Cependant, avant d'effectuer une mise à niveau de version majeure, nous vous recommandons de tester la mise à niveau en suivant les étapes décrites dans Test d'une mise à niveau (p. 633).

En revanche, une mise à niveau de version mineure contient uniquement des modifications rétrocompatibles avec les applications existantes. Vous pouvez lancer manuellement une mise à niveau de version mineure en modifiant votre instance de base de données.

Amazon RDS sur SQL Server ne prend pas en charge les mises à niveau automatiques des versions mineures. Vous pouvez confirmer ces informations en utilisant la commande `describe-db-engine-versions` AWS CLI. Exemples :

```
aws rds describe-db-engine-versions --engine sqlserver-se --engine-version 14.00.3049.1.v1
```

Dans cet exemple, la commande de l'interface de ligne de commande renvoie la réponse suivante qu indique que la mise à niveau ne sera pas automatique, même si l'option Mise à niveau automatique des versions mineures a été sélectionnée :

```
...

"ValidUpgradeTarget": [
    {
        "Engine": "sqlserver-se",
        "EngineVersion": "14.00.3192.2.v1",
        "Description": "SQL Server 2017 14.00.3192.2.v1",
        "AutoUpgrade": false,
        "IsMajorVersionUpgrade": false
    }

...
```

Pour de plus amples informations sur l'exécution de mises à niveau, veuillez consulter Mise à niveau d'une instance de base de données SQL Server (p. 634). Pour de plus amples informations sur les versions SQL Server disponibles sur Amazon RDS, veuillez consulter Microsoft SQL Server sur Amazon RDS (p. 592).

Rubriques

- Présentation de la mise à niveau (p. 630)
- Mises à niveau de version majeure. (p. 631)
- Considérations relatives à l'environnement Multi-AZ et à l'optimisation en mémoire (p. 632)
- Considérations relatives au groupe d'options et de paramètres (p. 632)
- Test d'une mise à niveau (p. 633)
- Mise à niveau d'une instance de base de données SQL Server (p. 634)
- Mise à niveau des instances de base de données obsolètes avant la fin de la prise en charge (p. 634)

Présentation de la mise à niveau

Amazon RDS prend deux instantanés de base de données au cours du processus de mise à niveau. Le premier instantané de base de données porte sur l'instance de base de données avant que toute modification de mise à niveau soit apportée. Si la mise à niveau ne fonctionne pas pour vos bases de données, vous pouvez restaurer cet instantané pour créer une instance de base de données exécutant l'ancienne version. Le second instantané de base de données est pris à la fin de la mise à niveau.

> **Note**
>
> Amazon RDS ne prend des instantanés de base de données que si vous avez défini la période de rétention des sauvegardes de votre instance de base de données sur un nombre supérieur à 0. Pour modifier la période de rétention des sauvegardes, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Une fois une mise à niveau terminée, vous ne pouvez pas rétablir la version précédente du moteur de base de données. Si vous souhaitez revenir à la version précédente, restaurez l'instantané de base de données pris avant la mise à niveau pour créer une nouvelle instance de base de données.

Au cours de la mise à niveau d'une version mineure ou majeure de SQL Server, les métriques Espace de stockage disponible et Profondeur de la file d'attente indiquent `-1`. Une fois la mise à niveau terminée, les deux métriques reviennent à la normale.

Mises à niveau de version majeure.

Amazon RDS prend actuellement en charge les mises à niveau de version majeure suivantes vers une instance de base de données Microsoft SQL Server.

Vous pouvez mettre à jour une instance de base de données existante vers SQL Server 2017 ou 2019 depuis n'importe quelle version, sauf SQL Server 2008. Pour mettre à niveau SQL Server 2008, effectuez d'abord une mise à niveau vers une des autres versions.

Version actuelle	Versions de mise à niveau prises en charge
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	SQL Server 2019 SQL Server 2017 SQL Server 2016 SQL Server 2014
SQL Server 2008 R2 (obsolète)	SQL Server 2016 SQL Server 2014 SQL Server 2012

Vous pouvez utiliser une requête AWS CLI, comme dans l'exemple suivant, pour rechercher les mises à niveau disponibles pour une version particulière du moteur de base de données.

Example

Pour Linux, macOS ou Unix :

```
aws rds describe-db-engine-versions \
    --engine sqlserver-se \
    --engine-version 14.00.3049.1.v1 \
    --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" \
    --output table
```

Pour Windows :

```
aws rds describe-db-engine-versions ^
    --engine sqlserver-se ^
    --engine-version 14.00.3049.1.v1 ^
    --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" ^
    --output table
```

La sortie indique que vous pouvez mettre à niveau la version 14.00.3049.1 vers la dernière version de SQL Server 2017 ou 2019.

```
-------------------------
|DescribeDBEngineVersions|
+------------------------+
|      EngineVersion     |
+------------------------+
|  14.00.3294.2.v1       |
|  15.00.4043.16.v1      |
+------------------------+
```

Niveau de compatibilité de base de données

Vous pouvez utiliser les niveaux de compatibilité de base de données Microsoft SQL Server afin de régler certains comportements de base de données pour imiter les versions précédentes de SQL Server. Pour de plus amples informations, veuillez consulter Niveau de compatibilité dans la documentation de Microsoft.

Lorsque vous mettez à niveau votre instance de base de données, toutes les bases de données existantes restent à leur niveau de compatibilité initial. Par exemple, si vous mettez à niveau SQL Server 2012 vers SQL Server 2014, toutes les bases de données existantes ont le niveau de compatibilité 110. Toute nouvelle base de données créée après la mise à niveau a le niveau de compatibilité 120.

Vous pouvez modifier le niveau de compatibilité d'une base de données en utilisant la commande ALTER DATABASE. Par exemple, pour modifier une base de données nommée `customeracct` afin qu'elle soit compatible avec SQL Server 2014, exécutez la commande suivante :

```
ALTER DATABASE customeracct SET COMPATIBILITY_LEVEL = 120
```

Considérations relatives à l'environnement Multi-AZ et à l'optimisation en mémoire

Amazon RDS prend en charge les déploiements Multi-AZ pour les instances de base de données exécutant Microsoft SQL Server à l'aide de la mise en miroir de bases de données (DBM) ou des groupes de disponibilité (AG) AlwaysOn. Pour de plus amples informations, veuillez consulter Déploiements multi-AZ pour Microsoft SQL Server (p. 664).

Si votre instance de base de données se trouve dans un déploiement multi-AZ, les deux instances de base de données principale et de secours sont mises à niveau. Amazon RDS effectue des mises à niveau propagées. L'interruption n'intervient que pendant la durée d'un basculement.

SQL Server 2014 à 2019 Enterprise Edition prend en charge l'optimisation en mémoire.

Considérations relatives au groupe d'options et de paramètres

Considérations relatives au groupe d'options

Si votre instance de base de données utilise un groupe d'options personnalisé, Amazon RDS ne peut pas toujours attribuer automatiquement un nouveau groupe d'options à votre instance de base de données. Par exemple, lorsque vous procédez à une mise à niveau de version majeure. Dans ce cas, vous devez

spécifier un nouveau groupe d'options pendant la mise à niveau. Nous vous recommandons de créer un nouveau groupe d'options et d'y ajouter les mêmes options qu'à votre groupe d'options personnalisé existant.

Pour de plus amples informations, veuillez consulter Création d'un groupe d'options (p. 212) ou Copie d'un groupe d'options (p. 213).

Considérations relatives au groupe de paramètres

Si votre instance de base de données utilise un groupe de paramètres personnalisé, Amazon RDS ne peut pas toujours attribuer automatiquement un nouveau groupe de paramètres à votre instance de base de données. Par exemple, lorsque vous procédez à une mise à niveau de version majeure. Dans ce cas, vous devez spécifier un nouveau groupe de paramètres pendant la mise à niveau. Nous vous recommandons de créer un nouveau groupe de paramètres et de configurer les mêmes paramètres que ceux de votre groupe de paramètres personnalisé existant.

Pour de plus amples informations, veuillez consulter Création d'un groupe de paramètres de bases de données (p. 227) ou Copie d'un groupe de paramètres de bases de données (p. 231).

Test d'une mise à niveau

Avant d'effectuer une mise à niveau de version majeure sur votre instance de base de données, vous devez tester soigneusement la compatibilité de votre base de données et de toutes les applications qui y accèdent avec la nouvelle version. Nous vous recommandons d'utiliser la procédure suivante.

Pour tester une mise à niveau de version majeure

1. Consultez la mise à niveau de SQL Server dans la documentation Microsoft pour la nouvelle version du moteur de base de données afin de voir s'il existe des problèmes de compatibilité susceptibles d'affecter votre base de données ou vos applications.
2. Si votre instance de base de données utilise un groupe d'options personnalisé, créez un nouveau groupe d'options compatible avec la version vers laquelle vous procédez à la mise à niveau. Pour de plus amples informations, veuillez consulter Considérations relatives au groupe d'options (p. 632).
3. Si votre instance de base de données utilise un groupe de paramètres personnalisé, créez un nouveau groupe de paramètres compatible avec la version vers laquelle vous procédez à la mise à niveau. Pour de plus amples informations, veuillez consulter Considérations relatives au groupe de paramètres (p. 633).
4. Créez un instantané de base de données de l'instance de base de données à mettre à niveau. Pour de plus amples informations, veuillez consulter Création d'un instantané de base de données (p. 327).
5. Restaurez l'instantané de base de données pour créer une nouvelle instance de base de données de test. Pour de plus amples informations, veuillez consulter Restauration à partir d'un instantané de base de données (p. 329).
6. Modifiez cette nouvelle instance de base de données de test pour la mettre à niveau vers la nouvelle version, en utilisant l'une des méthodes suivantes :
   - Console (p. 268)
   - AWS CLI (p. 268)
   - API RDS (p. 269)
7. Évaluez le stockage utilisé par l'instance mise à niveau pour déterminer si la mise à niveau requiert un stockage supplémentaire.
8. Exécutez sur l'instance de base de données mise à niveau autant de tests d'assurance qualité que nécessaire pour garantir que votre base de données et votre application fonctionnent correctement avec la nouvelle version. Implémentez tous les nouveaux tests requis pour évaluer l'impact des éventuels problèmes de compatibilité que vous avez identifiés à l'étape 1. Testez toutes les fonctions

et procédures stockées. Dirigez les versions de test de vos applications vers l'instance de base de données mise à niveau.

9. En cas de succès de tous les tests, effectuez la mise à niveau sur votre instance de base de données de production. Nous vous recommandons de ne pas autoriser les opérations d'écriture sur l'instance de base de données tant que vous n'avez pas confirmé que tout fonctionne correctement.

Mise à niveau d'une instance de base de données SQL Server

Pour de plus amples informations sur la mise à niveau manuelle ou automatique d'une instance de base de données SQL Server, veuillez consulter les ressources suivantes :

- Mise à niveau d'une version du moteur d'une instance de base de données (p. 267)
- Bonnes pratiques de mise à niveau de SQL Server 2008 R2 vers SQL Server 2016 sur Amazon RDS for SQL Server

> **Important**
>
> Si vous avez des instantanés qui sont chiffrés à l'aide de AWS KMS, nous vous recommandons de lancer une mise à niveau avant la fin de la prise en charge.

Mise à niveau des instances de base de données obsolètes avant la fin de la prise en charge

Lorsqu'une version majeure est obsolète, vous ne pouvez pas l'installer sur de nouvelles instances de base de données. RDS va essayer de mettre automatiquement à niveau toutes les instances de base de données existantes.

Si vous devez restaurer une instance de base de données obsolète, vous pouvez effectuer une restauration à un instant donné (PITR) ou restaurer un instantané. Cela vous donne un accès temporaire à une instance de base de données qui utilise la version considérée comme obsolète. Cependant, une fois qu'une version majeure est totalement obsolète, ces instances de base de données sont également automatiquement mises à niveau vers une version prise en charge.

Importation et exportation de bases de données SQL Server

Amazon RDS prend en charge les sauvegarde et restauration natives pour les bases de données Microsoft SQL Server à l'aide de fichiers de sauvegarde complète (fichiers .bak). Lorsque vous utilisez RDS, vous accédez aux fichiers stockés dans Amazon S3 au lieu d'utiliser le système de fichiers local sur le serveur de base de données.

Par exemple, vous pouvez créer une sauvegarde complète depuis votre serveur local, la stocker sur S3, puis la restaurer sur une instance de base de données Amazon RDS existante. Vous pouvez également créer des sauvegardes à partir de RDS, les stocker sur S3, puis les restaurer chaque fois que vous le souhaitez.

La sauvegarde et la restauration natives sont disponibles dans toutes les régions AWS pour les instances de base de données mono-AZ et multi-AZ, y compris les instances de base de données multi-AZ avec

réplicas en lecture. Les sauvegarde et restauration natives sont disponibles pour toutes les éditions de Microsoft SQL Server prises en charge sur Amazon RDS.

Le schéma suivant illustre les scénarios pris en charge.

L'utilisation de fichiers .bak natifs pour sauvegarder et restaurer des bases de données est généralement le moyen le plus rapide de sauvegarder et de restaurer des bases de données. Il existe de nombreux avantages supplémentaires à l'utilisation des sauvegarde et restauration natives. Par exemple, vous pouvez effectuer les opérations suivantes :

- Migrer des bases de données vers ou depuis Amazon RDS.
- Déplacer des bases de données entre des instances de base de données RDS SQL Server.
- Migrer des données, des schémas, des procédures stockées, des déclencheurs et tout autre code de base de données dans des fichiers .bak.
- Sauvegarder et restaurer des bases de données uniques, au lieu de la totalité d'instances de base de données.
- Créer des copies de bases de données à des fins de développement, de test, de formation et de démonstration.
- Stocker et transférer des fichiers de sauvegarde avec Amazon S3, pour offrir une couche de protection supplémentaire pour la reprise après sinistre.

Limitations et recommandations

Voici quelques limitations quant à l'utilisation des sauvegarde et restauration natives :

- Vous ne pouvez effectuer une sauvegarde vers, ou une restauration depuis, un compartiment Amazon S3 dans une autre région AWS que celle de votre instance de base de données Amazon RDS.
- Nous vous recommandons vivement de ne pas restaurer de fichiers de sauvegarde d'un fuseau horaire dans un autre fuseau horaire. Si vous restaurez des sauvegardes d'un fuseau horaire dans un autre fuseau horaire, vous devez auditer vos requêtes et vos applications afin de déterminer les effets du changement de fuseau horaire.

- Amazon S3 a une limite de taille de 5 To par fichier. Pour les sauvegardes natives de bases de données plus volumineuses, vous pouvez utiliser la sauvegarde multifichier.
- La taille maximale de la base de données pouvant être sauvegardée sur S3 dépend de la mémoire disponible, du processeur, des E/S et des ressources réseau sur l'instance de base de données. Plus la base de données est grande, plus l'agent de sauvegarde consomme de la mémoire. Nos tests montrent que vous pouvez effectuer une sauvegarde compressée d'une base de données de 16 To sur nos types d'instance de la nouvelle génération à partir de tailles d'instance `2xlarge` et plus grandes, en disposant de ressources système suffisantes.
- Vous ne pouvez pas effectuer une sauvegarde ou une restauration à partir de plus de 10 fichiers de sauvegarde simultanément.
- Une sauvegarde différentielle est basée sur la dernière sauvegarde complète. Pour que les sauvegardes différentielles fonctionnent, vous ne pouvez prendre un instantané entre la dernière sauvegarde complète et la sauvegarde différentielle. Si vous souhaitez faire une sauvegarde différentielle, mais qu'il existe un instantané manuel ou automatique, créez une autre sauvegarde complète avant de créer la sauvegarde différentielle.
- Les restaurations différentielles et de journaux ne sont pas prises en charge pour les bases de données possédant des fichiers dont l'identifiant unique file_guid est défini sur `NULL`.
- Vous pouvez exécuter jusqu'à deux tâches de sauvegarde ou restauration simultanément.
- Vous ne pouvez pas effectuer de sauvegardes natives de journaux à partir de SQL Server sur Amazon RDS.
- RDS prend en charge les restaurations natives des bases de données allant jusqu'à 16 To. Les restaurations natives des bases de données sur SQL Server Express Edition sont limitées à 10 Go.
- Vous ne pouvez pas sauvegarder une base de données pendant la fenêtre de maintenance, ou à tout moment où Amazon RDS prend un instantané de la base de données. Si une tâche de sauvegarde native se chevauche avec la fenêtre de sauvegarde quotidienne RDS, la tâche de sauvegarde native est annulée.
- Sur des instances de base de données multi-AZ, vous pouvez uniquement restaurer nativement des bases de données sauvegardées en utilisant le modèle de restauration « Full ».
- La restauration à partir de sauvegardes différentielles sur instances multi-AZ n'est pas prise en charge.
- L'appel des procédures RDS pour la sauvegarde/restauration au sein d'une transaction n'est pas pris en charge.
- Utilisez une clé principale client (CMK) AWS KMS symétrique pour chiffrer vos sauvegardes. Amazon RDS ne prend pas en charge les clés CMK asymétriques. Pour de plus amples informations, veuillez consulter Utilisation des clés symétriques et asymétriques dans le AWS Key Management Service Developer Guide.
- Les fichiers de sauvegarde sont chiffrés avec la clé CMK AWS KMS spécifiée à l'aide du mode cryptographique « Chiffrement seul ». Lorsque vous restaurez des fichiers de sauvegarde chiffrés, gardez à l'esprit qu'ils ont été chiffrés à l'aide du mode cryptographique « Chiffrement seul ».
- Vous ne pouvez pas restaurer une base de données contenant un groupe de fichiers FILESTREAM.

Nous vous recommandons d'utiliser les sauvegarde et restauration natives pour migrer votre base de données vers RDS si votre base de données peut être hors connexion pendant que le fichier de sauvegarde est créé, copié et restauré. Si votre base de données sur site ne peut pas être hors connexion, nous vous recommandons d'utiliser AWS Database Migration Service pour migrer votre base de données vers Amazon RDS. Pour de plus amples informations, veuillez consulter Qu'est-ce qu'AWS Database Migration Service ?

Les sauvegarde et restauration natives ne visent pas à remplacer les fonctionnalités de récupération des données de la fonction de copie d'instantané entre régions. Nous vous recommandons d'utiliser une copie d'instantané pour copier l'instantané de votre base de données vers une autre région AWS pour la reprise après sinistre entre régions dans Amazon RDS. Pour plus d'informations, consultez Copie d'un instantané (p. 332).

Configuration pour les sauvegarde et restauration natives

Pour configurer la sauvegarde et la restauration natives, vous avez besoin de trois composants :

1. Un compartiment Amazon S3 pour stocker vos fichiers de sauvegarde.

   Vous devez disposer d'un compartiment S3 pour vos fichiers de sauvegarde et charger les sauvegardes que vous souhaitez migrer vers RDS. Si vous avez déjà un compartiment Amazon S3, vous pouvez l'utiliser. Si vous n'en avez pas, vous pouvez en créer un. Sinon, vous pouvez choisir d'avoir un compartiment créé pour vous quand vous ajoutez l'option `SQLSERVER_BACKUP_RESTORE` à l'aide de AWS Management Console.

   Pour de plus amples informations sur l'utilisation de S3, veuillez consulter le Amazon Simple Storage Service Guide de mise en route pour une présentation succincte. Pour plus de détails, veuillez consulter Amazon Simple Storage Service Guide de l'utilisateur de la console.
2. Un rôle AWS Identity and Access Management (IAM) pour accéder au compartiment.

   Si vous avez déjà un rôle IAM, vous pouvez l'utiliser. Vous pouvez choisir d'avoir un nouveau rôle IAM créé pour vous quand vous ajoutez l'option `SQLSERVER_BACKUP_RESTORE` à l'aide de la AWS Management Console. Vous pouvez également en créer un nouveau manuellement.

   Si vous souhaitez créer un nouveau rôle IAM manuellement, optez pour l'approche abordée à la section suivante. Faites de même si vous souhaitez associer des relations d'approbation et des stratégies d'autorisations à un rôle IAM existant.
3. L'option `SQLSERVER_BACKUP_RESTORE` ajoutée à un groupe d'options sur votre instance de base de données.

   Pour activer les sauvegarde et restauration natives sur votre instance de base de données, vous ajoutez l'option `SQLSERVER_BACKUP_RESTORE` à un groupe d'options sur votre instance de base de données. Pour plus d'informations et des instructions, consultez Prise en charge des sauvegarde et restauration natives dans SQL Server (p. 701).

Création manuelle d'un rôle IAM pour les sauvegarde et restauration natives

Si vous souhaitez créer manuellement un rôle IAM à utiliser avec une sauvegarde native et à restaurer, vous pouvez le faire. Dans ce cas, vous créez un rôle pour déléguer des autorisations depuis le service Amazon RDS vers votre compartiment Amazon S3. Lorsque vous créez un rôle IAM, vous attachez une relation d'approbation et une stratégie d'autorisation. La relation d'approbation permet à RDS d'assumer ce rôle. La stratégie d'autorisation définit les actions que ce rôle peut exécuter. Pour plus d'informations sur la création d'un rôle, consultez Création d'un rôle pour déléguer des autorisations à un service AWS.

Pour la fonction de sauvegarde et restauration native, utilisez des relations d'approbation et des stratégies d'autorisation similaires aux exemples de cette section. Dans l'exemple suivant, nous utilisons le nom principal de service `rds.amazonaws.com` comme alias de tous les comptes de service. Dans les autres exemples, nous spécifions un ARN (Amazon Resource Name) pour identifier un autre compte, utilisateur ou rôle auquel nous accordons l'accès dans la stratégie d'approbation.

Example Relation de confiance pour la sauvegarde et la restauration natives

```
{
    "Version": "2012-10-17",
    "Statement":
```

```
    [{
        "Effect": "Allow",
        "Principal": {"Service":  "rds.amazonaws.com"},
        "Action": "sts:AssumeRole"
    }]
}
```

L'exemple suivant utilise un ARN pour spécifier une ressource. Pour plus d'informations sur l'utilisation des ARN, consultez la section Noms ARN (Amazon Resource Name).

Example Stratégie d'autorisation pour les sauvegarde et restauration natives sans prise en charge du chiffrement

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
        "Effect": "Allow",
        "Action":
            [
                "s3:ListBucket",
                "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/*"
        }
    ]
}
```

Example Stratégie d'autorisation pour les sauvegarde et restauration natives avec prise en charge du chiffrement

Si vous souhaitez chiffrer vos fichiers de sauvegarde, incluez une clé de chiffrement dans votre stratégie d'autorisation. Pour en savoir plus sur les clés de chiffrement, veuillez consulter la section Démarrez dans le AWS Key Management Service Developer Guide.

> **Note**
>
> Vous devez utiliser une clé CMK AWS KMS symétrique pour chiffrer vos sauvegardes. Amazon RDS ne prend pas en charge les clés CMK asymétriques. Pour de plus amples informations, veuillez consulter Utilisation des clés symétriques et asymétriques dans le AWS Key Management Service Developer Guide.
> Le rôle IAM doit également être un utilisateur clé et un administrateur de clé pour la clé CMK AWS KMS, c'est-à-dire qu'il doit être spécifié dans la stratégie de clé. Pour de plus amples informations, veuillez consulter Création de CMK symétriques dans le 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:GetObject",
                "s3:PutObject",
                "s3:ListMultipartUploadParts",
                "s3:AbortMultipartUpload"
            ],
        "Resource": "arn:aws:s3:::bucket_name/*"
        }
    ]
}
```

Utilisation des sauvegarde et restauration natives

Une fois que vous avez activé et configuré les sauvegarde et restauration natives, vous pouvez commencer à les utiliser. Tout d'abord, vous vous connectez à votre base de données Microsoft SQL Server, puis vous appelez une procédure stockée Amazon RDS pour faire le travail. Pour plus d'informations sur la connexion à votre base de données, consultez Connexion à une instance de base de données exécutant le moteur de base de données Microsoft SQL Server (p. 618).

Certaines procédures stockées nécessitent que vous fournissiez un Amazon Resource Name (ARN) à votre compartiment et votre fichier Amazon S3. Le format de votre ARN est `arn:aws:s3:::bucket_name/file_name.extension`. Amazon S3 n'a pas besoin d'un numéro de compte ou d'une région AWS dans les ARN.

Si vous fournissez également une clé principale client (CMK) AWS KMS facultative, le format de l'ARN de la clé est `arn:aws:kms:region:account-id:key/key-id`. Pour de plus amples informations, veuillez consulter Amazon Resource Name (ARN) et espaces de noms de service AWS. Vous devez utiliser une clé CMK AWS KMS symétrique pour chiffrer vos sauvegardes. Amazon RDS ne prend pas en charge les clés CMK asymétriques. Pour de plus amples informations, veuillez consulter Utilisation des clés symétriques et asymétriques dans le AWS Key Management Service Developer Guide.

> **Note**
>
> Que vous utilisiez ou non une clé CMK KMS, les tâches de sauvegarde et de restauration natives activent le chiffrement AES (Advanced Encryption Standard) 256 bits par défaut pour les fichiers téléchargés sur S3.

Pour de plus amples informations sur la façon d'appeler chaque procédure stockée, veuillez consulter les rubriques suivantes :

- Sauvegarde d'une base de données (p. 640)
- Restauration d'une base de données (p. 642)
- Restauration d'un journal (p. 645)
- Finalisation d'une restauration de base de données (p. 647)
- Utilisation de bases de données partiellement restaurées (p. 647)
- Annulation d'une tâche (p. 647)
- Suivi de l'état des tâches (p. 648)

Sauvegarde d'une base de données

Pour sauvegarder votre base de données, utilisez la procédure stockée `rds_backup_database`.

> **Note**
>
> Vous ne pouvez pas sauvegarder une base de données pendant la fenêtre de maintenance ou lorsqu'Amazon RDS prend un instantané.

Utilisation

```
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];
```

Les paramètres suivants sont obligatoires :

- `@source_db_name` – Nom de la base de données à sauvegarder.
- `@s3_arn_to_backup_to` – L'ARN indique le compartiment Amazon S3 à utiliser pour la sauvegarde, ainsi que le nom du fichier de sauvegarde.

  Le fichier peut avoir n'importe quelle extension mais `.bak` est généralement utilisée.

Les paramètres suivants sont facultatifs :

- `@kms_master_key_arn` – ARN de la CMK AWS KMS symétrique à utiliser pour chiffrer l'élément.
  - Vous ne pouvez pas utiliser la clé de chiffrement par défaut. Si vous utilisez la clé par défaut, la base de données n'est pas sauvegardée.
  - Si vous ne spécifiez pas d'identificateur de clé AWS KMS, le fichier de sauvegarde n'est pas chiffré. Pour de plus amples informations, veuillez consulter Chiffrer des ressources Amazon RDS.
  - Lorsque vous spécifiez une clé CMK AWS KMS, le chiffrement côté client est utilisé.
  - Amazon RDS ne prend pas en charge les clés CMK asymétriques. Pour de plus amples informations, veuillez consulter Utilisation des clés symétriques et asymétriques dans le AWS Key Management Service Developer Guide.
- `@overwrite_s3_backup_file` – Une valeur qui indique si un fichier de sauvegarde existant doit être écrasé.
  - `0` – N'écrase pas un fichier existant. Cette valeur est celle par défaut.

Si `@overwrite_s3_backup_file` est défini sur 0, une erreur est retournée si le fichier existe déjà.

- `1` – Écrase le fichier existant qui possède déjà le nom spécifié, même s'il ne s'agit pas d'un fichier de sauvegarde.

- `@type` – Le type de sauvegarde.
  - `DIFFERENTIAL` – Crée une sauvegarde différentielle.
  - `FULL` – Crée une sauvegarde complète. Cette valeur est celle par défaut.

  Une sauvegarde différentielle est basée sur la dernière sauvegarde complète. Pour que les sauvegardes différentielles fonctionnent, vous ne pouvez prendre un instantané entre la dernière sauvegarde complète et la sauvegarde différentielle. Si vous souhaitez faire une sauvegarde différentielle, mais qu'il existe un instantané, alors créez une autre sauvegarde complète avant de créer la sauvegarde différentielle.

  Vous pouvez rechercher la dernière sauvegarde complète ou le dernier instantané à l'aide de l'exemple de requête SQL suivant :

```
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` – Nombre de fichiers dans lesquels la sauvegarde sera divisée (en morceaux). Le nombre maximum est de 10.
  - La sauvegarde en plusieurs fichiers est prise en charge pour les sauvegardes complètes et différentielles.
  - Si vous entrez la valeur 1 ou omettez le paramètre, un seul fichier de sauvegarde est créé.

  Fournissez le préfixe que les fichiers ont en commun, puis ajoutez un astérisque comme suffixe (`*`). L'astérisque peut se trouver n'importe où dans la partie *`nom_fichier`* de l'ARN S3. L'astérisque est remplacé par une série de chaînes alphanumériques dans les fichiers générés, en commençant par `1-of-`*`number_of_files`*.

  Par exemple, si les noms de fichiers dans l'ARN S3 ont pour modèle `backup*.bak` et que vous définissez `@number_of_files=4`, les fichiers de sauvegarde générés auront pour noms `backup1-of-4.bak`, `backup2-of-4.bak`, `backup3-of-4.bak` et `backup4-of-4.bak`.
  - Si l'un des noms de fichier existe déjà et que `@overwrite_s3_backup_file` a pour valeur 0, une erreur est renvoyée.
  - Les sauvegardes sur plusieurs fichiers ne peuvent comporter qu'un seul astérisque dans la partie *`nom_fichier`* de l'ARN S3.
  - Les sauvegardes en un seul fichier peuvent comporter n'importe quel nombre d'astérisques dans la partie *`nom_fichier`* de l'ARN S3. Les astérisques ne sont pas supprimés du nom de fichier généré.

Exemples

Example de sauvegarde différentielle

```
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 de sauvegarde complète avec chiffrement

```
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 de sauvegarde sur plusieurs fichiers

```
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 de sauvegarde différentielle sur plusieurs fichiers

```
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 de sauvegarde sur plusieurs fichiers avec chiffrement

```
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 de sauvegarde sur plusieurs fichiers avec écrasement S3

```
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 de sauvegarde en un seul fichier avec le paramètre @number_of_files

Cet exemple génère un fichier de sauvegarde nommé `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;
```

Restauration d'une base de données

Pour restaurer votre base de données, appelez la procédure stockée `rds_restore_database`. Amazon RDS crée un instantané initial de la base de données après la fin de la tâche de restauration et l'ouverture de la base de données.

Utilisation

```
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'];
```

Les paramètres suivants sont obligatoires :

- `@restore_db_name` – Nom de la base de données à restaurer.
- `@s3_arn_to_restore_from` – L'ARN indique le préfixe Amazon S3 et les noms des fichiers de sauvegarde utilisés pour restaurer la base de données.
  - Pour une seule sauvegarde de fichier, fournissez la totalité du nom du fichier.
  - Pour une sauvegarde comportant plusieurs fichiers, fournissez le préfixe que les fichiers ont en commun, puis ajoutez un astérisque comme suffixe (`*`).
  - Si `@s3_arn_to_restore_from` est vide, le message d'erreur suivant est renvoyé : Le préfixe de l'ARN ne peut pas être vide.

Le paramètre suivant est obligatoire pour les différentes restaurations, mais facultatifs pour les restaurations complètes :

- `@with_norecovery` – La clause de restauration à utiliser pour l'opération de restauration.
  - Définissez le paramètre sur `0` pour restaurer avec RECOVERY (RESTAURATION). Dans ce cas, la base de données est en ligne après la restauration.
  - Définissez le paramètre sur `1` pour restaurer avec NORECOVERY (SANS RESTAURATION). Dans ce cas, la base de données reste à l'état RESTORING (EN COURS DE RESTAURATION) après la fin de la tâche de restauration. Grâce à cette approche, vous pouvez procéder à des restaurations différentielles ultérieurement.
  - Pour les restaurations DIFFÉRENTIELLES, spécifiez `0` ou `1`.
  - Pour les restaurations `FULL`, cette valeur par défaut est `0`.

Les paramètres suivants sont facultatifs :

- `@kms_master_key_arn` – Si vous avez chiffré le fichier de sauvegarde, la clé principale client (CMK) AWS KMS à utiliser pour déchiffrer le fichier.

  Lorsque vous spécifiez une clé CMK AWS KMS, le chiffrement côté client est utilisé.
- `@type` – Le type de restauration. Les types valides sont `DIFFERENTIAL` et `FULL`. La valeur par défaut est `FULL`.

  > **Note**
  >
  > Pour les restaurations différentielles, la base de données doit se trouver en état RESTORING (EN COURS DE RESTAURATION) ou une tâche de restauration doit déjà exister avec NORECOVERY (SANS RESTAURATION).
  > Vous ne pouvez pas restaurer ultérieurement des sauvegardes différentielles tant que la base de données est en ligne.
  > Vous ne pouvez pas envoyer de tâche de restauration pour une base de données qui possède déjà une tâche de restauration en attente avec RECOVERY (RESTAURATION).
  > Les restaurations complètes avec NORECOVERY (SANS RESTAURATION) et les restaurations différentielles ne sont pas prises en charge sur les instances multi-AZ.

La restauration d'une base de données sur une instance multi-AZ avec réplicas en lecture est similaire à la restauration d'une base de données sur une instance multi-AZ. Vous n'avez pas besoin d'effectuer d'actions supplémentaires pour restaurer une base de données sur un réplica.

Exemples

Example de restauration d'un seul fichier

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup1.bak';
```

Example de restauration de plusieurs fichiers

Pour éviter les erreurs lors de la restauration de plusieurs fichiers, assurez-vous que tous les fichiers de sauvegarde ont le même préfixe et qu'aucun autre fichier n'utilise ce préfixe.

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup*';
```

Example de restauration de base de données complète avec RECOVERY (RESTAURATION)

Les trois exemples suivants exécutent la même tâche de restauration complète avec RECOVERY (RESTAURATION).

```
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 de restauration de base de données complète avec chiffrement

```
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 de restauration de base de données complète avec NORECOVERY (SANS RESTAURATION)

```
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 de restauration différentielle avec NORECOVERY (SANS RESTAURATION)

```
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 de restauration différentielle avec RECOVERY (RESTAURATION).

```
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;
```

Restauration d'un journal

Pour restaurer votre journal, appelez la procédure stockée `rds_restore_log`.

Utilisation

```
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'];
```

Les paramètres suivants sont obligatoires :

- `@restore_db_name` – Le nom de la base de données dont vous souhaitez restaurer le journal.
- `@s3_arn_to_restore_from` – L'ARN indique le préfixe Amazon S3 et le nom du fichier journal utilisé pour restaurer le journal. Le fichier peut avoir n'importe quelle extension mais `.trn` est généralement utilisée.

  Si `@s3_arn_to_restore_from` est vide, le message d'erreur suivant est renvoyé : Le préfixe de l'ARN ne peut pas être vide.

Les paramètres suivants sont facultatifs :

- `@kms_master_key_arn` – Si vous avez chiffré le journal, la clé principale client (CMK) AWS KMS à utiliser pour déchiffrer le journal.
- `@with_norecovery` – La clause de restauration à utiliser pour l'opération de restauration. La valeur par défaut est `1`.
  - Définissez le paramètre sur `0` pour restaurer avec RECOVERY (RESTAURATION). Dans ce cas, la base de données est en ligne après la restauration. Vous ne pouvez pas restaurer ultérieurement des sauvegardes de journaux tant que la base de données est en ligne.
  - Définissez le paramètre sur `1` pour restaurer avec NORECOVERY (SANS RESTAURATION). Dans ce cas, la base de données reste à l'état RESTORING (EN COURS DE RESTAURATION) après la fin de la tâche de restauration. Grâce à cette approche, vous pouvez procéder à des restaurations de journaux ultérieurement.

- `@stopat` – Une valeur qui spécifie que la base de données est restaurée dans son état à la date et l'heure spécifiées (au format datetime). Seul les enregistrements de journaux de transaction écrits avant la date et l'heure spécifiées sont appliqués à la base de données.

  Si ce paramètre n'est pas spécifié (il est NULL), le journal complet est restauré.

  > **Note**
  >
  > Pour les restaurations de journaux, la base de données doit se trouver en état de restauration ou une tâche de restauration doit déjà exister avec NORECOVERY (SANS RESTAURATION).
  > Vous ne pouvez pas restaurer de sauvegardes de journaux tant que la base de données est en ligne.
  > Vous ne pouvez pas envoyer de tâche de restauration de journaux sur une base de données qui possède déjà une tâche de restauration en attente avec RECOVERY (RESTAURATION).
  > Les restaurations de journaux ne sont pas prises en charge sur les instances multi-AZ.

Exemples

Example de restaurations de journaux

```
exec msdb.dbo.rds_restore_log
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/mylog.trn';
```

Example de restaurations de journaux avec chiffrement

```
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 de restaurations de journaux avec NORECOVERY (SANS RESTAURATION)

Les trois exemples suivants exécutent la même tâche de restauration de journaux avec NORECOVERY (SANS RESTAURATION).

```
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 de restaurations de journaux avec RECOVERY (RESTAURATION)

```
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 de restaurations de journaux avec clause STOPAT

```
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';
```

Finalisation d'une restauration de base de données

Si la dernière tâche de restauration sur la base de données a été exécutée à l'aide de `@with_norecovery=1`, la base de données est désormais en état RECOVERY (RESTAURATION). Ouvrez cette base de données pour exécuter des opérations normales à l'aide de la procédure stockée `rds_finish_restore`.

Utilisation

```
exec msdb.dbo.rds_finish_restore @db_name='database_name';
```

> **Note**
>
> Pour utiliser cette approche, la base de données doit être en état RECOVERY (RESTAURATION) sans aucune tâche de restauration en attente.
> La procédure `rds_finish_restore` n'est pas prise en charge sur les instances multi-AZ.
> Pour finaliser la restauration de la base de données, utilisez l'identifiant principal. Ou utilisez l'identifiant utilisateur qui a permis de restaurer récemment la base de données ou de se connecter avec NORECOVERY (SANS RESTAURATION).

Utilisation de bases de données partiellement restaurées

Suppression d'une base de données partiellement restaurée

Pour supprimer une base de données partiellement restaurée (laissée en état RECOVERY (RESTAURATION), utilisez la procédure stockée `rds_drop_database`.

```
exec msdb.dbo.rds_drop_database @db_name='database_name';
```

> **Note**
>
> Vous ne pouvez pas envoyer de demande de base de données DROP (SUPPRIMER) pour une base de données qui possède déjà une tâche de restauration en attente ou de finalisation de restauration.
> Pour supprimer la base de données, utilisez l'identifiant principal. Ou utilisez l'identifiant utilisateur qui a permis de restaurer récemment la base de données ou de se connecter avec NORECOVERY (SANS RESTAURATION).

Restauration d'instantané et comportement de restauration à un instant dans le passé pour les bases de données partiellement restaurées

Les bases de données partiellement restaurées dans l'instance source (laissée en état RECOVERY (RESTAURATION) sont supprimées de l'instance cible lors de la restauration d'instantané et la restauration à un instant dans le passé.

Annulation d'une tâche

Pour annuler une tâche de sauvegarde ou de restauration, appelez la procédure stockée `rds_cancel_task`.

Note

Vous ne pouvez pas annuler une tâche FINISH_RESTORE.

Utilisation

```
exec msdb.dbo.rds_cancel_task @task_id=ID_number;
```

Les paramètres suivants sont obligatoires :

- `@task_id` – ID de la tâche à annuler. Vous pouvez obtenir l'ID de la tâche en appelant `rds_task_status`.

Suivi de l'état des tâches

Pour suivre l'état de vos tâches de sauvegarde et restauration, appelez la procédure stockée `rds_task_status`. Si vous ne fournissez pas de paramètre, la procédure stockée retourne l'état de toutes les tâches. Le statut des tâches est mis à jour environ toutes les deux minutes. L'historique des tâches est conservé pendant 36 jours.

Utilisation

```
exec msdb.dbo.rds_task_status
 [@db_name='database_name'],
 [@task_id=ID_number];
```

Les paramètres suivants sont facultatifs :

- `@db_name` – Nom de la base de données pour laquelle afficher l'état de la tâche.
- `@task_id` – ID de la tâche pour laquelle afficher l'état de tâche.

Exemples

Example de liste des statuts d'une tâche spécifique

```
exec msdb.dbo.rds_task_status @task_id=5;
```

Example de liste des statuts d'une base de données et d'une tâche spécifiques

```
exec msdb.dbo.rds_task_status
@db_name='my_database',
@task_id=5;
```

Example de liste de toutes les tâches et de leurs statuts sur une base de données spécifique

```
exec msdb.dbo.rds_task_status @db_name='my_database';
```

Example de liste de toutes les tâches et de leurs statuts sur l'instance actuelle

```
exec msdb.dbo.rds_task_status;
```

Réponse

La procédure stockée `rds_task_status` renvoie les colonnes suivantes.

Colonne	Description
`task_id`	ID de la tâche

`task_type`	Le type de tâche dépend des paramètres d'entrée, comme suit :
	• Pour les tâches de sauvegarde :
	  • BACKUP_DB – Sauvegarde de base de données complète
	  • BACKUP_DB_DIFFERENTIAL – Sauvegarde de base de données différentielle
	• Pour les tâches de restauration :
	  • RESTORE_DB – Restauration de base de données complète avec RECOVERY (RESTAURATION)
	  • RESTORE_DB_NORECOVERY – Restauration de base de données complète avec NORECOVERY (SANS RESTAURATION)
	  • RESTORE_DB_DIFFERENTIAL – Restauration de base de données différentielle avec RECOVERY (RESTAURATION)
	  • RESTORE_DB_DIFFERENTIAL_NORECOVERY – Restauration de base de données différentielle avec NORECOVERY (SANS RESTAURATION)
	  • RESTORE_DB_LOG – Restauration de journaux avec RECOVERY (RESTAURATION)
	  • RESTORE_DB_LOG_NORECOVERY – Restauration de journaux avec NORECOVERY (SANS RESTAURATION)
	• Pour les tâches qui finalisent une restauration :
	  • FINISH_RESTORE – Finalisation de restauration et ouverture de base de données
	
	Amazon RDS crée un instantané initial de la base de données après son ouverture à la fin des tâches de restauration suivantes :
	• RESTORE_DB
	• RESTORE_DB_DIFFERENTIAL
	• RESTORE_DB_LOG
	• FINISH_RESTORE

`database_name`	Nom de la base de données à laquelle est associée à la tâche.
`% complete`	La progression de la tâche sous forme de pourcentage.
`duration (mins)`	Temps consacré à la tâche, en minutes.
`lifecycle`	État de la tâche. Les statuts possibles sont les suivants : • `CREATED` – Dès que vous appelez `rds_backup_database` ou `rds_restore_database`, une tâche est créée et l'état est défini sur `CREATED`. • `IN_PROGRESS` – Après le démarrage d'une tâche de sauvegarde ou de restauration, l'état est défini sur `IN_PROGRESS`. Cela peut prendre jusqu'à 5 minutes pour que l'état change de `CREATED` à `IN_PROGRESS`. • `SUCCESS` – Après l'achèvement d'une tâche de sauvegarde ou de restauration, l'état est défini sur `SUCCESS`.

Colonne	Description
	• `ERROR` – En cas d'échec d'une tâche de sauvegarde ou de restauration, l'état est défini sur`ERROR`. Lisez la colonne `task_info` pour plus d'informations sur l'erreur. • `CANCEL_REQUESTED` – Dès que vous appelez `rds_cancel_task`, l'état de la tâche est défini sur `CANCEL_REQUESTED`. • `CANCELLED` – Une fois une tâche annulée avec succès, l'état de la tâche est défini sur `CANCELLED`.
`task_info`	Informations supplémentaires sur la tâche. Si une erreur se produit lors de la sauvegarde ou de la restauration d'une base de données, cette colonne contient des informations sur l'erreur. Pour obtenir une liste des erreurs possibles et des stratégies d'atténuation, consultez Dépannage (p. 651).
`last_updated`	Date et heure de la dernière mise à jour de l'état de la tâche. Le statut est mis à jour tous les 5 pour cent de progression.
`created_at`	Date et heure de création de la tâche.
`S3_object_arn`	L'ARN indique le préfixe Amazon S3 et le nom du fichier en cours de sauvegarde ou de restauration.
`overwrite_s3_backup_file`	Valeur du paramètre `@overwrite_s3_backup_file` spécifié lorsque vous appelez une tâche de sauvegarde. Pour plus d'informations, consultez Sauvegarde d'une base de données (p. 640).
`KMS_master_key_arn`	L'ARN pour la clé CMK AWS KMS utilisée pour le chiffrement (pour la sauvegarde) et le déchiffrement (pour la restauration).
`filepath`	Non applicable aux tâches de sauvegarde et de restauration natives
`overwrite_file`	Non applicable aux tâches de sauvegarde et de restauration natives

Compression des fichiers de sauvegarde

Pour économiser de l'espace sur votre compartiment Amazon S3, vous pouvez compresser vos fichiers de sauvegarde. Pour plus d'informations sur la compression de fichiers de sauvegarde, consultez Backup Compression (Compression de sauvegarde) dans la documentation Microsoft.

La compression des fichiers sauvegardés est prise en charge pour les éditions de base de données suivantes :

- Configurer SQL Server Enterprise Edition
- Microsoft SQL Server Standard Edition

Pour activer la compression de vos fichiers sauvegardés, exécutez le code suivant :

```
exec rdsadmin..rds_set_configuration 'S3 backup compression', 'true';
```

Pour désactiver la compression de vos fichiers sauvegardés, exécutez le code suivant :

```
exec rdsadmin..rds_set_configuration 'S3 backup compression', 'false';
```

Dépannage

Voici les problèmes que vous risquez de rencontrer lorsque vous utilisez la sauvegarde et la restauration natives.

Problème	Suggestions de dépannage
`Access Denied`	Le processus de sauvegarde ou de restauration ne parvient pas à accéder au fichier de sauvegarde. Cela est généralement provoqué par des problèmes tels que : • Référencement du compartiment incorrect. Référencement du compartiment avec un format incorrect. Référencement d'un nom de fichier sans utiliser l'ARN. • Autorisations incorrectes sur le fichier de compartiment. Par exemple, s'il a été créé par un compte différent qui essaie d'y accéder actuellement, ajoutez les autorisations correctes. • Une stratégie IAM incorrecte ou incomplète. Votre rôle IAM doit inclure tous les éléments nécessaires, y compris, par exemple, la version correcte. Ceux-ci sont mis en évidence dans Importation et exportation de bases de données SQL Server (p. 634).
`BACKUP DATABASE WITH COMPRESSION isn't supported on <edition_name> Edition`	La compression des fichiers de sauvegarde est uniquement prise en charge pour Microsoft SQL Server Enterprise Edition. La Standard Edition. Pour plus d'informations, consultez Compression des fichiers de sauvegarde (p. 650).
`Key <ARN> does not exist`	Vous avez essayé de restaurer une sauvegarde chiffrée, mais n'avez pas fourni une clé de chiffrement valide. Vérifiez votre clé de chiffrement et réessayez. Pour plus d'informations, consultez Restauration d'une base de données (p. 642).
`Please reissue task with correct type and overwrite property`	Si vous essayez de sauvegarder votre base de données et fournissez le nom d'un fichier qui existe déjà, mais que la propriété de remplacement est définie sur false, l'opération de sauvegarde échoue. Pour corriger cette erreur, entrez le nom d'un fichier qui n'existe pas déjà ou définissez la propriété de remplacement sur true. Pour plus d'informations, consultez Sauvegarde d'une base de données (p. 640). Il est également possible qu'en tentant de restaurer votre base de données, vous ayez accidentellement appelé la procédure stockée `rds_backup_database`. Dans ce cas, appelez la procédure stockée `rds_restore_database` à la place. Pour plus d'informations, consultez Restauration d'une base de données (p. 642). Si vous aviez pour but de restaurer votre base de données et avez appelé la procédure stockée `rds_restore_database`, assurez-vous que vous avez fourni le nom d'un fichier de sauvegarde valide.

Problème	Suggestions de dépannage
	Pour plus d'informations, consultez Utilisation des sauvegarde et restauration natives (p. 639).
`Please specify a bucket that is in the same region as RDS instance`	Vous ne pouvez effectuer une sauvegarde vers, ou une restauration depuis, un compartiment Amazon S3 dans une autre région AWS que celle de votre instance de base de données Amazon RDS. Utilisez la réplication d'Amazon S3 pour copier le fichier de sauvegarde vers la bonne région AWS. Pour plus d'informations, consultez Réplication entre régions dans la documentation Amazon S3.
`The specified bucket does not exist`	Vérifiez que vous avez fourni l'ARN correct pour votre compartiment et le fichier, dans le bon format. Pour plus d'informations, consultez Utilisation des sauvegarde et restauration natives (p. 639).
`User <ARN> is not authorized to perform <kms action> on resource <ARN>`	Vous avez demandé à une opération chiffrée, mais n'avez pas fourni d'autorisations AWS KMS correctes. Vérifiez que vous avez les autorisations appropriées ou ajoutez-les. Pour de plus amples informations, veuillez consulter Configuration pour les sauvegarde et restauration natives (p. 637).
`The Restore task is unable to restore from more than 10 backup file(s). Please reduce the number of files matched and try again.`	Réduisez le nombre de fichiers utilisés pour la restauration. Si nécessaire, vous pouvez augmenter la taille de chaque fichier.

Importation et exportation de données SQL Server à l'aide d'autres méthodes

Par la suite, vous trouverez des informations sur l'utilisation d'instantanés pour importer vos données Microsoft SQL Server vers Amazon RDS. Vous trouverez également des informations sur l'utilisation d'instantanés pour exporter vos données depuis une instance de base de données RDS exécutant SQL Server.

Si votre scénario le prend en charge, il est plus facile transférer des données vers et depuis Amazon RDS à l'aide de la fonctionnalité de sauvegarde et restauration natives. Pour plus d'informations, consultez Importation et exportation de bases de données SQL Server (p. 634).

> **Note**
>
> Amazon RDS pour Microsoft SQL Server ne prend pas en charge l'importation de données vers la base de données `msdb`.

Importation de données dans SQL Server sur Amazon RDS à l'aide d'un instantané

Pour importer des données dans une instance de base de données SQL Server à l'aide d'un instantané

1. Créez une instance de base de données. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).
2. Arrêtez l'accès des applications à l'instance de base de données de destination.

   Si vous empêchez l'accès à votre instance de base de données pendant l'importation des données, le transfert de données est plus rapide. En outre, vous n'aurez plus à vous inquiéter de conflits pendant le chargement de données si d'autres applications ne peuvent pas écrire sur l'instance de base de données simultanément. En cas de problème, et si vous devez procéder à une restauration vers un instantané de base de données antérieur, les seules modifications que vous perdez sont les données importées. Vous pouvez importer à nouveau ces données après avoir résolu le problème.

   Pour plus d'informations sur le contrôle de l'accès à votre instance de base de données, consultez Utilisation des groupes de sécurité DB (plateforme EC2-Classic) (p. 1596).
3. Créez un instantané de la base de données cible.

   Si la base de données cible contient déjà des données, nous vous recommandons de prendre un instantané de la base de données avant d'importer les données. En cas de problème d'importation des données ou si vous souhaitez ignorer les modifications, l'instantané vous permet de restaurer l'état précédent de la base de données. Pour de plus amples informations sur les instantanés de base de données, veuillez consulter Création d'un instantané de base de données (p. 327).

   > Note
   >
   > Lorsque vous prenez un instantané de base de données, les opérations E/S vers la base de données sont suspendues pendant un moment (millisecondes) pendant la progression de la sauvegarde.
4. Désactivez les sauvegardes automatiques sur la base de données cible.

   La désactivation des sauvegardes automatiques sur l'instance de base de données cible améliore la performance pendant l'importation de vos données, car Amazon RDS ne consigne pas de transactions lorsque les sauvegardes automatiques sont désactivées. Cependant, certains éléments sont à prendre en compte. Les sauvegardes automatiques sont obligatoires pour exécuter une restauration à un instant dans le passé. Ainsi, vous ne pouvez pas restaurer la base de données à un instant spécifique dans le passé tant que vous importez des données. En outre, toutes les sauvegardes automatiques qui ont été créées sur l'instance de base de données sont effacées à moins que vous choisissiez de les conserver.

   Si vous choisissez de conserver les sauvegardes automatiques, vous évitez la suppression accidentelle des données. Amazon RDS enregistre également les propriétés de l'instance de base de données avec chaque sauvegarde automatique afin de faciliter la récupération. Cette option vous permet de restaurer une instance de base de données supprimée à un moment donné dans le cadre de la période de conservation des sauvegardes, y compris après sa suppression. Les sauvegardes automatisées sont automatiquement supprimées à la fin de la plage de sauvegarde spécifiée, comme pour une instance de base de données active.

   Vous pouvez également utiliser des instantanés précédents pour récupérer la base de données. En outre, tous les instantanés que vous avez pris demeureront disponibles. Pour plus d'informations sur les sauvegardes automatiques, consultez Utilisation des sauvegardes (p. 317).
5. Désactivez les contraintes de clé étrangère, le cas échéant.

Si vous avez besoin de désactiver des contraintes de clé étrangère, vous pouvez utiliser pour cela le script suivant.

```
--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. Abandonnez les index, le cas échéant.
7. Désactivez les déclencheurs, le cas échéant.

   Si vous avez besoin de désactiver des déclencheurs, vous pouvez utiliser pour cela le script suivant.

```
--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. Interrogez l'instance SQL Server source pour tous les ID de connexion que vous souhaitez importer dans l'instance de base de données de destination.

SQL Server stocke des ID de connexion et des mots de passe dans la base de données `master`. Du fait que Amazon RDS n'accorde pas l'accès à la base de données `master`, vous ne pouvez pas importer directement des ID de connexion et des mots de passe dans votre instance de base de données de destination. À la place, vous devez interroger la base de données `master` sur l'instance SQL Server source pour générer un fichier Langage de définition de données (DDL). Ce fichier doit inclure tous les identifiants et les mots de passe que vous souhaitez ajouter à l'instance de base de données de destination. Ce fichier doit également inclure des appartenances à un rôle et des autorisations que vous souhaitez transférer.

Pour de plus amples informations sur la manière d'interroger la base de données `master`, veuillez consulter Comment faire pour transférer des noms d'accès et des mots de passe entre instances de SQL Server 2005 et SQL Server 2008 dans la base de connaissances Microsoft.

Le résultat du script est un script que vous pouvez exécuter sur l'instance de base de données de destination. Le script dans l'article de base de connaissances comporte le code suivant :

```
p.type IN
```

Partout où `p.type` s'affiche, utilisez plutôt le code suivant :

```
p.type = 'S'
```

9. Importez les données à l'aide de la méthode dans Importer les données (p. 656).
10. Accordez aux applications l'accès à l'instance de base de données cible.

    Lorsque l'importation de vos données est terminée, vous pouvez accorder l'accès à l'instance de base de données aux applications que vous avez bloquées pendant l'importation. Pour plus d'informations sur le contrôle de l'accès à votre instance de base de données, consultez Utilisation des groupes de sécurité DB (plateforme EC2-Classic) (p. 1596).
11. Activez les sauvegardes automatiques sur l'instance de base de données cible.

    Pour de plus amples informations sur les sauvegardes automatiques, veuillez consulter Utilisation des sauvegardes (p. 317).
12. Activer les contraintes de clé étrangère.

    Si vous avez désactivé les contraintes de clé étrangère précédemment, vous pouvez à présent les activer avec le script suivant.

```
--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. Activez les index, le cas échéant.
14. Activez les déclencheurs, le cas échéant.

Si vous avez désactivé les déclencheurs précédemment, vous pouvez à présent les activer avec le script suivant.

```
--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;
```

Importer les données

Microsoft SQL Server Management Studio est un client SQL Server graphique qui est inclus dans toutes les éditions de Microsoft SQL Server, sauf Express Edition. SQL Server Management Studio Express est disponible auprès de Microsoft en téléchargement gratuit. Pour trouver ce téléchargement, consultez le site Web de Microsoft.

> **Note**
>
> SQL Server Management Studio Express est disponible uniquement en tant qu'application basée sur Microsoft.

SQL Server Management Studio inclut les outils suivants, qui sont utiles pour l'importation de données dans une instance de base de données SQL Server :

- Assistant de génération et de publication de scripts
- Assistant d'importation et d'exportation
- Copie en bloc

Assistant de génération et de publication de scripts

L'assistant de génération et de publication de scripts crée un script qui contient le schéma d'une base de données, les données elles-mêmes, ou les deux. Vous pouvez générer un script pour une base de données dans votre déploiement SQL Server local. Vous pouvez ensuite exécuter le script pour transférer les informations qu'il contient vers une instance de base de données Amazon RDS.

> **Note**
>
> Pour les bases de données d'1 GiB ou plus, il est plus efficace de scripter uniquement le schéma de la base de données. Ensuite, vous utilisez l'assistant d'importation et d'exportation ou la fonctionnalité de copie en bloc de SQL Server pour transférer les données.

Pour plus d'informations sur l'assistant de génération et de publication de scripts, consultez la documentation Microsoft SQL Server.

Dans l'assistant, prêtez une attention particulière aux options avancées sur la page Définir les options de script pour garantir que tout ce que vous souhaitez que votre script inclue soit sélectionné. Par exemple, par défaut, les déclencheurs de base de données ne sont pas inclus dans le script.

Lorsque le script est généré et enregistré, vous pouvez utiliser SQL Server Management Studio pour vous connecter à votre instance de base de données puis exécuter le script.

Assistant d'importation et d'exportation

L'assistant d'importation et d'exportation crée un package Integration Services spécial que vous pouvez utiliser pour copier des données depuis votre base de données SQL Server locale vers l'instance de base de données de destination. L'assistant peut filtrer les tables et même les tuples dans une table qui sont copiés vers l'instance de base de données de destination.

> **Note**
>
> L'assistant d'importation et d'exportation est efficace pour les jeux de données de grande taille, mais ce n'est peut-être pas la manière la plus rapide d'exporter des données à distance depuis votre déploiement local. Pour une manière encore plus rapide, envisagez la fonction de copie en bloc SQL Server.

Pour plus d'informations sur l'assistant d'importation et d'exportation, consultez la documentation Microsoft SQL Server.

Dans l'assistant, sur la page Choose a Destination (Choisir une destination), procédez comme suit :

- Pour Server Name (Nom de serveur), saisissez le nom du point de terminaison pour votre instance de base de données.
- Pour le mode d'authentification de serveur, sélectionnez Use SQL Server Authentication (Utiliser l'authentification SQL Server).
- Pour Nom d'utilisateur et Mot de passe, entrez les informations d'identification pour l'utilisateur principal que vous avez créé pour l'instance de base de données.

Copie en bloc

La fonction Copie en bloc de SQL Server est un moyen efficace de copier des données depuis une base de données source vers votre instance de base de données. La copie en bloc écrit les données que vous spécifiez vers un fichier de données, tel qu'un fichier ASCII. Vous pouvez ensuite exécuter à nouveau la copie en bloc pour écrire le contenu du fichier dans l'instance de base de données de destination.

Cette section utilise l'utilitaire bcp qui est inclus dans toutes les éditions de SQL Server. Pour plus d'informations sur les opérations d'importation et d'exportation en bloc, consultez la documentation Microsoft SQL Server.

> **Note**
>
> Avant d'utiliser la copie en bloc, vous devez importer votre schéma de base de données vers l'instance de base de données de destination. L'assistant de génération et de publication de scripts, décrit plus tôt dans cette rubrique, est un excellent outil à cette fin.

La commande suivante se connecte à l'instance SQL Server locale. Elle génère un fichier délimité par des tabulations d'une table spécifique dans le répertoire racine C:\ de votre déploiement SQL Server existant. La table est spécifiée par son nom entièrement qualifié, et le fichier texte a le même nom que la table qui est copiée.

```
bcp dbname.schema_name.table_name out C:\table_name.txt -n -S localhost -U username -
P password -b 10000
```

Le code précédent inclut les options suivantes :

- `-n` spécifie que la copie en bloc utilise les types de données natifs des données à copier.
- `-S` spécifie l'instance SQL Server à laquelle l'utilitaire bcp se connecte.
- `-U` spécifie le nom d'utilisateur du compte qui se connecte à l'instance SQL Server.
- `-P` spécifie le mot de passe pour l'utilisateur spécifié par `-U`.
- `-b` spécifie le nombre de lignes par lot de données importées.

> **Note**
>
> Il peut exister d'autres paramètres qui sont importants pour votre situation d'importation. Par exemple, vous pouvez avoir besoin du paramètre `-E` qui concerne les valeurs d'identité. Pour plus d'informations, consultez la description complète de la syntaxe de ligne de commande pour l'utilitaire bcp dans la documentation Microsoft SQL Server.

Prenons l'exemple d'une base de données nommée `store` qui utilise le schéma par défaut, `dbo`, et qui contient une table nommée `customers`. Le compte utilisateur `admin`, avec le mot de passe `insecure`, copie 10 000 lignes de la table `customers` dans un fichier nommé `customers.txt`.

```
bcp store.dbo.customers out C:\customers.txt -n -S localhost -U admin -P insecure -b 10000
```

Après avoir généré le fichier de données, vous pouvez charger les données sur votre instance de base de données à l'aide d'une commande similaire. Au préalable, créez la base de données et le schéma sur l'instance de base de données cible. Ensuite, utiliser l'argument `in` pour spécifier un fichier d'entrée au lieu de `out` pour spécifier un fichier de sortie. Au lieu d'utiliser l'hôte local pour spécifier l'instance SQL Server locale, vous spécifiez le point de terminaison de votre instance de base de données. Si vous utilisez un port autre que 1433, vous le spécifiez également. Le nom d'utilisateur et le mot de passe sont identiques à l'utilisateur principal et au mot de passe de votre instance de base de données. La syntaxe est la suivante.

```
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
```

Pour poursuivre l'exemple précédent, supposons que le nom d'utilisateur maître soit `admin`, et que le mot de passe soit `insecure`. Le point de terminaison pour l'instance de base de données est `rds.ckz2kqd4qsn1.us-east-1.rds.amazonaws.com`, et vous utilisez le port 4080. La commande est la suivante.

```
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
```

Exportation de données depuis SQL Server sur Amazon RDS

Vous pouvez choisir l'une des options suivantes pour exporter des données à partir d'une instance de base de données RDS SQL Server :

- Sauvegarde et restauration natives à l'aide d'un fichier de sauvegarde complète (.bak) – L'utilisation de fichiers .bak pour sauvegarder des bases de données est fortement optimisée et constitue généralement

le moyen le plus rapide d'exporter des données. Pour plus d'informations, consultez Importation et exportation de bases de données SQL Server (p. 634).

- Assistant d'importation et d'exportation SQL Server – Pour plus d'informations, consultez Assistant d'importation et d'exportation SQL Server (p. 659).
- Assistant de génération et de publication de scripts SQL Server et utilitaire bcp – Pour plus d'informations, consultez Assistant Générer et publier des scripts et utilitaire bcp (p. 660).

Assistant d'importation et d'exportation SQL Server

Vous pouvez utiliser l'assistant d'importation et d'exportation SQL Server pour copier une ou plusieurs tables, vues ou requêtes depuis votre instance de base de données RDS SQL Server vers un autre magasin de données. Ce choix est le meilleur si le magasin de données cible n'est pas SQL Server. Pour plus d'informations, consultez la section relative à l'Assistant d'importation et exportation SQL Server dans la documentation Microsoft SQL Server.

L'assistant d'importation et d'exportation SQL Server est disponible dans le cadre de Microsoft SQL Server Management Studio. Ce client SQL Server graphique est inclus dans toutes les éditions de Microsoft SQL Server, sauf Express Edition. SQL Server Management Studio Express est disponible uniquement en tant qu'application basée sur Microsoft. SQL Server Management Studio Express est disponible auprès de Microsoft en téléchargement gratuit. Pour trouver ce téléchargement, consultez le site Web de Microsoft.

Pour utiliser l'assistant d'importation et d'exportation SQL Server pour exporter des données

1. Dans SQL Server Management Studio, connectez-vous à votre instance de base de données RDS SQL Server. Pour plus d'informations sur la manière de procéder, consultez Connexion à une instance de base de données exécutant le moteur de base de données Microsoft SQL Server (p. 618).
2. Dans Object Explorer (Navigateur d'objet), développez Databases (Bases de données), ouvrez le menu contextuel (clic droit) pour la base de données source, et sélectionnez Tasks (Tâches), puis Export Data (Exporter des données). L'assistant s'affiche.
3. Sur la page Choose a Data Source (Choisir une source de données), procédez comme suit :
   a. Pour Data source (Source de données), choisissez **`SQL Server Native Client 11.0`**.
   b. Vérifiez que le Server name (Nom du serveur) affiche le point de terminaison de votre instance de base de données RDS SQL Server.
   c. Sélectionnez Use SQL Server Authentication (Utiliser l'authentification SQL Server). Pour Nom d'utilisateur et Mot de passe, saisissez l'identifiant principal et le mot de passe de votre base de données Amazon RDS SQL.
   d. Vérifiez que la zone Base de données affiche la base de données depuis laquelle vous souhaitez exporter des données.
   e. Choisissez Suivant.
4. Sur la page Choose a Destination (Choisir une destination), procédez comme suit :
   a. Pour Destination, choisissez **`SQL Server Native Client 11.0`**.

      Note

      D'autres sources de données cibles sont disponibles. Elles incluent les suivantes : les fournisseurs de données .NET Framework, les fournisseurs OLE DB, les fournisseurs SQL Server Native Client, les fournisseurs ADO.NET, Microsoft Office Excel, Microsoft Office Access et la source du fichier plat. Si vous choisissez de cibler l'une de ces sources de données, ignorez le reste de l'étape 4. Pour obtenir des détails sur les informations de connexion à fournir ensuite, veuillez consulter Choix d'une destination dans la documentation SQL Server.

   b. Pour Server name (Nom de serveur), saisissez le nom du serveur de l'instance de base de données SQL Server cible.
   c. Choisissez le type d'authentification qui convient. Saisissez un nom d'utilisateur et un mot de passe si nécessaire.
   d. Pour Base de données, choisissez le nom de base de données cible, ou sélectionnez Nouveau pour créer une base de données qui contiendra les données exportées.

      Si vous choisissez Nouveau, consultez Créer une base de données dans la documentation SQL Server pour obtenir des renseignements sur les informations de base de données à fournir.
   e. Choisissez Suivant.
5. Sur la page Table Copy or Query (Copie ou requête de tableau), choisissez Copy data from one or more tables or views (Copier des données à partir d'un ou plusieurs tableaux ou affichages) ou Write a query to specify the data to transfer (Rédiger une requête pour spécifier les données à transférer). Choisissez Suivant.
6. Si vous avez choisi Write a query to specify the data to transfer (Rédiger une requête pour spécifier les données à transférer), vous voyez la page Provide a Source Query (Fournir une requête source). Saisissez ou collez une requête SQL, puis choisissez Parse (Analyser) pour la vérifier. Après la validation de la requête, choisissez Suivant.
7. Sur la page Select Source Tables and Views (Sélectionner les tableaux et affichages source), procédez comme suit :
   a. Sélectionnez les tables et les affichages que vous souhaitez exporter, ou bien vérifiez que la requête que vous avez fournie est sélectionnée.
   b. Choisissez Edit Mappings (Modifier le mappage) puis spécifiez les informations de mappage de la colonne et de la base de données. Pour de plus amples informations, veuillez consulter Mapping de colonnes (Mappage des colonnes) dans la documentation SQL Server.
   c. (Facultatif) Pour afficher un aperçu des données à exporter, sélectionnez la table, l'affichage ou la requête, puis choisissez Preview (Aperçu).
   d. Choisissez Suivant.
8. Sur la page Run Package (Exécuter le package), vérifiez que l'option Run immediately (Exécuter immédiatement) est sélectionnée. Choisissez Suivant.
9. Sur la page Complete the Wizard (Finaliser l'assistant), vérifiez que les informations d'exportation des données sont telles que vous les attendez. Choisissez Finish (Terminer).
10. Sur la page The execution was successful (L'exécution est réussie), choisissez Close (Fermer).

Assistant Générer et publier des scripts et utilitaire bcp

Vous pouvez utiliser l'assistant de génération et de publication de scripts pour créer des scripts pour une base de données entière ou seulement des objets sélectionnés. Vous pouvez exécuter ces scripts sur une instance de base de données SQL Server pour recréer les objets à base de script. Vous pouvez ensuite utiliser l'utilitaire bcp pour exporter en bloc les données pour les objets sélectionnés vers l'instance de base de données cible. Ce choix est préférable si vous souhaitez déplacer une base de données complète (dont des objets autres que des tables) ou d'importantes quantités de données entre deux instances DB SQL Server. Pour une description complète de la syntaxe de ligne de commande bcp, veuillez consulter la section relative à l'utilitaire bcp dans la documentation Microsoft SQL Server.

L'assistant SQL Server Generate et Publish Scripts est disponible dans le cadre de Microsoft SQL Server Management Studio. Ce client SQL Server graphique est inclus dans toutes les éditions de Microsoft SQL Server, sauf Express Edition. SQL Server Management Studio Express est disponible uniquement en tant qu'application basée sur Microsoft. SQL Server Management Studio Express est disponible auprès de Microsoft en téléchargement gratuit.

Pour utiliser l'assistant de génération et de publication de scripts et l'utilitaire bcp pour exporter des données, procédez comme suit :

1. Dans SQL Server Management Studio, connectez-vous à votre instance de base de données RDS SQL Server. Pour plus d'informations sur la manière de procéder, consultez Connexion à une instance de base de données exécutant le moteur de base de données Microsoft SQL Server (p. 618).
2. Dans Object Explorer (Navigateur d'objet), développez le nœud Bases de données et sélectionnez la base de données que vous souhaitez baser sur script.
3. Suivez les instructions dans Assistant générer et publier des scripts dans la documentation SQL Server pour créer un fichier script.
4. Dans SQL Server Management Studio, connectez-vous à votre instance de base de données SQL Server cible.
5. Avec l'instance de base de données SQL Server cible sélectionnée dans Object Explorer (Navigateur d'objet), choisissez Open (Ouvrir) dans le menu File (Fichier), sélectionnez File (Fichier) puis ouvrez le fichier script.
6. Si vous avez scripté la base de données entière, examinez l'instruction CREATE DATABASE dans le script. Veillez à ce que la base de données soit créée dans l'emplacement avec les paramètres de votre choix. Pour plus d'informations, consultez CREATE DATABASE (CRÉER UNE BASE DE DONNÉES) dans la documentation SQL Server.
7. Si vous créez des utilisateurs de base de données dans le script, assurez-vous que les ID de connexion serveur existent sur l'instance de base de données cible pour ces utilisateurs. Sinon, créez des ID de connexion pour ces utilisateurs. Dans le cas contraire, les commandes à base de script pour créer les utilisateurs de base de données échoueront. Pour de plus amples informations, veuillez consulter Créer un compte de connexion dans la documentation SQL Server.
8. Choisissez !Execute dans le menu SQL Editor pour exécuter le fichier script et créer les objets de base de données. Lorsque le script se termine, vérifiez que tous les objets de base de données existent comme prévu.
9. Utilisez l'utilitaire bcp pour exporter des données depuis l'instance de base de données RDS SQL Server dans des fichiers. Ouvrez une invite de commande et saisissez la commande suivante.

```
bcp database_name.schema_name.table_name out data_file -n -S aws_rds_sql_endpoint -U
 username -P password
```

Le code précédent inclut les options suivantes :

- table_name correspond au nom d'une des tables que vous avez recréées dans la base de données cible et que vous voulez à présent remplir avec des données.
- data_file correspond au nom et au chemin d'accès complet du fichier de données à créer.
- `-n` spécifie que la copie en bloc utilise les types de données natifs des données à copier.
- `-S` spécifie l'instance de base de données SQL Server d'origine de l'exportation.
- `-U` spécifie le nom d'utilisateur à utiliser lors de la connexion à l'instance de base de données SQL Server.
- `-P` spécifie le mot de passe pour l'utilisateur spécifié par `-U`.

Ce qui suit présente un exemple de commande.

```
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
```

Répétez cette étape jusqu'à ce que vous ayez des fichiers de données pour toutes les tables que vous souhaitez exporter.

10. Préparez votre instance de base de données cible pour l'importation en bloc de données en suivant les instructions dans Préparer l'importation de données en bloc dans la documentation SQL Server.
11. Décidez du choix d'une méthode d'importation en bloc à utiliser après avoir pris en compte la performance et d'autres problèmes abordés dans A propos des opérations d'exportation et d'importation en bloc dans la documentation SQL Server.
12. Importez en bloc les données depuis les fichiers de données que vous créez à l'aide de l'utilitaire bcp. Pour ce faire, suivez les instructions dans Importer et exporter des données en bloc à l'aide de l'utilitaire bcp ou Importer des données en bloc à l'aide de BULK INSERT ou OPENROWSET(BULK...) dans la documentation SQL Server, selon ce que vous avez décidé à l'étape 11.

Utilisation des réplicas en lecture pour Microsoft SQL Server dans Amazon RDS

Vous utilisez généralement des réplicas en lecture pour configurer la réplication entre instances de base de données Amazon RDS. Pour obtenir des informations générales sur les réplicas en lecture, veuillez consulter Utilisation des réplicas en lecture (p. 275).

Cette section contient des informations spécifiques sur l'utilisation des réplicas en lecture sur Amazon RDS pour SQL Server.

Rubriques

- Configuration des réplicas en lecture pour SQL Server (p. 662)
- Limites des réplicas en lecture avec SQL Server (p. 663)
- Résolution d'un problème de réplica en lecture SQL Server (p. 663)

Configuration des réplicas en lecture pour SQL Server

Avant qu'une instance de base de données puisse être utilisée comme instance source pour la réplication, vous devez activer les sauvegardes automatiques sur l'instance de base de données source. Pour cela, vous devez définir la période de rétention des sauvegardes sur une valeur autre que 0. L'instance de base de données source doit être un déploiement Multi-AZ avec groupes de disponibilité Always On. Pour définir ce type de déploiement, l'activation des sauvegardes automatiques doit également être effective.

La création d'un réplica en lecture SQL Server ne nécessite pas de coupure pour l'instance de base de données principale. Amazon RDS définit les paramètres et les autorisations nécessaires pour l'instance de base de données source et le réplica en lecture sans aucune interruption de service. Un instantané de l'instance de base de données source est pris, et devient le réplica en lecture. Aucune interruption de service ne se produit lorsque vous supprimez un réplica en lecture.

Vous pouvez créer jusqu'à cinq réplicas en lecture à partir d'une seule instance de base de données source. Pour que la réplication fonctionne de façon efficace, chaque réplica en lecture doit avoir la même quantité de ressources de calcul et de stockage que l'instance de base de données source. Si vous mettez à l'échelle l'instance de base de données source, faites-le également pour les réplicas en lecture.

La version du moteur de base de données SQL Server de l'instance de base de données source et tous ses réplicas en lecture doivent être identiques. Amazon RDS met à niveau le réplica principal immédiatement après la mise à niveau des réplicas en lecture, indépendamment de la fenêtre de maintenance. Pour de plus amples informations sur la mise à niveau de la version du moteur de base de données, veuillez consulter Mise à niveau du moteur de base de données Microsoft SQL Server (p. 629).

Pour qu'un réplica en lecture reçoive et applique les modifications de la source, il doit disposer de ressources de calcul et de stockage suffisantes. Si un réplica en lecture atteint sa capacité en ce qui concerne les ressources de calcul, de réseau ou de stockage, il arrête de recevoir ou d'appliquer les

modifications provenant de sa source. Vous pouvez modifier les ressources de stockage et d'UC d'un réplica en lecture indépendamment de sa source et d'autres réplicas en lecture.

Limites des réplicas en lecture avec SQL Server

Les limites suivantes s'appliquent aux réplicas en lecture SQL Server sur Amazon RDS :

- Les réplicas en lecture sont uniquement disponibles sur le moteur SQL Server Enterprise Edition (EE).
- Les réplicas en lecture sont disponibles pour SQL Server versions 2016 et 2017.
- L'instance de base de données source à répliquer doit être un déploiement multi-AZ avec des groupes de disponibilité Always On.
- Les réplicas en lecture sont uniquement disponibles pour les instances de base de données de la plateforme EC2-VPC.
- Les réplicas en lecture sont uniquement disponibles pour les instances de base de données exécutées sur les classes d'instances de base de données avec quatre vCPU ou plus.
- Les éléments suivants ne sont pas pris en charge sur Amazon RDS pour SQL Server :
  - Création d'un réplica en lecture dans une autre région AWS (réplica en lecture entre régions)
  - Rétention des sauvegardes des réplicas en lecture
  - Restauration à un instant dans le passé à partir de réplicas en lecture
  - Instantanés manuels de réplicas en lecture
  - Réplicas en lecture multi-AZ
  - Création de réplicas en lecture à partir de réplicas en lecture
  - Synchronisation des connexions utilisateur pour lire les réplicas en lecture
- Amazon RDS pour SQL Server n'intervient pas pour atténuer un retard de réplica élevé entre une instance de base de données source et ses réplicas en lecture. Assurez-vous que l'instance de base de données et ses réplicas en lecture ont une taille appropriée, en termes de puissance de calcul et de stockage, afin de pouvoir répondre aux besoins de la charge opérationnelle.
- Un réplica en lecture SQL Server appartient au même groupe d'options que l'instance de base de données source. Les modifications apportées au groupe d'options source ou à l'appartenance au groupe d'options source sont propagées aux réplicas en lecture. Ces modifications sont appliquées aux réplicas en lecture immédiatement après leur application à l'instance de base de données source, quelle que soit la fenêtre de maintenance du réplica en lecture.

  Pour de plus amples informations sur les groupes d'options, veuillez consulter Utilisation de groupes d'options (p. 209).

Résolution d'un problème de réplica en lecture SQL Server

Vous pouvez surveiller le retard de réplication dans Amazon CloudWatch en consultant la métrique Amazon RDS `ReplicaLag`. Pour de plus amples informations sur la durée du retard de réplication, veuillez consulter Supervision de la réplication en lecture (p. 291).

Si le retard de réplication est trop long, vous pouvez utiliser la requête suivante pour obtenir des informations sur le retard

```
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;
```

Déploiements multi-AZ pour Microsoft SQL Server

Les déploiements Multi-AZ améliorent la disponibilité, la durabilité des donnés et la tolérance aux pannes pour les instances de bases de données. En cas de maintenance planifiée de la base de données ou d'interruption imprévue du service, Amazon RDS bascule automatiquement vers l'instance de base de données secondaire à jour. Cette fonctionnalité permet aux opérations de la base de données de reprendre rapidement sans intervention manuelle. Les instances principales et de secours utilisent le même point de terminaison, l'adresse réseau physique de celui-ci étant transférée vers le réplica secondaire dans le cadre du processus de basculement. Vous n'avez pas à reconfigurer votre application lorsqu'un basculement se produit.

Amazon RDS prend en charge les déploiements multi-AZ pour Microsoft SQL Server à l'aide des groupes de disponibilité Mise en miroir de bases de données SQL Server ou Always On. Amazon RDS surveille et gère l'état de santé de votre déploiement multi-AZ. En cas de survenue de problèmes, RDS répare automatiquement les instances de bases de données non saines, rétablit la synchronisation et démarre le basculement. Le basculement n'a lieu que si les instances de secours et principales sont parfaitement synchronisées. Vous ne devez rien gérer.

Lorsque vous configurez le déploiement multi-AZ de SQL Server, RDS configure automatiquement toutes les bases de données de l'instance pour l'utilisation de la mise en miroir ou des groupes de disponibilité Always On. Amazon RDS gère les instances de base de données principale, témoin et secondaire pour vous. Dans la mesure où la configuration est automatique, RDS sélectionne la mise en miroir ou les groupes de disponibilité Always On en fonction de la version de SQL Server déployée.

Amazon RDS prend en charge les déploiements Multi-AZ avec les groupes de disponibilité Always On pour les éditions et les versions de SQL Server suivantes :

- SQL Server 2019 : Enterprise Edition 15.00.4043.16 ou version ultérieure
- SQL Server 2017: Enterprise Edition 14.00.3049.1 ou version ultérieure
- SQL Server 2016: Enterprise Edition 13.00.5216.0 ou version ultérieure

Amazon RDS prend en charge les déploiements Multi-AZ avec la mise en miroir pour les versions et éditions suivantes de SQL Server, à l'exception des version d'Enterprise Edition indiquées auparavant :

- SQL Server 2017 : Standard Edition et Enterprise Edition
- SQL Server 2016 : Standard Edition et Enterprise Edition
- SQL Server 2014 : Standard Edition et Enterprise Edition
- SQL Server 2012 : Standard Edition et Enterprise Edition

Amazon RDS prend en charge les déploiements multi-AZ pour SQL Server dans toutes les régions AWS, hormis les exceptions suivantes :

- Asie-Pacifique (Osaka-Local) : ni la mise en miroir ni les groupes de disponibilité Always On ne sont pris en charge ici.
- Asie-Pacifique (Sydney) : prise en charge pour les instances de bases de données dans des VPC.
- Asie-Pacifique (Tokyo) : prise en charge pour les instances de bases de données dans des VPC.
- Amérique du Sud (São Paulo) : prise en charge sur toutes les classes d'instance de bases de données, sauf m1 et m2.

Ajout d'un déploiement multi-AZ à une instance de base de données Microsoft SQL Server

Lorsque vous créez une nouvelle instance de base de données SQL Server à l'aide d'AWS Management Console, vous pouvez ajouter un déploiement multi-AZ avec mise en miroir ou groupes de disponibilité Always On. Pour ce faire, définissez Déploiement multi-AZ sur Oui (Mise en miroir/Always On). Pour de plus amples informations, veuillez consulter Création d'une instance de base de données Amazon RDS (p. 146).

Lorsque vous modifiez une instance de base de données SQL Server existante à l'aide d'AWS Management Console, vous pouvez ajouter un déploiement multi-AZ avec mise en miroir ou Always On en choisissant Yes (Mirroring /Always On) (Oui (Mise en miroir / Always On)) dans la liste Déploiement multi-AZ de la page Modifier l'instance DB. Pour de plus amples informations, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

> Note
>
> Si votre instance de base de données exécute la mise en miroir de bases de données (et non les groupes de disponibilité Always On), vous devrez peut-être désactiver l'optimisation en mémoire avant d'ajouter un déploiement multi-AZ. Désactivez l'optimisation en mémoire avec la mise en miroir de bases de données avant d'ajouter un déploiement multi-AZ si votre instance de base de données exécute SQL Server 2014, 2016 ou 2017 Enterprise Edition et que l'optimisation en mémoire est activée.
> Si votre instance de base de données exécute des groupes de disponibilité, cette étape n'est pas obligatoire.

Notes et recommandations concernant le déploiement multi-AZ de Microsoft SQL Server

Voici quelques restrictions lorsque vous travaillez avec des déploiements Multi-AZ pour les instances de bases de données Microsoft SQL Server :

- Le Multi-AZ entre régions n'est pas pris en charge.
- Vous ne pouvez pas configurer l'instance de base de données secondaire pour accepter l'activité de lecture de base de données.
- Le déploiement multi-AZ avec les groupes de disponibilité Always On prend en charge l'optimisation en mémoire.
- Le déploiement multi-AZ avec les groupes de disponibilité Always On ne prend pas en charge l'authentification Kerberos pour l'écouteur du groupe de disponibilité. En effet, l'écouteur ne possède pas de nom de principal de service (SPN).
- Vous ne pouvez pas renommer une base de données sur une instance de base de données SQL Server située dans un déploiement multi-AZ SQL Server. Si vous devez renommer une base de données sur une telle instance, vous devez d'abord désactiver le déploiement multi-AZ pour l'instance de base de données, puis renommer la base de données. Réactivez ensuite le déploiement multi-AZ pour l'instance de base de données.
- Vous pouvez uniquement restaurer des instances de base de données multi-AZ sauvegardées en utilisant le modèle de récupération « Full ».

Voici quelques notes sur l'utilisation des déploiements Multi-AZ pour les instances de bases de données Microsoft SQL Server :

- Amazon RDS expose le point de terminaison de l'écouteur des groupes de disponibilité Always On. Le point de terminaison est visible dans la console et est renvoyé par l'API `DescribeDBInstances` en tant qu'entrée dans le champ des points de terminaison.

- Amazon RDS prend en charge les basculements à plusieurs sous-réseaux du groupe de disponibilité.
- Pour utiliser les déploiements multi-AZ SQL Server avec une instance de base de données SQL Server dans un VPC, créez d'abord un groupe de sous-réseaux de base de données comportant des sous-réseaux dans au moins deux zones de disponibilité distinctes. Affectez ensuite le groupe de sous-réseaux de base de données au réplica principal de l'instance de base de données SQL Server.
- Lorsqu'une instance de base de données est transformée en déploiement multi-AZ, elle présente le statut modification lors de la modification. Amazon RDS crée l'instance de secours et effectue une sauvegarde de l'instance de base de données principale. Une fois le processus terminé, le statut de l'instance de base de données principale devient disponible.
- Les déploiements Multi-AZ maintiennent toutes les bases de données sur le même nœud. Si une base de données sur l'hôte principal bascule, toutes vos bases de données SQL Server font l'objet d'un basculement avec une unité atomique sur votre hôte de secours. Amazon RDS alloue un nouvel hôte sain et remplace l'hôte non sain.
- Le Multi-AZ avec DBM ou AG prend en charge un réplica de secours unique.
- Les utilisateurs, les ID de connexion et les autorisations sont automatiquement répliqués pour vous sur l'instance secondaire. Vous n'avez pas besoin de les recréer. Les rôles de serveur définis par l'utilisateur (une fonction de SQL Server 2012) sont uniquement répliqués dans les instances multi-AZ pour les instances de groupes de disponibilité Always On.
- Si vous avez des tâches SQL Server Agent, recréez-les sur l'instance secondaire. En effet, ces tâches sont stockées dans la base de données msdb, que vous ne pouvez pas répliquer à l'aide de la mise en miroir ou des groupes de disponibilité Always On. Créez les tâches tout d'abord dans l'instance primaire d'origine, puis basculez et créez les mêmes tâches dans la nouvelle instance primaire.
- Il est possible que vous observiez des temps de latence élevés par rapport à un déploiement d'instance de base de données standard (dans une zone de disponibilité unique) en raison de la réplication synchrone des données.
- Les délais de basculement sont affectés par le temps nécessaire à la réalisation du processus de récupération. Le délai de basculement est allongé pour les transactions de volume important.

Voici quelques recommandations sur l'utilisation des déploiements Multi-AZ pour les instances de bases de données Microsoft SQL Server :

- Pour les bases de données utilisées en production ou préproduction, nous vous recommandons les options suivantes :
  - Déploiements multi-AZ pour une haute disponibilité
  - IOPS provisionnés pour des performances rapides et cohérentes
  - « Mémoire optimisée » plutôt que « Usage général »
- Vous ne pouvez pas sélectionner la zone de disponibilité (AZ) pour l'instance secondaire. Tenez-en compte lorsque vous déployez les hôtes d'application. Votre base de données peut basculer vers une autre zone de disponibilité et les hôtes d'application peuvent ne pas se trouver dans la même zone de disponibilité que la base de données. C'est pourquoi nous vous recommandons d'équilibrer vos hôtes d'application sur toutes les zones de disponibilité (AZ) de la région AWS concernée.
- Pour optimiser les performances, n'activez pas la mise en miroir ou les groupes de disponibilité Always On pendant une opération de chargement d'un volume important de données. Pour optimiser la vitesse de chargement de vos données, terminez le chargement des données avant de convertir votre instance de base de données en déploiement multi-AZ.
- Les applications qui ont accès aux bases de données SQL Server doit disposer d'une gestion des exceptions qui identifie les erreurs de connexion. L'exemple de code suivant illustre un bloc try/catch qui identifie une erreur de communication.

```
for (int iRetryCount = 0; (iRetryCount < RetryMaxAttempts && keepInserting); iRetryCount+
+)
{
   using (SqlConnection connection = new SqlConnection(DatabaseConnString))
```

```
   {
      using (SqlCommand command = connection.CreateCommand())
      {
         command.CommandText = "INSERT INTO SOME_TABLE VALUES ('SomeValue');";

         try
         {
            connection.Open();

            while (keepInserting)
            {
               command.ExecuteNonQuery();
               intervalCount++;
            }
                  connection.Close();
         }

         catch (Exception ex)
         {
                  Logger(ex.Message);
         }
      }
   }

   if (iRetryCount < RetryMaxAttempts && keepInserting)
   {
            Thread.Sleep(RetryIntervalPeriodInSeconds * 1000);
   }
}
```

- N'utilisez pas la commande `Set Partner Off` lorsque vous travaillez avec des instances multi-AZ. Par exemple, n'effectuez pas les opérations suivantes :

```
--Don't do this
ALTER DATABASE db1 SET PARTNER off
```

- Ne définissez pas le mode de récupération sur `simple`. Par exemple, n'effectuez pas les opérations suivantes :

```
--Don't do this
ALTER DATABASE db1 SET RECOVERY simple
```

- N'utilisez pas le paramètre `DEFAULT_DATABASE` lors de la création de nouveaux ID de connexion sur des instances de bases de données multi-AZ car ces paramètres ne peuvent pas être appliqués au miroir de secours. Par exemple, n'effectuez pas les opérations suivantes :

```
--Don't do this
CREATE LOGIN [test_dba] WITH PASSWORD=foo, DEFAULT_DATABASE=[db2]
```

  En outre, n'effectuez pas les opérations suivantes :

```
--Don't do this
ALTER LOGIN [test_dba] SET DEFAULT_DATABASE=[db3]
```

Détermination de l'emplacement du réplica secondaire

Vous pouvez déterminer l'emplacement du réplica secondaire à l'aide d'AWS Management Console. Vous devez connaître l'emplacement du réplica secondaire si vous configurez votre instance de base de données principale dans un VPC.

Vous pouvez également consulter la zone de disponibilité du réplica secondaire à l'aide de la commande `describe-db-instances` de l'AWS CLI ou de l'opération d'API RDS `DescribeDBInstances`. Le résultat indique la zone de disponibilité secondaire où se situe le miroir de secours.

Migration de la mise en miroir de bases de données (DBM) vers les groupes de disponibilité AlwaysOn

Dans la version 14.00.3049.1 de l'édition Microsoft SQL Server Enterprise, les groupes de disponibilité Always On sont activés par défaut.

Pour migrer de la mise en miroir de bases de données vers les groupes de disponibilité, commencez par vérifier votre version. Lorsque vous utilisez une instance de base de données de version antérieure à 13.00.5216.0, modifiez l'instance pour la faire passer à la version 13.00.5216.0 ou une version ultérieure. Lorsque vous utilisez une instance de base de données de version antérieure à 14.00.3049.1, modifiez-la pour la faire passer à la version 14.00.3049.1 ou une version ultérieure.

Si vous souhaitez mettre à niveau une instance de base de données en miroir afin d'utiliser des groupes de disponibilité, exécutez d'abord la mise à niveau, modifiez l'instance pour supprimer le multi-AZ, puis modifiez-la à nouveau afin d'ajouter le multi-AZ. Cette opération convertit votre instance en vue de l'utilisation des groupes de disponibilité Always On.

Fonctionnalités supplémentaires pour Microsoft SQL Server sur Amazon RDS

Dans les sections suivantes, vous trouverez des informations sur l'augmentation des instances Amazon RDS exécutant le moteur de base de données Microsoft SQL Server en ajoutant les certificats SSL, l'authentification Windows et l'intégration S3.

Rubriques

- Utilisation de SSL avec une instance DB Microsoft SQL Server (p. 669)
- Configuration des protocoles de sécurité et des chiffrements (p. 672)

- Utilisation de l'authentification Windows avec une instance de base de données Amazon RDS pour SQL Server (p. 676)
- Intégration d'un Amazon RDS pour instance de base de données SQL Server avec Amazon S3 (p. 686)

Utilisation de SSL avec une instance DB Microsoft SQL Server

Vous pouvez utiliser SSL (Secure Sockets Layer) pour chiffrer les connexions entre vos applications clientes et vos instances de base de données Amazon RDS exécutant Microsoft SQL Server. Le support SSL est disponible dans toutes les régions AWS pour toutes les éditions SQL Server prises en charge.

Lorsque vous créez une instance de base de données SQL Server, Amazon RDS crée un certificat SSL pour celle-ci. Le certificat SSL inclut le point de terminaison de l'instance de base de données en tant que nom commun du certificat SSL pour assurer une protection contre les attaques par usurpation.

Il existe deux façons d'utiliser SSL pour vous connecter à votre instance de base de données SQL Server :

- Forcer SSL pour toutes les connexions — cette opérations s'exécute en toute transparence pour le client qui n'a rien à faire pour utiliser SSL.
- Chiffrer des connexions spécifiques — cela permet de configurer une connexion SSL depuis un ordinateur spécifique du client que vous devez utiliser pour chiffrer les connexions.

Pour plus d'informations sur la prise en charge du protocole TLS (Transport Layer Security) pour SQL Server, consultez la documentation relative à la prise en charge de TLS 1.2 pour Microsoft SQL Server.

Forcer les connexions à votre instance de base de données pour utiliser SSL

Vous pouvez forcer toutes les connexions à votre instance de base de données à utiliser SSL. Si vous forcez les connexions à utiliser SSL, cette opération s'exécute en toute transparence pour le client qui n'a rien à faire pour utiliser SSL.

Si vous souhaitez forcer SSL, utilisez le paramètre `rds.force_ssl`. Par défaut, le paramètre `rds.force_ssl` est défini sur `0 (off)`. Définissez le paramètre `rds.force_ssl` sur `1 (on)` pour forcer les connexions à utiliser SSL. Le paramètre `rds.force_ssl` est statique, donc après avoir modifié la valeur, vous devez redémarrer votre instance de base de données pour que la modification soit effective.

Pour forcer toutes les connexions à votre instance de base de données à utiliser SSL

1. Déterminez le groupe de paramètres attaché à votre instance de base de données :
   a. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
   b. Dans le coin supérieur droit de la console Amazon RDS, choisissez la région AWS de votre instance de base de données.
   c. Dans le panneau de navigation, choisissez Bases de données, puis le nom de votre instance de base de données pour afficher ses détails.
   d. Choisissez l'onglet Configuration. Recherchez le groupe de paramètres dans la section.
2. Le cas échéant, créez un nouveau groupe de paramètres. Si votre instance de base de données utilise le groupe de paramètres par défaut, vous devez créer un nouveau groupe de paramètres. Si votre instance de base de données utilise un groupe de paramètres personnalisé, vous pouvez choisir

de modifier le groupe de paramètres existant ou de créer un nouveau groupe de paramètre. Si vous modifiez un groupe de paramètre existant, la modification s'applique à l'ensemble des instances de base de données qui utilisent ce groupe de paramètres.

Pour créer un nouveau groupe de paramètres, suivez les instructions dans Création d'un groupe de paramètres de bases de données (p. 227).

3. Modifiez le groupe de paramètres nouvellement créé ou existant pour définir le paramètre `rds.force_ssl` sur `true`. Pour modifier le groupe de paramètres, suivez les instructions dans Modification de paramètres dans un groupe de paramètres de bases de données (p. 229).
4. Si vous créez un nouveau groupe de paramètres, modifiez votre instance de base de données à attacher au nouveau groupe de paramètres. Modifiez le paramètre Groupe de paramètres de base de données de l'instance de base de données. Pour de plus amples informations, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).
5. Redémarrez votre instance de base de données. Pour plus d'informations, consultez Redémarrage d'une instance de base de données (p. 272).

Chiffrement de connexions spécifiques

Vous pouvez forcer toutes les connexions à votre instance de base de données à utiliser SSL ou vous pouvez chiffrer les connexions depuis des ordinateurs client spécifiques uniquement. Pour utiliser SSL depuis l'ordinateur spécifique du client, vous devez obtenir des certificats pour l'ordinateur client, importer des certificats sur l'ordinateur client, puis chiffrer les connexions depuis l'ordinateur client.

Note

Toutes les instances SQL Server créées après le 5 août 2014 utilisent le point de terminaison d'instance de base de données dans le champ Common Name (CN) du certificat SSL. Avant le 5 août 2014, la vérification de certificat SSL n'était pas disponible pour les instances SQL Server basées sur VPC. Si vous disposez d'une instance de base de données SQL Server basée sur VPC qui a été créée avant le 5 août 2014, et que vous voulez utiliser la vérification de certificat SSL et assurer que le point de terminaison de l'instance soit inclus comme CN pour le certificat SSL de cette instance de base de données, renommez l'instance. Lorsque vous renommez une instance de base de données, un nouveau certificat est déployé et l'instance est redémarrée pour activer le nouveau certificat.

Obtention de certificats pour les ordinateurs clients

Pour chiffrer les connexions d'un ordinateur client vers une instance de base de données Amazon RDS exécutant Microsoft SQL Server, vous avez besoin d'un certificat sur votre ordinateur client.

Pour obtenir ce certificat, téléchargez-le sur votre ordinateur client. Vous pouvez télécharger un certificat racine valide pour toutes les régions. Un ensemble de certificats contenant l'ancien certificat racine et le nouveau certificat racine peut également être téléchargé. De plus, vous pouvez télécharger des certificats intermédiaires propres à une région. Pour en savoir plus sur le téléchargement de certificats, consultez Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).

Après avoir téléchargé le certificat approprié, importez-le dans votre système d'exploitation Microsoft Windows en suivant la procédure de la section suivante.

Importation de certificats sur des ordinateurs clients

Vous pouvez utiliser la procédure suivante pour importer votre certificat dans le système d'exploitation Microsoft Windows de votre ordinateur client.

Pour importer le certificat dans votre système d'exploitation Windows :

1. Dans le menu Début, saisissez **`Run`** dans la zone de recherche et appuyez sur Entrée.
2. Dans la zone Ouvrir, saisissez **`MMC`** et choisissez OK.

3. Dans la console MMC, dans le menu Fichier, choisissez Add/Remove Snap-in (Ajouter/Supprimer Snap-in).
4. Dans la boîte de dialogue Add or Remove Snap-ins (Ajouter ou Supprimer les Snap-ins), pour Available snap-ins (Snap-ins disponibles), sélectionnez **`Certificates`** et choisissez Ajouter.
5. Dans la boîte de dialogue Certificates snap-in (Certificats snap-in), choisissez Computer account (Compte d'ordinateur) et Suivant.
6. Dans la boîte de dialogue Select computer (Sélectionner ordinateur), choisissez Terminer.
7. Dans la boîte de dialogue Add or Remove Snap-ins (Ajouter ou supprimer snap-ins), choisissez OK.
8. Dans la console MMC, développez Certificats, ouvrez le menu contextuel (clic droit) et pour Trusted Root Certification Authorities (Autorités de certification de racine de confiance), choisissez All Tasks (Toutes les tâches) et Importer.
9. Sur la première page de l'assistant d'importation de certificat, choisissez Suivant.
10. Sur la deuxième page de l'assistant d'importation de certificat, choisissez Browse (Naviguer). Dans la fenêtre de navigation, modifiez le type de fichier à Tous les fichiers (*.*), car .pem n'est pas une extension de certificat standard. Recherchez le fichier .pem que vous avez téléchargé précédemment.
11. Choisissez Ouvrir pour sélectionner le fichier de certificat, puis Suivant.
12. Sur la troisième page de l'assistant d'importation de certificat, choisissez Suivant.
13. Sur la quatrième page de l'assistant d'importation de certificat, choisissez Terminer. Une boîte de dialogue apparaît confirmant la réussite de l'importation.
14. Dans la console MMC, développez Certificats, développez Trusted Root Certification Authorities (Autorités de certification racine de confiance) et choisissez Certificats. Recherchez le certificat pour confirmer son existence, comme illustré ici.

15. Redémarrez votre ordinateur.

Chiffrement des connexions vers une instance de base de données Amazon RDS exécutant Microsoft SQL Server

Après avoir importé un certificat dans votre ordinateur client, vous pouvez chiffrer des connexions d'un ordinateur client vers une instance de base de données Amazon RDS exécutant Microsoft SQL Server.

Pour SQL Server Management Studio, utilisez la procédure suivante. Pour de plus amples informations sur SQL Server Management Studio, veuillez consulter Utilisation de SQL Server Management Studio.

Pour chiffrer des connexions à partir de SQL Server Management Studio

1. Lancez SQL Server Management Studio.
2. Pour Connect to server (Se connecter au serveur), entrez les informations serveur, le mot de passe et le nom d'utilisateur de connexion.
3. Choisissez Options.
4. Sélectionnez Encrypt connection (Chiffrer la connexion).
5. Choisissez Connexion.
6. Vérifiez que votre connexion est chiffrée en exécutant la requête suivante. Vérifiez que la requête renvoie `true` pour `encrypt_option`.

```
select ENCRYPT_OPTION from SYS.DM_EXEC_CONNECTIONS where SESSION_ID = @@SPID
```

Pour tout autre client SQL, utilisez la procédure suivante.

Pour chiffrer des connexions d'autres clients SQL

1. Ajoutez `encrypt=true` au début du votre chaîne de connexion. Cette chaîne peut être disponible en tant qu'option ou en tant que propriété sur la page de connexion dans les outils d'interface utilisateur graphique.

   Note

   Pour activer le chiffrement SSL pour des clients qui se connectent en utilisant JDBC, vous devrez peut-être ajouter le certificat SQL Amazon RDS au magasin de certificats d'autorité de certification (cacerts) Java. Vous pouvez faire cela en utilisant l'utilitaire keytool.

2. Vérifiez que votre connexion est chiffrée en exécutant la requête suivante. Vérifiez que la requête renvoie `true` pour `encrypt_option`.

```
select ENCRYPT_OPTION from SYS.DM_EXEC_CONNECTIONS where SESSION_ID = @@SPID
```

Configuration des protocoles de sécurité et des chiffrements

Vous pouvez activer et désactiver certains protocoles de sécurité et chiffrements à l'aide des paramètres de base de données. Les paramètres de sécurité que vous pouvez configurer (à l'exception de TLS version 1.2) sont présentés dans le tableau suivant.

La valeur `default` signifie que la valeur par défaut du système d'exploitation est utilisée, qu'il s'agisse de `enabled` ou `disabled`.

Note

Vous ne pouvez pas désactiver TLS 1.2, car Amazon RDS l'utilise en interne.

Paramètre de base de données	Valeurs autorisées (valeur par défaut en gras)	Description
rds.tls10	par défaut, activé, désactivé	TLS 1.0.
rds.tls11	par défaut, activé, désactivé	TLS 1.1.
rds.tls12	default	TLS 1.2. Vous ne pouvez pas modifier cette valeur.
rds.rc4	par défaut, activé, désactivé	Chiffrement du flux RC4.
rds.diffie-hellman	par défaut, activé, désactivé	Chiffrement d'échange de clés Diffie-Hellman.
rds.diffie-hellman-min-key-bit-length	par défaut, 1024, 2048, 4096	Longueur minimale de bits pour les clés Diffie-Hellman.
rds.curve25519	par défaut, activé, désactivé	Chiffrement Curve25519 elliptic-curve. Ce paramètre n'est pas pris en charge pour toutes les versions du moteur.
rds.3des168	par défaut, activé, désactivé	Chiffrement des données Triple Data Encryption Standard (DES)

Paramètre de base de données	Valeurs autorisées (valeur par défaut en gras)	Description
		avec une longueur de clé de 168 bits.

Utilisez la procédure suivante pour configurer les protocoles de sécurité et les chiffrements :

1. Créez un groupe de paramètres DB personnalisé.
2. Modifiez les paramètres du groupe de paramètres.
3. Associez le groupe de paramètres DB à l'instance de base de données.

Pour plus d'informations sur les groupes de paramètres de base de données, consultez Utilisation de groupes de paramètres de base de données (p. 225).

Création du groupe de paramètres liés à la sécurité

Créez un groupe de paramètres pour vos paramètres liés à la sécurité qui correspond à l'édition et à la version de SQL Server de votre instance de base de données.

Console

La procédure suivante crée un groupe de paramètres pour SQL Server Standard Edition 2016.

Pour créer le groupe de paramètres

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes de paramètres.
3. Choisissez Créer un groupe de paramètres.
4. Dans le volet Créer un groupe de paramètres, faites ce qui suit :
   a. Pour Famille de groupes de paramètres, choisissez sqlserver-se-13.0.
   b. Pour Nom du groupe, saisissez un identifiant pour le groupe de paramètres, tel que **`sqlserver-ciphers-se-13`**.
   c. Pour Description, saisissez **`Parameter group for security protocols and ciphers`**.
5. Sélectionnez Créer.

Interface de ligne de commande

La procédure suivante crée un groupe de paramètres pour SQL Server Standard Edition 2016.

Pour créer le groupe de paramètres

- Exécutez une des commandes suivantes :

  Example

  Pour Linux, macOS ou 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"
```

Pour 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"
```

Modification des paramètres liés à la sécurité

Modifiez les paramètres liés à la sécurité dans le groupe de paramètres qui correspond à l'édition et à la version SQL Server de votre instance de base de données.

Console

La procédure suivante modifie le groupe de paramètres que vous avez créé pour SQL Server Standard Edition 2016. Cet exemple montre comment désactiver TLS version 1.0.

Pour modifier le groupe de paramètres

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes de paramètres.
3. Choisissez le groupe de paramètres, tel que sqlserver-ciphers-se-13.
4. Sous Paramètres, filtrez la liste des paramètres pour **rds**.
5. Choisissez Modifier les paramètres.
6. Choisissez rds.tls10.
7. Pour Valeurs, choisissez désactivé.
8. Sélectionnez Save Changes.

Interface de ligne de commande

La procédure suivante modifie le groupe de paramètres que vous avez créé pour SQL Server Standard Edition 2016. Cet exemple montre comment désactiver TLS version 1.0.

Pour modifier le groupe de paramètres

- Exécutez une des commandes suivantes :

  Example

  Pour Linux, macOS ou Unix :

```
aws rds modify-db-parameter-group \
    --db-parameter-group-name sqlserver-ciphers-se-13 \
    --parameters
 "ParameterName='rds.tls10',ParameterValue='disabled',ApplyMethod=pending-reboot"
```

  Pour Windows :

```
aws rds modify-db-parameter-group ^
    --db-parameter-group-name sqlserver-ciphers-se-13 ^
    --parameters
 "ParameterName='rds.tls10',ParameterValue='disabled',ApplyMethod=pending-reboot"
```

Association du groupe de paramètres liés à la sécurité à votre instance de base de données

Pour associer le groupe de paramètres à votre instance de base de données, utilisez le AWS Management Console ou le AWS CLI.

Console

Vous pouvez associer le groupe de paramètres à une instance de base de données nouvelle ou existante :

- Pour une nouvelle instance de base de données, associez-la lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).
- Pour une instance de base de données existante, associez-la en modifiant l'instance. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Interface de ligne de commande

Vous pouvez associer le groupe de paramètres à une instance de base de données nouvelle ou existante.

Pour créer une instance de base de données avec le groupe de paramètres

- Spécifiez le type de moteur de base de données et la version majeure utilisés lors de la création du groupe de paramètres.

  Example

  Pour Linux, macOS ou 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
```

  Pour 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
```

Pour modifier une instance de base de données et associer le groupe de paramètres

- Exécutez une des commandes suivantes :

Example

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --db-parameter-group-name sqlserver-ciphers-se-13 \
    --apply-immediately
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --db-parameter-group-name sqlserver-ciphers-se-13 ^
    --apply-immediately
```

Utilisation de l'authentification Windows avec une instance de base de données Amazon RDS pour SQL Server

Vous pouvez utiliser l'authentification Microsoft Windows pour authentifier les utilisateurs lorsqu'ils se connectent à votre instance de base de données Amazon RDS pour Microsoft SQL Server. L'instance de base de données utilise AWS Directory Service for Microsoft Active Directory (Enterprise Edition), également appelé AWS Managed Microsoft AD, pour activer l'authentification Windows. Lorsque les utilisateurs s'authentifient à une instance de base de données SQL Server jointe au domaine d'approbation, les demandes d'authentification sont transmises à l'annuaire de domaine que vous créez avec AWS Directory Service.

Amazon RDS prend en charge l'authentification Windows pour SQL Server dans toutes les régions AWS.

Amazon RDS utilise le mode mixte pour l'authentification Windows. Cette approche signifie que l'utilisateur principal (nom et mot de passe utilisés pour créer votre instance de base de données SQL Server) utilise l'authentification SQL. Étant donné que le compte utilisateur principal comporte des informations d'identification privilégiées, vous devez limiter l'accès à ce compte.

Pour obtenir l'authentification Windows à l'aide d'un compte Microsoft Active Directory sur site ou auto-géré, créez une approbation de forêt. L'approbation peut être unidirectionnelle ou bidirectionnelle. Pour en savoir plus sur la configuration d'approbations de forêts à l'aide d'AWS Directory Service, consultez la section Quand créer une relation d'approbation dans le AWS Directory Service Administration Guide.

Pour configurer l'authentification Windows pour une instance de base de données SQL Server, procédez comme suit. Les étapes sont expliquées de façon plus détaillée dans Configuration de l'authentification Windows pour les instances de base de données SQL Server (p. 677) :

1. Utilisez AWS Managed Microsoft AD, à partir de l'AWS Management Console ou de l'API AWS Directory Service, pour créer un répertoire AWS Managed Microsoft AD.
2. Si vous utilisez l'AWS CLI ou l'API Amazon RDS pour créer votre instance de base de données SQL Server, créez un rôle AWS Identity and Access Management (IAM). Ce rôle utilise la stratégie IAM gérée `AmazonRDSDirectoryServiceAccess` et autorise Amazon RDS à effectuer des appels vers votre annuaire. Si vous utilisez la console pour créer votre instance de base de données SQL Server, AWS crée le rôle IAM pour vous.

   Pour que le rôle autorise l'accès, le point de terminaison AWS Security Token Service (AWS STS) doit être activé dans la région AWS pour votre compte AWS. Les points de terminaison AWS STS sont actifs

par défaut dans toutes les régions AWS et vous pouvez les utiliser sans qu'aucune autre action soit nécessaire. Pour de plus amples informations, veuillez consulter Gestion de AWS STS dans une région AWS dans le IAM Guide de l'utilisateur.

3. Créez et configurez des utilisateurs et des groupes dans l'annuaire AWS Managed Microsoft AD à l'aide des outils Microsoft Active Directory. Pour en savoir plus sur la création d'utilisateurs et de groupes dans Active Directory, veuillez consulter Gestion des utilisateurs et des groupes dans AWS Managed Microsoft AD dans le AWS Directory Service Administration Guide.
4. Si vous prévoyez de localiser le répertoire et l'instance de base de données dans différents VPC, activez le trafic entre VPC.
5. Utilisez Amazon RDS pour créer une nouvelle instance de base de données SQL Server à partir de la console, de l'AWS CLI ou de l'API Amazon RDS. Dans la demande de création, vous indiquez l'identifiant du domaine (identifiant « `d-*` ») généré lors de la création de votre annuaire, ainsi que le nom du rôle que vous avez créé. Vous pouvez également modifier une instance de base de données SQL Server pour qu'elle utilise l'authentification Windows en configurant les paramètres de domaine et de rôle IAM de l'instance de base de données.
6. Utilisez les informations d'identification de l'utilisateur principal Amazon RDS pour vous connecter à l'instance de base de données SQL Server de la même manière qu'à n'importe quelle instance de base de données. Étant donné que l'instance de base de données est jointe au domaine AWS Managed Microsoft AD, vous pouvez allouer les connexions et utilisateurs SQL Server à partir des utilisateurs et groupes Active Directory dans leur domaine. (Ceux-ci sont connus sous le nom de connexions SQL Server « Windows ».) Les autorisations pour la base de données sont gérées via des autorisations SQL Server standard accordées et révoquées en fonction des connexions Windows.

Création d'un point de terminaison pour l'authentification Kerberos

L'authentification basée sur Kerberos nécessite que le point de terminaison soit le nom d'hôte spécifié par le client, un point, puis le nom de domaine complet (FQDN). Par exemple, l'exemple suivant illustre un point de terminaison à utiliser avec l'authentification basée sur Kerberos. Dans cet exemple, le nom d'hôte de l'instance de base de données SQL Server est `ad-test` et le nom de domaine est `corp-ad.company.com` :

```
ad-test.corp-ad.company.com
```

Pour vérifier que votre connexion utilise Kerberos, exécutez la requête suivante :

```
SELECT net_transport, auth_scheme
  FROM sys.dm_exec_connections
 WHERE session_id = @@SPID;
```

Configuration de l'authentification Windows pour les instances de base de données SQL Server

Vous utilisez AWS Directory Service for Microsoft Active Directory (Enterprise Edition), également appelé AWS Managed Microsoft AD, pour configurer l'authentification Windows pour une instance de base de données SQL Server. Pour configurer l'authentification Windows, procédez comme suit.

Étape 1 : Créer un annuaire à l'aide d'AWS Directory Service for Microsoft Active Directory (Enterprise Edition)

AWS Directory Service crée un annuaire Microsoft Active Directory totalement géré dans le Cloud AWS. Lorsque vous créez un annuaire AWS Managed Microsoft AD, AWS Directory Service crée deux contrôleurs de domaine et serveurs de service de noms de domaine (DNS) en votre nom. Les

serveurs de répertoire sont créés dans deux sous-réseaux sur deux zones de disponibilité différentes avec un VPC. Cette redondance permet de s'assurer que votre répertoire reste accessible y compris en cas de défaillance.

Lorsque vous créez un annuaire AWS Managed Microsoft AD, AWS Directory Service effectue les tâches suivantes en votre nom :

- Configuration de Microsoft Active Directory dans le VPC.
- Création d'un compte d'administrateur d'annuaire avec le nom d'utilisateur Admin et le mot de passe spécifié. Ce compte est utilisé pour gérer votre annuaire.

  Note

  Veillez à enregistrer ce mot de passe. AWS Directory Service ne stocke pas ce mot de passe et vous ne pouvez pas le récupérer ni le réinitialiser.
- Création d'un groupe de sécurité pour les contrôleurs de l'annuaire.

Lorsque vous lancez un AWS Directory Service for Microsoft Active Directory (Enterprise Edition), AWS crée une unité d'organisation (UO) qui contient les objets de votre annuaire. Cette unité d'organisation, qui porte le nom NetBIOS que vous avez saisi lorsque vous avez créé votre annuaire, est située dans la racine du domaine. La racine du domaine appartient à AWS, qui la gère.

Le compte admin qui a été créé avec votre annuaire AWS Managed Microsoft AD dispose des autorisations pour les activités administratives les plus courantes pour votre unité d'organisation :

- Créer, mettre à jour ou supprimer des utilisateurs, des groupes et des ordinateurs
- Ajouter des ressources à votre domaine, comme des serveurs de fichiers ou d'impression, puis attribuer des autorisations pour ces ressources aux utilisateurs et groupes dans votre unité d'organisation.
- Créer des unités d'organisation et des conteneurs supplémentaires.
- Déléguer des autorités.
- Créer et associer des stratégies de groupes.
- Restaurer des objets supprimés de la corbeille Active Directory.
- Exécuter des modules AD et DNS Windows PowerShell sur le service Web Active Directory.

Le compte admin dispose également de droits pour exécuter les activités suivantes au niveau du domaine :

- Gérer les configurations DNS (ajouter, supprimer ou mettre à jour des enregistrements, des zones et des redirecteurs)
- Afficher les journaux d'événements DNS.
- Afficher les journaux d'événements de sécurité.

Pour créer un annuaire avec AWS Managed Microsoft AD

1. Dans le panneau de navigation de la console AWS Directory Service, choisissez Annuaires, puis Configurer un annuaire.
2. Choisissez AWS Managed Microsoft AD. Il s'agit de la seule option prise en charge actuellement pour être utilisée avec Amazon RDS.
3. Choisissez Suivant.
4. Sur la page Enter directory information (Saisir les détails de l'annuaire), renseignez les informations suivantes :

   Edition

   Choisissez l'édition qui correspond à vos besoins.

Nom de DNS de l'annuaire

Nom complet de l'annuaire, par exemple `corp.example.com`. Les noms de plus de 47 caractères ne sont pas pris en charge par SQL Server.

Nom NetBIOS de l'annuaire

Nom court facultatif pour l'annuaire, par exemple `CORP`.

Description de l'annuaire

Description facultative de l'annuaire.

Mot de passe administrateur

Mot de passe de l'administrateur de l'annuaire. Le processus de création d'un annuaire crée un compte d'administrateur avec le nom d'utilisateur Admin et ce mot de passe.

Le mot de passe de l'administrateur de l'annuaire ne peut pas inclure le terme `admin`. Le mot de passe est sensible à la casse et doit comporter entre 8 et 64 caractères. Il doit également contenir au moins un caractère de trois des quatre catégories suivantes :

- Lettres minuscules (a-z)
- Lettres majuscules (A-Z)
- Chiffres (0-9)
- Caractères non alphanumériques (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Confirmer le mot de passe

Saisissez à nouveau le mot de passe de l'administrateur.

5. Choisissez Suivant.
6. Sur la page Choose VPC and subnets (Choisir un VPC et des sous-réseaux), indiquez les informations suivantes :

   VPC

   Sélectionnez le VPC pour l'annuaire.

   > **Note**
   >
   > Vous pouvez localiser l'annuaire et l'instance de base de données dans différents VPC, mais si vous procédez ainsi, assurez-vous d'activer le trafic entre VPC. Pour plus d'informations, consultez Étape 4 : Activer le trafic entre VPC entre le répertoire et l'instance de base de données (p. 682).

   Sous-réseaux

   Choisissez les sous-réseaux pour les serveurs d'annuaires. Les deux sous-réseaux doivent être dans des zones de disponibilité différentes.
7. Choisissez Suivant.
8. Vérifiez les informations de l'annuaire. Si vous devez apporter des modifications, choisissez Previous (Précédent). Lorsque les informations sont correctes, choisissez Create directory (Créer l'annuaire).

La création de l'annuaire prend plusieurs minutes. Lorsqu'il est créé, la valeur du champ Statut devient Actif.

Pour consulter les informations relatives à votre annuaire, choisissez l'ID de l'annuaire dans la liste. Notez la valeur de ID de l'annuaire. Vous en aurez besoin pour créer ou modifier votre instance de base de données SQL Server.

Étape 2 : Créer le rôle IAM qui sera utilisé par Amazon RDS

Si vous utilisez la console pour créer votre instance de base de données SQL Server, vous pouvez ignorer cette étape. Si vous utilisez l'interface de ligne de commande ou l'API RDS pour créer votre instance de base de données SQL Server, vous devez créer un rôle IAM qui utilise la stratégie IAM gérée `AmazonRDSDirectoryServiceAccess`. Ce rôle permet à Amazon RDS d'effectuer des appels vers AWS Directory Service en votre nom.

Si vous utilisez une stratégie personnalisée pour joindre un domaine, plutôt que la stratégie `AmazonRDSDirectoryServiceAccess` gérée par AWS, assurez-vous d'autoriser l'action `ds:GetAuthorizedApplicationDetails`. Cette exigence est en vigueur à compter de juillet 2019, suite à un changement de l'API AWS Directory Service.

La stratégie IAM suivante, `AmazonRDSDirectoryServiceAccess`, permet d'accéder à AWS Directory Service.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
            "ds:DescribeDirectories",
            "ds:AuthorizeApplication",
            "ds:UnauthorizeApplication",
            "ds:GetAuthorizedApplicationDetails"
        ],
      "Effect": "Allow",
```

```
      "Resource": "*"
    }
  ]
}
```

Créez un rôle IAM à l'aide de cette stratégie. Pour de plus amples informations sur la création de rôles IAM, veuillez consulter Création de stratégies gérées par le client dans le IAM Guide de l'utilisateur.

Étape 3 : Créer et configurer des utilisateurs et des groupes

Vous pouvez créer des utilisateurs et des groupes avec l'outil Utilisateurs et ordinateurs Active Directory. Cet outil fait partie des outils Services AD DS (Active Directory Domain Services) et Services AD LDS (Active Directory Lightweight Directory Services). Les utilisateurs représentent des individus ou des entités individuelles qui ont accès à votre annuaire. Les groupes sont très utiles pour octroyer ou refuser des privilèges à des groupes d'utilisateurs, plutôt que d'appliquer ces privilèges à chaque utilisateur.

Pour créer des utilisateurs et des groupes dans un annuaire AWS Directory Service, vous devez être connecté à une instance Windows EC2 membre de l'annuaire AWS Directory Service. Vous devez également être connecté en tant qu'utilisateur disposant de privilèges pour créer des utilisateurs et des groupes. Pour de plus amples informations, veuillez consulter Ajouter des utilisateurs et des groupes (Simple AD et AWS Managed Microsoft AD) dans le AWS Directory Service Administration Guide.

Étape 4 : Activer le trafic entre VPC entre le répertoire et l'instance de base de données

Si vous avez l'intention de rechercher l'annuaire et l'instance de base de données dans le même VPC, ignorez cette étape et passez à Étape 5 : Créer ou modifier une instance de base de données SQL Server (p. 683).

Si vous avez l'intention de rechercher l'annuaire et l'instance de base de données dans des VPC différents, configurez le trafic entre VPC à l'aide de l'appairage de VPC ou à l'aide de AWS Transit Gateway.

La procédure suivante active le trafic entre les VPC à l'aide de l'appairage de VPC. Suivez les instructions de Qu'est-ce que l'appairage de VPC ? dans le Guide de l'appairage Amazon Virtual Private Cloud.

Pour activer le trafic entre VPC à l'aide de l'appairage de VPC

1. Configurez les règles de routage de VPC appropriées afin de veiller à ce que le trafic réseau puisse être acheminé dans les deux sens.
2. Assurez-vous que le groupe de sécurité de l'instance de base de données puisse recevoir le trafic entrant depuis le groupe de sécurité de cet annuaire.
3. Assurez-vous qu'il n'existe aucune règle de liste de contrôle d'accès (ACL) pour bloquer le trafic.

Si un autre compte AWS possède l'annuaire, vous devez le partager.

Pour partager l'annuaire entre des comptes AWS

1. Commencez le partage de l'annuaire avec le compte AWS dans lequel l'instance de base de données sera créée en suivant les instructions du Didacticiel : Partage de votre annuaire AWS Managed Microsoft AD pour la jonction de domaines EC2 en toute transparence dans le Guide d'administration AWS Directory Service.
2. Connectez-vous à la console AWS Directory Service à l'aide du compte pour l'instance de base de données et assurez-vous que l'état du domaine est `SHARED` avant de poursuivre.
3. Lorsque vous êtes connecté à la console AWS Directory Service avec le compte de l'instance de base de données, notez la valeur de ID de l'annuaire. Vous utilisez cet ID pour joindre l'instance de base de données au domaine.

Étape 5 : Créer ou modifier une instance de base de données SQL Server

Créez ou modifiez une instance de base de données SQL Server en vue de son utilisation avec votre annuaire. Vous pouvez utiliser la console, l'interface de ligne de commande ou l'API RDS pour associer une instance de base de données à un annuaire. Vous pouvez effectuer cette opération de différentes manières :

- Créez une instance de base de données SQL Server à l'aide de la console, de la commande de l'interface de ligne de commande create-db-instance ou de l'opération d'API RDS CreateDBInstance.

  Pour obtenir des instructions, consultez Création d'une instance de base de données Amazon RDS (p. 146).
- Modifiez une instance de base de données SQL Server existante à l'aide de la console, de la commande de l'interface de ligne de commande modify-db-instance ou de l'opération d'API RDS ModifyDBInstance.

  Pour obtenir des instructions, consultez Modification d'une instance de base de données Amazon RDS (p. 243).
- Restaurez une instance de base de données SQL Server à partir d'un instantané de bases de données à l'aide de la console, de la commande de l'interface de ligne de commande restore-db-instance-from-db-snapshot ou de l'opération d'API RDS RestoreDBInstanceFromDBSnapshot.

  Pour obtenir des instructions, consultez Restauration à partir d'un instantané de base de données (p. 329).
- Restaurez une instance de base de données SQL Server à un instant dans le passé en utilisant la console, la commande de l'interface de ligne de commande restore-db-instance-to-point-in-time ou l'opération d'API RDS RestoreDBInstanceToPointInTime.

  Pour obtenir des instructions, consultez Restauration d'une instance de base de données à une date spécifiée (p. 365).

L'authentification Windows est uniquement prise en charge pour les instances de base de données SQL dans un VPC.

Pour que l'instance de base de données puisse utiliser l'annuaire de domaine que vous avez créé, les éléments suivants sont nécessaires :

- Pour Annuaire, vous devez choisir l'identifiant du domaine (`d-ID`) généré lors de la création de l'annuaire.
- Assurez-vous que le groupe de sécurité VPC dispose d'une règle sortante qui permet à l'instance de base de données de communiquer avec l'annuaire.

Lorsque vous utilisez AWS CLI, les paramètres suivants sont obligatoires pour que l'instance de base de données puisse utiliser l'annuaire que vous avez créé :

- Pour le paramètre `--domain`, vous devez indiquer l'identifiant du domaine (`d-ID`) généré lors de la création de l'annuaire.
- Pour le paramètre `--domain-iam-role-name`, utilisez le rôle que vous avez créé qui utilise la stratégie IAM gérée `AmazonRDSDirectoryServiceAccess`.

Par exemple, la commande d'interface de ligne de commande suivante modifie une instance de base de données de façon à utiliser un annuaire.

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --domain d-ID \
    --domain-iam-role-name role-name
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --domain d-ID ^
    --domain-iam-role-name role-name
```

> **Important**
>
> Si vous modifiez une instance de base de données de façon à activer l'authentification Kerberos, redémarrez l'instance de base de données après avoir effectué la modification.

Étape 6 : Créer des connexions SQL Server pour l'authentification Windows

Utilisez les informations d'identification de l'utilisateur principal Amazon RDS pour vous connecter à l'instance de base de données SQL Server de la même manière qu'à n'importe quelle instance de base de données. Étant donné que l'instance de base de données est jointe au domaine AWS Managed Microsoft AD, vous pouvez allouer les connexions et utilisateurs SQL. Vous effectuez cette opération à partir des utilisateurs et groupes Active Directory de votre domaine. Les autorisations pour la base de données sont gérées via des autorisations SQL Server standard accordées et révoquées en fonction des connexions Windows.

Pour qu'un utilisateur Active Directory puisse s'authentifier à SQL Server, une connexion Windows SQL Server doit exister pour l'utilisateur ou un groupe dont l'utilisateur est membre. Un contrôle précis des accès est géré par l'attribution ou la révocation d'autorisations pour ces connexions SQL Server. Un utilisateur qui n'a pas de connexion SQL Server ou qui n'appartient pas à un groupe avec une telle connexion ne peut pas accéder à l'instance de base de données SQL Server.

L'autorisation ALTER ANY LOGIN est requise pour créer une connexion SQL Server Active Directory. Si vous n'avez pas créé de connexion avec cette autorisation, connectez vous en tant qu'utilisateur principal de l'instance de base de données à l'aide de l'authentification SQL Server. Exécutez la commande DDL (Data Definition Language) suivante pour créer une connexion SQL Server pour un utilisateur ou un groupe Active Directory.

```
CREATE LOGIN [<user or group>] FROM WINDOWS WITH DEFAULT_DATABASE = [master],
   DEFAULT_LANGUAGE = [us_english];
```

Spécifiez les utilisateurs ou les groupes à l'aide du nom de connexion antérieur à Windows 2000 au format `domainName\login_name`. Vous ne pouvez pas utiliser un nom principal de l'utilisateur (UPN) au format `login_name@DomainName`. Pour de plus amples informations sur CREATE LOGIN, accédez à https://msdn.microsoft.com/en-us/library/ms189751.aspx dans la documentation Microsoft Developer Network.

Les utilisateurs (personnes et applications) de votre domaine peuvent désormais se connecter à l'instance SQL Server Amazon RDS à partir d'un ordinateur client joint au domaine à l'aide de l'authentification Windows.

Gestion d'une instance de base de données dans un domaine

Vous pouvez utiliser la console, l'AWS CLI ou l'API Amazon RDS pour gérer votre instance de base de données et sa relation avec votre domaine. Par exemple, vous pouvez déplacer l'instance de base de données dans, hors ou entre des domaines.

Par exemple, l'API Amazon RDS vous permet d'effectuer les actions suivantes :

- Pour tenter à nouveau une jonction de domaines pour une appartenance ayant échoué, utilisez l'opération d'API ModifyDBInstance et spécifiez l'ID d'annuaire de l'appartenance actuelle.
- Pour mettre à jour le nom du rôle IAM de l'appartenance, utilisez l'opération d'API `ModifyDBInstance` et spécifiez l'ID d'annuaire de l'appartenance actuelle et le nouveau rôle IAM.
- Pour supprimer une instance de base de données d'un domaine, utilisez l'opération d'API `ModifyDBInstance` et spécifiez `none` pour le paramètre de domaine.
- Pour déplacer une instance de base de données d'un domaine à un autre, utilisez l'opération d'API `ModifyDBInstance` et spécifiez l'identifiant du nouveau domaine en tant que paramètre de domaine.
- Pour répertorier l'appartenance pour chaque instance de base de données, utilisez l'opération d'API DescribeDBInstances.

Présentation de l'appartenance au domaine

Après la création ou la modification de votre instance de base de données, l'instance devient un membre du domaine. La console AWS indique le statut de l'appartenance au domaine pour l'instance de base de données. Le statut de l'instance de base de données peut avoir les valeurs suivantes :

- joined–L'instance est membre du domaine.
- joining–L'instance est en train de devenir membre du domaine.
- pending-join – L'appartenance de l'instance est en attente.
- pending-maintenance-join–AWS va tenter de faire de l'instance un membre du domaine pendant la prochaine fenêtre de maintenance planifiée.
- pending-removal–La suppression de l'instance du domaine est en attente.
- pending-maintenance-removal–AWS va tenter de supprimer l'instance du domaine pendant la prochaine fenêtre de maintenance planifiée.
- failed–Un problème de configuration a empêché l'instance d'effectuer la jonction du domaine. Vérifiez et corrigez votre configuration avant d'émettre à nouveau la commande de modification de l'instance.
- removing–La suppression de l'instance du domaine est en cours.

Une demande visant à devenir membre d'un domaine peut échouer à cause d'un problème de connectivité réseau ou d'un rôle IAM incorrect. Par exemple, vous pouvez créer une instance de base de données ou modifier une instance existante et faire échouer la tentative pour que l'instance de base de données devienne membre d'un domaine. Dans ce cas, émettez à nouveau la commande pour créer ou modifier l'instance de base de données, ou modifiez l'instance nouvellement créée pour rejoindre le domaine.

Connexion à SQL Server avec l'authentification Windows

Pour vous connecter à SQL Server via l'authentification Windows, vous devez être connecté à un ordinateur joint au domaine en tant qu'utilisateur de domaine. Après le lancement de SQL Server Management Studio, choisissez le type d'authentification Windows Authentication, comme illustré ci-après.

Restauration d'une instance de base de données SQL Server puis ajout de cette instance à un domaine

Vous pouvez restaurer un instantané de base de données ou effectuer une restauration à un instant donné (PITR) pour une instance de base de données SQL Server, puis l'ajouter à un domaine. Une fois que l'instance de base de données est restaurée, modifiez l'instance à l'aide du processus expliqué dans Étape 5 : Créer ou modifier une instance de base de données SQL Server (p. 683) afin d'ajouter l'instance de base de données à un domaine.

Intégration d'un Amazon RDS pour instance de base de données SQL Server avec Amazon S3

Vous pouvez transférer des fichiers entre une instance de base de données exécutant Amazon RDS pour SQL Server et un compartiment Amazon S3. Ainsi, vous pouvez utiliser Amazon S3 avec des fonctionnalités SQL, telles que BULK INSERT. Par exemple, vous pouvez télécharger des fichiers .csv, .xml, .txt, etc. depuis Amazon S3 vers l'hôte de l'instance de base de données, puis importer les données depuis `D:\S3\` dans la base de données. Tous les fichiers sont stockés dans `D:\S3\` sur l'instance de base de données.

Les limites suivantes s'appliquent :

- Les fichiers du dossier `D:\S3` sont supprimés du réplica de secours après un basculement sur des instances Multi-AZ. Pour de plus amples informations, veuillez consulter Limitations Multi-AZ pour l'intégration S3 (p. 698).
- L'instance de base de données et le compartiment S3 doivent se trouver dans la même région AWS.
- Si vous exécutez plusieurs tâches d'intégration S3 simultanément, les tâches s'exécutent de manière séquentielle et non en parallèle.

  Note

  Les tâches d'intégration S3 partagent la même file d'attente que les tâches de sauvegarde et de restauration natives. Vous pouvez uniquement disposer de deux tâches maximum en cours à tout moment dans cette file d'attente. Par conséquent, deux tâches de sauvegarde et de restauration natives en cours d'exécution bloquent toutes les tâches d'intégration S3.
- Vous devez réactiver la fonctionnalité d'intégration S3 sur les instances restaurées. Elle ne se propage pas depuis l'instance source vers l'instance restaurée. Les fichiers dans D:\S3 sont supprimés sur une instance restaurée.

- Le téléchargement vers l'instance de base de données est limité à 100 fichiers. En d'autres termes, il ne peut pas y avoir plus de 100 fichiers dans `D:\S3\`.
- Seuls les fichiers sans extension de fichier ou avec les extensions de fichiers suivantes sont pris en charge pour le téléchargement : .bcp, .csv, .dat, .fmt, .info, .lst, .tbl, .txt et .xml.

  Note

  Les fichiers avec l'extension de fichier .ispac sont pris en charge pour le téléchargement lorsque SQL Server Integration Services est activé. Pour de plus amples informations sur l'activation de SSIS, veuillez consulter SQL Server Integration Services (p. 724).
  Les fichiers avec les extensions de fichier suivantes sont pris en charge pour le téléchargement lorsque SQL Server Analysis Services est activé : .abf, .asdatabase, .configsettings, .deploymentoptions, .deploymenttargets et .xmla. Pour de plus amples informations sur l'activation de SSAS, veuillez consulter SQL Server Analysis Services (p. 713).
- Le compartiment S3 doit disposer du même propriétaire que le rôle (IAM) AWS Identity and Access Management lié. Par conséquent, l'intégration S3 entre comptes n'est pas prise en charge.
- Le compartiment S3 ne peut pas être ouvert au public.
- La taille des fichiers pour les chargements est limitée à 50 Go par fichier.

Rubriques

- Prérequis pour l'intégration RDS SQL Server avec S3 (p. 687)
- Activation de l'intégration RDS SQL Server avec S3 (p. 691)
- Transfert de fichiers entre RDS SQL Server et un compartiment S3 (p. 693)
- Limitations Multi-AZ pour l'intégration S3 (p. 698)
- Désactivation de l'intégration RDS SQL Server avec S3 (p. 698)

Pour de plus amples informations sur l'utilisation des fichiers dans Amazon S3, veuillez consulter Démarrer avec Amazon Simple Storage Service.

Prérequis pour l'intégration RDS SQL Server avec S3

Avant de commencer, recherchez ou créez le compartiment S3 que vous souhaitez utiliser. De plus, ajoutez des autorisations afin que l'instance de base de données RDS puisse accéder au compartiment S3. Pour configurer cet accès, vous créez une stratégie et un rôle IAM.

Console

Pour créer une stratégie IAM afin d'accéder à Amazon S3

1. Dans la console IAM Management Console, choisissez Stratégie dans le panneau de navigation.
2. Créez une nouvelle stratégie et utilisez l'onglet Éditeur visuel pour exécuter les étapes suivantes.
3. Pour Service, saisissez **`S3`** et choisissez le service S3.
4. Pour Actions, choisissez les actions suivantes pour accorder l'accès nécessaire à votre instance de base de données :

   - `ListAllMyBuckets` – Obligatoire
   - `ListBucket` – Obligatoire
   - `GetBucketACL` – Obligatoire
   - `GetBucketLocation` – Obligatoire
   - `GetObject` – Obligatoire pour télécharger des fichiers depuis S3 vers `D:\S3\`
   - `PutObject` – Obligatoire pour charger des fichiers depuis `D:\S3\` vers S3

- `ListMultipartUploadParts` – Obligatoire pour charger des fichiers depuis `D:\S3\` vers S3
- `AbortMultipartUpload` – Obligatoire pour charger des fichiers depuis `D:\S3\` vers S3

5. Pour Ressources, les options qui s'affichent dépendent des actions choisies dans l'étape précédente. Vous pourrez voir des options pour compartiment, objet ou les deux. Pour chacune d'entre elles, ajoutez l'Amazon Resource Name (ARN) approprié.

   Pour compartiment, ajoutez l'ARN du compartiment que vous souhaitez utiliser. Par exemple, si votre compartiment est nommé `example-bucket`, définissez l'ARN sur `arn:aws:s3:::example-bucket`.

   Pour objet, saisissez l'ARN pour le compartiment, puis choisissez l'une des options suivantes :

   - Pour accorder l'accès à tous les fichiers d'un compartiment spécifié, choisissez Tous pour le Bucket name (Nom du compartiment) et le Object name (Nom de l'objet).
   - Pour accorder l'accès à des fichiers ou des dossiers spécifiques, fournissez des ARNs pour les compartiments et objets spécifiques auxquels vous souhaitez que SQL Server accède.
6. Suivez les instructions dans la console jusqu'à la création de la stratégie.

   Ce qui précède est un guide abrégé pour configurer une stratégie. Pour obtenir des instructions détaillées sur la création de stratégies IAM, veuillez consulter Création de stratégies IAM dans le Guide de l'utilisateur IAM.

Pour créer un rôle IAM utilisant la stratégie IAM de la procédure précédente.

1. Dans la console IAM Management Console, choisissez Rôles dans le panneau de navigation.
2. Créez un rôle IAM et choisissez les options suivantes à mesure qu'elles s'affichent dans la console :

   - Service AWS
   - RDS
   - RDS – Ajoutez un rôle à la base de données

   Ensuite, choisissez Suivant : Autorisations en bas.
3. Pour Attach permissions policies (Attacher des stratégies d'autorisations), saisissez le nom de la stratégie IAM précédemment créée. Ensuite, choisissez la stratégie dans la liste.
4. Suivez les instructions dans la console jusqu'à la création du rôle.

   Ce qui précède est un guide abrégé pour configurer un rôle. Pour obtenir des instructions plus détaillées sur la création des rôles, veuillez consulter Rôles IAM dans le Guide de l'utilisateur IAM.

AWS CLI

Pour accorder à Amazon RDS l'accès à un compartiment Amazon S3

1. Créez une stratégie IAM qui accorde à Amazon RDS l'accès à un compartiment S3.

   Ajoutez les actions appropriées pour accorder l'accès nécessaire à votre instance de base de données :

   - `ListAllMyBuckets` – Obligatoire
   - `ListBucket` – Obligatoire
   - `GetBucketACL` – Obligatoire
   - `GetBucketLocation` – Obligatoire
   - `GetObject` – Obligatoire pour télécharger des fichiers depuis S3 vers `D:\S3\`

- `PutObject` – Obligatoire pour charger des fichiers depuis `D:\S3\` vers S3
- `ListMultipartUploadParts` – Obligatoire pour charger des fichiers depuis `D:\S3\` vers S3
- `AbortMultipartUpload` – Obligatoire pour charger des fichiers depuis `D:\S3\` vers S3

La commande AWS CLI suivante permet de créer une stratégie IAM nommée *`rds-s3-integration-policy`* avec ces options. Elle accorde un accès à un compartiment nommé *`your-s3-bucket-arn`*.

Example

Pour Linux, macOS ou 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/*"
            }
        ]
    }'
```

Pour Windows :

Veillez à remplacer les fins de ligne par celles prises en charge par votre interface (`^` au lieu de `\`). De plus, dans Windows, vous devez utiliser une séquence d'échappement sur tous les guillemets doubles avec un `\`. Pour éviter d'utiliser une séquence d'échappement sur tous les guillemets dans le JSON, vous pouvez l'enregistrer dans un fichier et le transmettre en tant que paramètre.

Tout d'abord, créez le fichier `policy.json` avec la stratégie d'autorisation suivante :

```
{
    "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/*"
        }
    ]
}
```

Ensuite, utilisez la commande suivante pour créer la stratégie :

```
aws iam create-policy ^
     --policy-name rds-s3-integration-policy ^
     --policy-document file://policy_file_path
```

2. Après avoir créé la stratégie, notez son ARN (Amazon Resource Name). Vous aurez besoin de l'ARN lors d'une étape ultérieure.
3. Créez un rôle IAM qu'Amazon RDS peut endosser en votre nom pour accéder à vos compartiments S3.

   La commande AWS CLI suivante crée le paramètre `rds-s3-integration-role` à cet effet.

   Example

   Pour Linux, macOS ou 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"
        }
      ]
    }'
```

   Pour Windows :

   Veillez à remplacer les fins de ligne par celles prises en charge par votre interface (`^` au lieu de `\`). De plus, dans Windows, vous devez utiliser une séquence d'échappement sur tous les guillemets doubles avec un `\`. Pour éviter d'utiliser une séquence d'échappement sur tous les guillemets dans le JSON, vous pouvez l'enregistrer dans un fichier et le transmettre en tant que paramètre.

Tout d'abord, créez le fichier `assume_role_policy.json` avec la stratégie suivante :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "rds.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Ensuite, utilisez la commande suivante pour créer le rôle IAM :

```
aws iam create-role ^
     --role-name rds-s3-integration-role ^
     --assume-role-policy-document file://assume_role_policy_file_path
```

Pour de plus amples informations, veuillez consulter Création d'un rôle pour déléguer des autorisations à un utilisateur IAM dans le Guide de l'utilisateur IAM.

4. Une fois le rôle IAM créé, notez son ARN. Vous aurez besoin de l'ARN lors d'une étape ultérieure.
5. Attachez la stratégie IAM que vous avez créée au rôle IAM que vous venez de créer.

   La commande AWS CLI suivante attache la stratégie au rôle nommé *`rds-s3-integration-role`*.

   Example

   Pour Linux, macOS ou Unix :

```
aws iam attach-role-policy \
    --policy-arn your-policy-arn \
    --role-name rds-s3-integration-role
```

   Pour Windows :

```
aws iam attach-role-policy ^
    --policy-arn your-policy-arn ^
    --role-name rds-s3-integration-role
```

   Remplacez *`your-policy-arn`* par l'ARN de stratégie que vous avez noté lors d'une étape précédente.

Activation de l'intégration RDS SQL Server avec S3

Dans la section suivante, vous trouverez comment activer l'intégration Amazon S3 avec Amazon RDS pour SQL Server. Pour utiliser une intégration S3, votre instance de base de données doit être associée au rôle IAM précédemment créé avant d'utiliser le paramètre feature-name `S3_INTEGRATION`.

Note

Pour ajouter un rôle IAM à une instance de base de données, le statut de l'instance de base de données doit être disponible.

Console

Pour associer le rôle IAM à votre instance de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Choisissez le nom de l'instance de base de données RDS SQL Server pour en afficher les détails.
3. Dans l'onglet Connectivity & security (Connexion et sécurité) de la section Gestion des rôles IAM, choisissez le rôle IAM à ajouter sous Add IAM roles to this instance (Ajouter des rôles IAM à cette instance).
4. Pour Fonction, choisissez S3_INTEGRATION.

5. Choisissez Add role (Ajouter un rôle).

AWS CLI

Pour ajouter le rôle IAM à l'instance de base de données RDS SQL Server

- La commande AWS CLI suivante ajoute votre rôle IAM à une instance de base de données RDS SQL Server nommée *mydbinstance*.

  Example

  Pour Linux, macOS ou Unix :

```
aws rds add-role-to-db-instance \
    --db-instance-identifier mydbinstance \
    --feature-name S3_INTEGRATION \
    --role-arn your-role-arn
```

  Pour Windows :

```
aws rds add-role-to-db-instance ^
    --db-instance-identifier mydbinstance ^
    --feature-name S3_INTEGRATION ^
    --role-arn your-role-arn
```

  Remplacez *your-role-arn* par l'ARN du rôle que vous avez noté lors d'une étape précédente. `S3_INTEGRATION` doit être spécifié pour l'option `--feature-name`.

Transfert de fichiers entre RDS SQL Server et un compartiment S3

Vous pouvez utiliser des procédures stockées Amazon RDS pour télécharger et charger des fichiers entre S3 et votre instance de base de données RDS. Vous pouvez également utiliser des procédures stockées Amazon RDS pour répertorier et supprimer des fichiers sur l'instance RDS.

Les fichiers que vous téléchargez depuis/chargez sur Amazon S3 sont stockés dans le dossier `D:\S3`. Il s'agit du seul dossier que vous pouvez utiliser pour accéder à vos fichiers. Vous pouvez organiser vos fichiers en sous-dossiers, qui sont créés pour vous lorsque vous incluez le dossier de destination lors du téléchargement.

Certaines des procédures stockées exigent que vous fournissiez un Amazon Resource Name (ARN) à votre compartiment et fichier Amazon S3. Le format pour votre ARN est `arn:aws:s3:::bucket_name/file_name`. Amazon S3 n'a pas besoin d'un numéro de compte ou d'une région AWS dans les ARN.

Les tâches d'intégration S3 s'exécutent de manière séquentielle, partagent la même file d'attente que la sauvegarde native et restaurent des tâches. Vous pouvez uniquement disposer de deux tâches maximum en cours à tout moment dans cette file d'attente. Le traitement de la tâche peut mettre jusqu'à cinq minutes avant de commencer.

Téléchargement des fichiers d'un compartiment Amazon S3 vers une instance de base de données SQL Server

Pour télécharger des fichiers depuis un compartiment S3 vers une instance de base de données RDS SQL Server, utilisez la procédure stockée Amazon RDS `msdb.dbo.rds_download_from_s3` avec les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`@s3_arn_of_file`	NVARCHAR	–	Obligatoire	L'ARN S3 du fichier à télécharger, par exemple : `arn:aws:s3:::bucket_name/mydata.csv`
`@rds_file_path`	NVARCHAR	–	Facultatif	Le chemin du fichier pour l'instance RDS. Si aucun n'est spécifié, le chemin du fichier est `D:\S3\<filename in s3>`. RDS prend en charge des chemins absolus et relatifs. Si vous souhaitez créer un sous-dossier, incluez-le dans le chemin du fichier.
`@overwrite_file`	INT	0	Facultatif	Écraser le fichier existant : 0 = Ne pas écraser 1 = Écraser

Vous pouvez télécharger des fichiers sans extension de fichier et des fichiers avec les extensions de fichier suivantes : .bcp, .csv, .dat, .fmt, .info, .lst, .tbl, .txt et .xml.

Note

Les fichiers avec l'extension de fichier .ispac sont pris en charge pour le téléchargement lorsque SQL Server Integration Services est activé. Pour de plus amples informations sur l'activation de SSIS, veuillez consulter SQL Server Integration Services (p. 724).
Les fichiers avec les extensions de fichier suivantes sont pris en charge pour le téléchargement lorsque SQL Server Analysis Services est activé : .abf, .asdatabase, .configsettings, .deploymentoptions, .deploymenttargets et .xmla. Pour de plus amples informations sur l'activation de SSAS, veuillez consulter SQL Server Analysis Services (p. 713).

L'exemple suivant illustre la procédure stockée pour télécharger des fichiers depuis 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;
```

L'exemple `rds_download_from_s3` créé un dossier nommé `seed_data` in `D:\S3\`, si le dossier n'existe pas encore. Ensuite, l'exemple télécharge le fichier source `bulk_data.csv` depuis S3 vers un nouveau fichier nommé `data.csv` sur l'instance de base de données. Si le fichier existait déjà, il est écrasé car le paramètre `@overwrite_file` est défini sur `1`.

Téléchargement des fichiers depuis une instance de base de données SQL Server vers un compartiment Amazon S3

Pour charger des fichiers depuis une instance de base de données RDS SQL Server vers un compartiment S3, utilisez la procédure stockée Amazon RDS `msdb.dbo.rds_upload_to_s3` avec les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`@s3_arn_of_file`	NVARCHAR	–	Obligatoire	L'ARN S3 du fichier à créer dans S3, par exemple : `arn:aws:s3:::bucket_name/mydata.csv`
`@rds_file_path`	NVARCHAR	–	Obligatoire	Le chemin du fichier à charger sur S3. Les chemins absolus et relatifs sont pris en charge.
`@overwrite_file`	INT	–	Facultatif	Écraser le fichier existant : 0 = Ne pas écraser 1 = Écraser

L'exemple suivant charge le fichier nommé `data.csv` depuis l'emplacement spécifié dans `D:\S3\seed_data\` vers un fichier `new_data.csv` dans le compartiment S3 spécifié par l'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;
```

Si le fichier existait déjà dans S3, il est écrasé car le paramètre @overwrite_file est défini sur `1`.

Liste des fichiers sur l'instance de base de données RDS

Pour répertorier les fichiers disponibles sur l'instance de base de données, utilisez une procédure stockée et une fonction. Tout d'abord, exécutez la procédure stockée suivante pour récupérer les détails depuis les fichiers dans `D:\S3\`.

```
exec msdb.dbo.rds_gather_file_details;
```

La procédure stockée retourne l'ID de la tâche. À l'instar d'autres tâches, cette procédure stockée s'exécute de manière asynchrone. Dès que le statut de la tâche est `SUCCESS`, vous pouvez utiliser l'ID de tâche dans la fonction `rds_fn_list_file_details` pour répertorier les fichiers et répertoires existants dans D:\S3\, comme illustré ci-dessous.

```
SELECT * FROM msdb.dbo.rds_fn_list_file_details(TASK_ID);
```

La fonction `rds_fn_list_file_details` retourne un tableau avec les colonnes suivantes.

Paramètre de sortie	Description
`filepath`	Chemin absolu du fichier (par exemple, `D:\S3\mydata.csv`)
`size_in_bytes`	Taille du fichier (en octets)
`last_modified_utc`	Date et heure de la dernière modification au format UTC
`is_directory`	Option qui indique si l'objet est un annuaire (`true`/`false`)

Suppression des fichiers sur l'instance RDS

Pour supprimer les fichiers disponibles sur l'instance de base de données, utilisez la procédure stockée Amazon RDS `msdb.dbo.rds_delete_from_filesystem` avec les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`@rds_file_path`	NVARCHAR	–	Obligatoire	Le chemin du fichier à supprimer. Les chemins absolus et relatifs sont pris en charge.
`@force_delete`	INT	0	Facultatif	Pour supprimer un annuaire, cet indicateur doit être inclus et défini sur `1`. `1` = supprimer un annuaire Ce paramètre est ignoré si vous supprimez un fichier.

Pour supprimer un annuaire, `@rds_file_path` doit se terminer par une barre oblique inverse (`\`) et `@force_delete` doit être défini sur `1`.

L'exemple suivant supprimer le fichier `D:\S3\delete_me.txt`.

```
exec msdb.dbo.rds_delete_from_filesystem
    @rds_file_path='D:\S3\delete_me.txt';
```

L'exemple suivant supprime l'annuaire `D:\S3\example_folder\`.

```
exec msdb.dbo.rds_delete_from_filesystem
    @rds_file_path='D:\S3\example_folder\',
    @force_delete=1;
```

Surveillance du statut d'une tâche de transfert de fichiers

Pour suivre le statut de votre tâche d'intégration S3, appelez la fonction `rds_fn_task_status`. Deux paramètres sont nécessaires. Le premier paramètre doit toujours être `NULL` car il ne s'applique pas à l'intégration S3. Le second paramètre accepte l'ID de tâche. Définissez le second paramètre sur `0` pour obtenir des résultats pour toutes les tâches.

Pour consulter une liste de toutes les tâches, définissez le premier paramètre sur `NULL` et le second sur `0`, comme illustré dans l'exemple suivant.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,0);
```

Pour obtenir une tâche spécifique, définissez le premier paramètre sur `NULL` et le second sur l'ID de tâche, comme illustré dans l'exemple suivant.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,42);
```

La fonction `rds_fn_task_status` retourne les informations suivantes.

Paramètre de sortie	Description
`task_id`	ID de la tâche
`task_type`	Pour l'intégration S3, des tâches peuvent avoir les types suivants : • `DOWNLOAD_FROM_S3` • `UPLOAD_TO_S3` • `LIST_FILES_ON_DISK` • `DELETE_FILES_ON_DISK`
`database_name`	Non applicable aux tâches d'intégration S3.
`% complete`	Progression de la tâche sous forme de pourcentage.
`duration(mins)`	Temps consacré à la tâche, en minutes.
`lifecycle`	État de la tâche. Les statuts possibles sont les suivants :

Paramètre de sortie	Description
	• `CREATED` – Après que vous avez appelé une des procédures stockées d'intégration S3, une tâche est créée et le statut est défini sur `CREATED`. • `IN_PROGRESS` – Après le démarrage d'une tâche, le statut est défini sur `IN_PROGRESS`. Le passage du statut `CREATED` à `IN_PROGRESS` peut prendre jusqu'à cinq minutes. • `SUCCESS` – Lorsqu'une tâche est terminée, le statut est défini sur `SUCCESS`. • `ERROR` – Si une tâche échoue, le statut est défini sur `ERROR`. Lisez la colonne `task_info` pour plus d'informations sur l'erreur. • `CANCEL_REQUESTED` – Après que vous avez appelé `rds_cancel_task`, le statut de la tâche est défini sur `CANCEL_REQUESTED`. • `CANCELLED` – Une fois une tâche annulée avec succès, l'état de la tâche est défini sur `CANCELLED`.
`task_info`	Informations supplémentaires sur la tâche. Si une erreur se produit pendant le traitement, cette colonne contient des informations sur l'erreur.
`last_updated`	Date et heure de la dernière mise à jour de l'état de la tâche.
`created_at`	Date et heure de création de la tâche.
`S3_object_arn`	L'ARN de l'objet S3 depuis lequel le téléchargement est effectué et vers lequel le chargement est effectué.
`overwrite_S3_backup_file`	Non applicable aux tâches d'intégration S3.
`KMS_master_key_arn`	Non applicable aux tâches d'intégration S3.
`filepath`	Chemin du fichier sur l'instance de base de données RDS.
`overwrite_file`	Option qui indique si un fichier existant a été écrasé.
`task_metadata`	Non applicable aux tâches d'intégration S3.

Annulation d'une tâche

Pour annuler une tâche d'intégration S3, utilisez la procédure stockée `msdb.dbo.rds_cancel_task` avec le paramètre `task_id`. Les tâches de suppression et la liste des tâches en cours ne peuvent pas être annulées. L'exemple suivant illustre une demande d'annulation d'une tâche.

```
exec msdb.dbo.rds_cancel_task @task_id = 1234;
```

Pour obtenir un aperçu de toutes els tâches et de leurs ID de tâche, utilisez la fonction `rds_fn_task_status`, telle que décrite dans Surveillance du statut d'une tâche de transfert de fichiers (p. 696).

Limitations Multi-AZ pour l'intégration S3

Sur des instances Multi-AZ, les fichiers du dossier `D:\S3` sont supprimés du réplica de secours après un basculement. Un basculement peut être planifié, par exemple, lors de modifications apportées à une instance de base de données telles que la modification de la classe d'instance ou la mise à niveau de la version du moteur. La planification d'un basculement peut être annulée, par exemple en cas d'arrêt de l'instance principale.

> **Note**
>
> Nous ne recommandons pas d'utiliser le dossier `D:\S3` pour le stockage de fichiers. La bonne pratique consiste à charger des fichiers créés dans Amazon S3 afin de les rendre durables, et à télécharger les fichiers lorsque vous avez besoin d'importer des données.

Pour déterminer l'heure du dernier basculement, vous pouvez utiliser la procédure stockée `msdb.dbo.rds_failover_time`. Pour de plus amples informations, veuillez consulter Détermination de l'heure du dernier basculement (p. 769).

Example de Aucun basculement récent

Cet exemple illustre la sortie lorsqu'il n'y a pas de basculement récent dans les journaux d'erreurs. Aucun basculement ne s'est produit depuis le 29/04/2020 à 23:59:00.01.

Par conséquent, tous les fichiers téléchargés après cette date et cette heure et qui n'ont pas été supprimés avec la procédure stockée `rds_delete_from_filesystem` sont toujours accessibles sur l'hôte actuel. Les fichiers téléchargés avant cette date et cette heure peuvent également être disponibles.

errorlog_available_from	recent_failover_time
2020-04-29 23:59:00.0100000	null

Example de Basculement récent

Cet exemple illustre la sortie lorsqu'un basculement récent est détecté dans les journaux d'erreurs. Le basculement le plus récent a eu lieu le 05/05/2020 à 18:57:51.89.

Tous les fichiers téléchargés après cette date et cette heure et qui n'ont pas été supprimés avec la procédure stockée `rds_delete_from_filesystem` sont toujours accessibles sur l'hôte actuel.

errorlog_available_from	recent_failover_time
2020-04-29 23:59:00.0100000	2020-05-05 18:57:51.8900000

Désactivation de l'intégration RDS SQL Server avec S3

Par la suite, vous trouverez comment désactiver l'intégration Amazon S3 avec Amazon RDS pour SQL Server. Les fichiers stockés dans `D:\S3\` ne sont pas supprimés lors de la désactivation de l'intégration S3.

> **Note**
>
> Pour supprimer un rôle IAM d'une instance de base de données, le statut de l'instance de base de données doit être `available`.

Console

Pour dissocier votre rôle IAM de votre instance de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Choisissez le nom de l'instance de base de données RDS SQL Server pour en afficher les détails.
3. Dans l'onglet Connectivity & security (Connectivité et sécurité) de la section Gérer les rôles IAM, choisissez le rôle IAM à supprimer.
4. Sélectionnez Delete.

AWS CLI

Pour supprimer le rôle IAM de l'instance de base de données RDS SQL Server

- La commande AWS CLI suivante supprime le rôle IAM d'une instance de base de données RDS SQL Server nommée *mydbinstance*.

  Example

  Pour Linux, macOS ou Unix :

```
aws rds remove-role-from-db-instance \
    --db-instance-identifier mydbinstance \
    --feature-name S3_INTEGRATION \
    --role-arn your-role-arn
```

  Pour Windows :

```
aws rds remove-role-from-db-instance ^
    --db-instance-identifier mydbinstance ^
    --feature-name S3_INTEGRATION ^
    --role-arn your-role-arn
```

  Remplacez *your-role-arn* par l'ARN du rôle IAM approprié pour l'option `--feature-name`.

Options pour le moteur de base de données Microsoft SQL Server

Dans cette section, vous trouverez des descriptions pour les options disponibles pour les instances Amazon RDS exécutant le moteur de base de données Microsoft SQL Server. Pour activer ces options, vous les ajoutez à un groupe d'options, puis associer celui-ci à votre instance de base de données. Pour plus d'informations, consultez Utilisation de groupes d'options (p. 209).

Si vous recherchez des fonctions facultatives qui ne sont pas ajoutées via les groupes d'options RDS (par exemple, SSL, authentification Microsoft Windows et intégration Amazon S3), consultez Fonctionnalités supplémentaires pour Microsoft SQL Server sur Amazon RDS (p. 668).

Amazon RDS prend en charge les options suivantes pour les instances de base de données Microsoft SQL Server.

Option	ID d'option	Editions de moteur
Sauvegarde et restauration natives (p. 701)	`SQLSERVER_BACKUP_RESTORE`	SQL Server Enterprise Edition SQL Server Standard Edition SQL Server Web Edition SQL Server Express Edition
Transparent Data Encryption (p. 704)	`TRANSPARENT_DATA_ENCRYPTION` (console RDS) `TDE` (AWS CLI et API RDS)	SQL Server 2012–2019 Enterprise Edition SQL Server 2019 Standard Edition
SQL Server Audit (p. 707)	`SQLSERVER_AUDIT`	Dans RDS, à partir de SQL Server 2012, toutes les éditions de SQL Server prennent en charge les audits au niveau du serveur, et l'édition Enterprise prend également en charge les audits au niveau de la base de données. À partir de SQL Server SQL Server 2016 (13.x) SP1, toutes les éditions prennent en charge les audits au niveau du serveur et les audits au niveau de la base de données. Pour de plus amples informations, consultez SQL Server Audit (moteur de base de données) dans la documentation SQL Server.
SQL Server Analysis Services (p. 713)	`SSAS`	SQL Server Enterprise Edition SQL Server Standard Edition
SQL Server Integration Services (p. 724)	`SSIS`	SQL Server Enterprise Edition

Option	ID d'option	Editions de moteur
		SQL Server Standard Edition
SQL Server Reporting Services (p. 738)	`SSRS`	SQL Server Enterprise Edition SQL Server Standard Edition
Microsoft Distributed Transaction Coordinator (p. 748)	`MSDTC`	Dans RDS, à partir de SQL Server 2012, toutes les éditions de SQL Server prennent en charge les transactions distribuées.

Prise en charge des sauvegarde et restauration natives dans SQL Server

La fonction de sauvegarde et restauration natives pour les bases de données SQL Server vous permet de créer une sauvegarde différentielle ou complète de votre base de données sur site et de stocker les fichiers de sauvegarde sur Amazon S3. Vous pouvez ensuite effectuer la restauration sur une instance de base de données Amazon RDS existante exécutant SQL Server. Vous pouvez également sauvegarder une base de données RDS SQL Server, la stocker sur Amazon S3, puis la restaurer dans d'autres emplacements. En outre, vous pouvez restaurer la sauvegarde sur un serveur sur site ou sur une autre instance de base de données Amazon RDS exécutant SQL Server. Pour de plus amples informations, consultez Importation et exportation de bases de données SQL Server (p. 634).

Amazon RDS prend en charge l'option de sauvegarde et restauration natives pour les bases de données Microsoft SQL Server à l'aide de fichiers de sauvegarde différentielle et complète (fichiers .bak).

Ajout de l'option de sauvegarde et restauration natives

Le processus général d'ajout de l'option de sauvegarde et restauration natives à une instance de base de données est le suivant :

1. Créer un groupe d'options ou copier ou modifier un groupe existant.
2. Ajoutez l'option `SQLSERVER_BACKUP_RESTORE` au groupe d'options.
3. Associez un rôle AWS Identity and Access Management (IAM) à l'option. Le rôle IAM doit avoir accès à un compartiment S3 pour stocker les sauvegardes de bases de données.

   Cela signifie qu'il doit avoir un ARN (Amazon Resource Name) valide au format `arn:aws:iam::`*`account-id`*`:role/`*`role-name`*. Pour plus d'informations, consultez Amazon Resource Names (ARN) dans le document AWS General Reference.
4. Associer un groupe d'options à une instance de base de données.

Après que vous avez ajouté l'option de sauvegarde et restauration natives, vous n'avez pas besoin de redémarrer votre instance de base de données. Dès que le groupe d'options est actif, vous pouvez commencer à sauvegarder et restaurer immédiatement.

Console

Pour ajouter l'option de sauvegarde et restauration natives

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Groupes d'options.
3. Créez un groupe d'options ou utilisez un groupe d'options existant. Pour de plus amples informations sur la création d'un groupe d'options de base de données personnalisé, veuillez consulter Création d'un groupe d'options (p. 212).

   Pour utiliser un groupe d'options existant, passez à l'étape suivante.
4. Ajoutez l'option SQLSERVER_BACKUP_RESTORE au groupe d'options. Pour plus d'informations sur l'ajout d'options, consultez Ajout d'une option à un groupe d'options (p. 214).
5. Effectuez l'une des actions suivantes :
   - Pour utiliser un rôle IAM existant et des paramètres Amazon S3, choisissez un rôle IAM existant pour Rôle IAM. Si vous utilisez un rôle IAM existant, RDS utilise les paramètres Amazon S3 que vous avez configurés pour ce rôle.
   - Pour créer un nouveau rôle et configurer de nouveaux paramètres Amazon S3, procédez comme suit :
     1. Pour Rôle IAM, choisissez Créer un rôle.
     2. Pour Select S3 Bucket (Sélectionner un compartiment S3), créez un compartiment S3 ou utilisez un compartiment S3 existant. Pour créer un nouveau compartiment, choisissez Create a New S3 Bucket (Créer un nouveau compartiment S3). Pour utiliser un compartiment existant, choisissez-le dans la liste.
     3. Pour Préfixe du chemin de dossier S3 (facultatif), saisissez un préfixe à utiliser pour les fichiers stockés dans votre compartiment Amazon S3.

        Ce préfixe peut inclure un chemin de fichier mais cela n'est pas obligatoire. Si vous fournissez un préfixe, RDS l'attache à tous les fichiers de sauvegarde. RDS utilise alors le préfixe durant une restauration pour identifier les fichiers connexes et ignorer les fichiers non concernés. Par exemple, vous pouvez utiliser le compartiment S3 pour d'autres choses que le stockage de fichiers de sauvegarde. Dans ce cas, vous pouvez utiliser le préfixe pour que RDS effectue une sauvegarde et restauration natives uniquement sur un dossier particulier et ses sous-dossiers.

        Si vous laissez le préfixe vide, RDS n'utilise pas de préfixe pour identifier les fichiers de sauvegarde ou les fichiers à restaurer. Par conséquent, lors d'une restauration de plusieurs fichiers, RDS tente de restaurer chaque fichier dans chaque dossier de ce compartiment S3.
     4. Pour Enable Encryption (Activer le chiffrement), choisissez Oui pour chiffrer le fichier de sauvegarde. Choisissez Non pour laisser le fichier de sauvegarde non chiffré.

        Si vous choisissez Oui, choisissez une clé de chiffrement pour Clé principale. Pour de plus amples informations sur les clés de chiffrement, veuillez consulter la section de Démarrez dans le AWS Key Management Service Developer Guide.
6. Sélectionnez Ajouter une option.
7. Appliquez le groupe d'options à une instance de base de données nouvelle ou existante:
   - Pour une nouvelle instance de base de données, appliquez le groupe d'options lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).
   - Pour une instance de base de données existante, appliquez le groupe d'options en modifiant l'instance et en attachant le nouveau groupe d'options. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Interface de ligne de commande

Cette procédure se base sur les hypothèses suivantes :

- Vous ajoutez l'option SQLSERVER_BACKUP_RESTORE à un groupe d'options qui existe déjà. Pour plus d'informations sur l'ajout d'options, consultez Ajout d'une option à un groupe d'options (p. 214).
- Vous associez l'option à un rôle IAM qui existe déjà et qui a accès à un compartiment S3 pour stocker les sauvegardes.
- Vous appliquez le groupe d'options à une instance de base de données qui existe déjà. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Pour ajouter l'option de sauvegarde et restauration natives

1. Ajoutez l'option `SQLSERVER_BACKUP_RESTORE` au groupe d'options.

   Example

   Pour Linux, macOS ou 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}]"
   ```

   Pour 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

   Lorsque vous utilisez l'invite de commande Windows, vous devez utiliser des guillemets doubles (") d'échappement dans le code JSON en les préfixant d'une barre oblique inverse (\).

2. Appliquez le groupe d'options à l'instance de base de données.

   Example

   Pour Linux, macOS ou Unix :

   ```
   aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --option-group-name mybackupgroup \
    --apply-immediately
   ```

   Pour Windows :

   ```
   aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --option-group-name mybackupgroup ^
    --apply-immediately
   ```

Modification des paramètres d'option de sauvegarde et restauration natives

Une fois que vous avez activé l'option de sauvegarde et restauration natives, vous pouvez modifier les paramètres de l'option. Pour plus d'informations sur la modification des paramètres d'options, consultez Modification d'un paramètre d'option (p. 219).

Suppression de l'option de sauvegarde et restauration natives

Vous pouvez désactiver la fonction de sauvegarde et restauration natives en supprimant l'option de votre instance de base de données. Une fois que vous avez supprimé l'option de sauvegarde et restauration natives, vous n'avez pas besoin de redémarrer votre instance de base de données.

Pour supprimer l'option de sauvegarde et restauration natives d'une instance de base de données, effectuez l'une des actions suivantes :

- Supprimez l'option du groupe d'options auquel elle appartient. Ce changement affecte toutes les instances de bases de données qui utilisent le groupe d'options. Pour plus d'informations, consultez Suppression d'une option d'un groupe d'options (p. 222).
- Modifiez l'instance de base de données et spécifiez un groupe d'options différent qui n'inclut pas l'option de sauvegarde et restauration natives. Ce changement affecte une seule instance de base de données. Vous pouvez spécifier le groupe d'options (vide) par défaut, ou un groupe d'options personnalisées différent. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Prise en charge de Transparent Data Encryption dans SQL Server

Amazon RDS prend en charge Transparent Data Encryption (TDE) pour le chiffrement des données stockées sur vos instances de base de données exécutant Microsoft SQL Server. La fonction TDE chiffre automatiquement les données avant qu'elles ne soient écrites sur le stockage et déchiffre automatiquement les données lorsqu'elles sont lues depuis le stockage.

Amazon RDS prend en charge TDE pour les versions et éditions suivantes de SQL Server :

- SQL Server 2019 Standard Edition et Enterprise Edition
- SQL Server 2017 Enterprise Edition
- SQL Server 2016 Enterprise Edition
- SQL Server 2014 Enterprise Edition
- SQL Server 2012 Enterprise Edition

Pour activer la fonction TDE pour une instance de base de données RDS SQL Server, spécifiez l'option TDE dans un groupe d'options RDS associé à cette instance de base de données.

La fonction TDE pour SQL Server fournit une gestion des clés de chiffrement à l'aide d'une architecture de clé à deux niveaux. Un certificat, qui est généré à partir de la clé principale de la base de données, permet de protéger les clés de chiffrement des données. La clé de chiffrement de la base de données exécute le chiffrement et le déchiffrement des données sur la base de données utilisateur. Amazon RDS sauvegarde et gère la clé principale de la base de données ainsi que le certificat TDE. Pour se conformer à plusieurs normes de sécurité, Amazon RDS travaille à implémenter une rotation automatique régulière de la clé principale.

La fonction TDE (Transparent Data Encryption) est utilisée dans les scénarios où vous devez chiffrer des données sensibles. Par exemple, vous pouvez souhaiter fournir des fichiers de données et des sauvegardes à un tiers, ou résoudre des problèmes de conformité réglementaire liés à la sécurité. Vous ne pouvez pas chiffrer les bases de données système pour SQL Server, telles que les bases de données `model` ou `master`.

Une présentation détaillée d'Oracle TDE dépasse le propos de ce guide, mais vous devez bien comprendre les points forts et les points faibles de chaque algorithme et de chaque clé. Pour plus d'informations sur le chiffrement TDE pour SQL Server, consultez Transparent Data Encryption (TDE) sur le site web de Microsoft.

Déterminez si votre instance de base de données est déjà associée à un groupe d'options ayant l'option TDE. Pour afficher le groupe d'options auquel une instance de base de données est associée, vous pouvez utiliser la console RDS, la commande describe-db-instance de l'AWS CLI ou l'opération d'API DescribeDBInstances.

Le processus d'activation d'Oracle TDE sur une instance de base de données SQL Server est le suivant :

1. Si l'instance de base de données n'est pas associée à un groupe d'options pour lequel TDE est activé, vous avez deux possibilités. Vous pouvez créer un groupe d'options et ajouter l'option TDE, ou vous pouvez modifier le groupe d'options associé pour l'ajouter.

   > **Note**
   >
   > Dans la console RDS, l'option est nommée `TRANSPARENT_DATA_ENCRYPTION`. Dans l'AWS CLI et l'API RDS, elle est nommée `TDE`.

   Pour plus d'informations sur la création ou la modification d'un groupe d'options, consultez Utilisation de groupes d'options (p. 209). Pour plus d'informations sur l'ajout d'une option à un groupe d'options, consultez Ajout d'une option à un groupe d'options (p. 214).
2. Associez l'instance de base de données au groupe d'options qui dispose de l'option TDE. Pour plus d'informations sur l'association d'une instance de base de données à un groupe d'options, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Lorsque l'option TDE est ajoutée à un groupe d'options, Amazon RDS génère un certificat qui est utilisé dans le processus de chiffrement. Vous pouvez alors utiliser le certificat pour exécuter les instructions SQL qui chiffrent les données d'une base de données sur l'instance de base de données. L'exemple suivant utilise le certificat créé par RDS et appelé `RDSTDECertificateName` pour chiffrer la base de données `customerDatabase`.

```
---------- Enabling TDE -------------

-- Find a RDSTDECertificate to use
USE [master]
GO
SELECT name FROM sys.certificates WHERE name LIKE 'RDSTDECertificate%'
GO

USE [customerDatabase]
GO
-- Create DEK using one of the certificates from the previous step
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_128
ENCRYPTION BY SERVER CERTIFICATE [RDSTDECertificateName]
GO

-- Enable encryption on the database
ALTER DATABASE [customerDatabase]
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
```

La durée du chiffrement d'une base de données SQL Server à l'aide de TDE dépend de plusieurs facteurs. Elle dépend notamment de la taille de l'instance de base de données, de l'activation ou non de PIOPS pour l'instance, de la quantité de données, et d'autres facteurs.

L'option TDE est une option persistante que vous ne pouvez pas supprimer d'un groupe d'options tant que l'ensemble des instances de base de données et des sauvegardes n'a pas été dissocié du groupe d'options. Une fois que vous avez ajouté l'option TDE à un groupe d'options, le groupe d'options peut uniquement être associé aux instances de bases de données qui utilisent TDE. Pour plus d'informations sur les options persistantes dans un groupe d'options, consultez Présentation des groupes d'options (p. 210).

Comme l'option TDE est une option persistante, un conflit peut se produire entre le groupe d'options et une instance de base de données associée. Vous pouvez avoir un conflit entre le groupe d'options et une instance de base de données associée dans les cas suivants :

- Le groupe d'options actuel a l'option TDE et vous le remplacez par un groupe d'options qui n'a pas l'option TDE.
- Vous restaurez à partir d'un instantané de base de données vers une nouvelle instance de base de données qui n'a pas de groupe d'options contenant l'option TDE. Pour plus d'informations sur ce scénario, consultez Considérations relatives au groupe d'options (p. 335).

Pour désactiver TDE pour une instance de base de données, assurez-vous d'abord qu'il ne reste pas d'objets chiffrés sur l'instance de base de données en déchiffrant les objets ou en les supprimant. Si un objet chiffré existe sur l'instance de base de données, vous ne pouvez pas désactiver TDE pour celle-ci. Quand vous utilisez la console pour supprimer l'option TDE d'un groupe d'options, la console indique qu'elle est en cours de traitement. En outre, un événement d'erreur est créé si le groupe d'options est associé à une instance de base de données ou un instantané de bases de données chiffré.

L'exemple suivant supprime le chiffrement TDE d'une base de données appelée `customerDatabase`.

```
------------- Removing TDE ----------------

USE [customerDatabase]
GO

-- Disable encryption on 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
GO
```

Lorsque tous les objets sont déchiffrés, vous disposez de deux options. Vous pouvez modifier l'instance de base de données pour l'associer à un groupe d'options sans l'option TDE. Vous pouvez également supprimer l'option TDE du groupe d'options.

Considérations relatives aux performances de SQL Server

Les performances d'une instance de base de données SQL Server peuvent être impactées par la fonction TDE.

Les performances des bases de données non chiffrées peuvent aussi être dégradées si les bases de données se trouvent sur une instance de base de données qui possède au moins une base de données chiffrée. En conséquence, il est recommandé de garder les bases de données chiffrées et les bases de données non chiffrées sur des instances de base de données distinctes.

En raison de la nature du chiffrement, la taille de la base de données et la taille du journal des transactions sont plus grandes que celle d'une base de données non chiffrée. Vous pouvez remplacer votre allocation d'espace de sauvegarde libre. La nature de TDE entraîne une baisse des performances inévitable. Si vous avez besoin de TDE et de performances élevées, mesurez l'impact et assurez-vous qu'il satisfait à vos besoins. L'impact sur les performances est moindre si vous utilisez IOPS provisionnées et au moins une classe d'instance de base de données M3.Large.

SQL Server Audit

Dans Amazon RDS, vous pouvez effectuer un audit des bases de données Microsoft SQL Server à l'aide du mécanisme d'audit SQL Server intégré. Vous pouvez créer des audits et des spécifications d'audit de la même manière que pour des serveurs de base de données sur site.

RDS charge les journaux d'audit terminés dans votre compartiment S3 à l'aide du rôle IAM que vous fournissez. Si vous activez la rétention, RDS conserve vos journaux d'audit sur votre instance de base de données pendant la période configurée.

Pour de plus amples informations, veuillez consulter SQL Server Audit (Database Engine) dans la documentation Microsoft SQL Server.

Rubriques

- Prise en charge de SQL Server Audit (p. 707)
- Ajout de SQL Server Audit aux options d'instance de base de données (p. 708)
- Utilisation de SQL Server Audit (p. 710)
- Consultation des journaux d'audit (p. 710)
- Utilisation de SQL Server Audit avec des instances multi-AZ (p. 711)
- Configuration d'un compartiment S3 (p. 711)
- Création manuelle d'un rôle IAM pour SQL Server Audit (p. 712)

Prise en charge de SQL Server Audit

Dans Amazon RDS à partir de SQL Server 2012, toutes les éditions de SQL Server prennent en charge les audits au niveau du serveur, et l'édition Enterprise prend également en charge les audits au niveau de la base de données. À partir de SQL Server 2016 (13.x) SP1, toutes les éditions prennent en charge les audits au niveau du serveur et au niveau de la base de données. Pour de plus amples informations, consultez SQL Server Audit (moteur de base de données) dans la documentation SQL Server.

RDS prend en charge la configuration des paramètres d'option suivants pour SQL Server Audit :

Paramètre d'option	Valeurs valides	Description
`IAM_ROLE_ARN`	Un Amazon Resource Name (ARN) valide au format `arn:aws:iam::account-id:role/role-name`.	L'ARN du rôle IAM accorde l'accès au compartiment S3 où vous voulez stocker vos journaux d'audit. Pour plus d'informations, consultez Amazon Resource Names (ARN) dans le document AWS General Reference.
`S3_BUCKET_ARN`	Un ARN valide au format `arn:aws:s3:::bucket-name` ou `arn:aws:s3:::bucket-name/key-prefix`	L'ARN du compartiment S3 où vous voulez stocker vos journaux d'audit.
`ENABLE_COMPRESSION`	`true` ou `false`	Contrôle la compression des journaux d'audit. Par défaut, la compression est activée (définie sur `true`).
`RETENTION_TIME`	`0` sur `840`	Durée de conservation (en heures) pendant laquelle les enregistrements d'audit SQL Server sont conservés sur votre instance RDS. Par défaut, la conservation est désactivée.

RDS prend en charge SQL Server Audit dans toutes les régions AWS sauf Moyen-Orient (Bahreïn).

Ajout de SQL Server Audit aux options d'instance de base de données

L'activation de SQL Server Audit se fait en deux étapes : l'activation de l'option sur l'instance de base de données et l'activation de la fonction dans SQL Server. Le processus d'ajout de l'option SQL Server Audit à une instance de base de données est le suivant :

1. Créer un groupe d'options ou copier ou modifier un groupe existant.
2. Ajouter et configurer toutes les options requises.
3. Associer un groupe d'options à une instance de base de données.

Une fois que vous avez ajouté l'option SQL Server Audit, vous n'avez pas besoin de redémarrer votre instance de base de données. Dès que le groupe d'options est actif, vous pouvez créer des audits et stocker les journaux d'audit dans votre compartiment S3.

Pour ajouter et configurer SQL Server Audit sur le groupe d'options d'une instance de base de données

1. Choisissez l'une des méthodes suivantes :
   - Utiliser un groupe d'options existant.
   - Créer un groupe d'options d'instance de base de données personnalisé et utiliser ce groupe d'options. Pour plus d'informations, consultez Création d'un groupe d'options (p. 212).

2. Ajoutez l'option SQLSERVER_AUDIT au groupe d'options et configurez les paramètres de l'option. Pour plus d'informations sur l'ajout d'options, consultez Ajout d'une option à un groupe d'options (p. 214).
   - Pour Rôle IAM, si vous avez déjà un rôle IAM avec les stratégies requises, vous pouvez choisir ce rôle. Pour créer un nouveau rôle IAM choisissez Créer un rôle. Pour plus d'informations sur les stratégies requises, consultez Création manuelle d'un rôle IAM pour SQL Server Audit (p. 712).
   - Pour Select S3 destination (Sélectionner une destination S3), si vous avez déjà un compartiment S3 que vous souhaitez utiliser, choisissez-le. Pour créer un compartiment S3, choisissez Create a New S3 Bucket (Créer un nouveau compartiment S3).
   - Pour Enable Compression (Activer la compression), laissez cette option cochée pour compresser les fichiers d'audit. La compression est activée par défaut. Pour désactiver la compression, désélectionnez Enable Compression (Activer la compression).
   - Pour Audit log retention (Rétention des journaux d'audit), pour conserver les enregistrement sue l'instance de base de données, choisissez cette option. Spécifiez une durée de rétention en heures. La durée de rétention maximale est de 35 jours.
3. Appliquez le groupe d'options à une instance de base de données nouvelle ou existante. Choisissez l'une des méthodes suivantes :
   - Si vous créez une nouvelle instance de base de données, appliquez le groupe d'options lorsque vous lancez l'instance.
   - Sur une instance de base de données existante, appliquez le groupe d'options en modifiant l'instance et en attachant le nouveau groupe d'options. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Modification de l'option SQL Server Audit

Une fois que vous avez activé l'option SQL Server Audit, vous pouvez modifier les paramètres. Pour de plus amples informations sur la modification des paramètres d'options, veuillez consulter Modification d'un paramètre d'option (p. 219).

Suppression de SQL Server Audit des options d'instance de base de données

Vous pouvez désactiver la fonction SQL Server Audit en désactivant les audits, puis en supprimant l'option.

Pour supprimer les audits

1. Désactivez tous les paramètres d'audit au sein de SQL Server. Pour savoir où les audits s'exécutent, interrogez les vues du catalogue de sécurité SQL Server. Pour plus d'informations, consultez Security Catalog Views dans la documentation Microsoft SQL Server.
2. Supprimez l'option SQL Server Audit de l'instance de base de données. Choisissez l'une des méthodes suivantes :
   - Supprimez l'option SQL Server Audit du groupe d'options utilisé par l'instance de base de données. Ce changement affecte toutes les instances de bases de données qui utilisent le même groupe d'options. Pour plus d'informations, consultez Suppression d'une option d'un groupe d'options (p. 222).
   - Modifiez l'instance de base de données, puis choisissez le groupe d'options sans l'option SQL Server Audit. Cette modification affecte uniquement l'instance de base de données que vous modifiez. Vous pouvez spécifier le groupe d'options (vide) par défaut, ou un groupe d'options personnalisées différent. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).
3. Après que vous avez supprimé l'option SQL Server Audit de l'instance de base de données, vous n'avez pas besoin de redémarrer l'instance. Supprimez les fichiers d'audit non requis de votre compartiment S3.

Utilisation de SQL Server Audit

Vous pouvez contrôler les audits de serveur, les spécifications d'audit de serveur et les spécifications d'audit de base de données, de la même manière que vous les contrôlez pour vos serveurs de base de données sur site.

Création d'audits

Vous pouvez créer des audits de serveur de la même manière que pour des serveurs de base de données sur site. Pour plus d'informations sur la création d'audits de serveur, consultez CREATE SERVER AUDIT dans la documentation Microsoft SQL Server.

Pour éviter les erreurs, respectez les limitations suivantes :

- Ne dépassez pas le nombre maximal d'audits de serveur pris en charge par instance de 50.
- Demandez à SQL Server d'écrire les données dans un fichier binaire.
- N'utilisez pas `RDS_` comme préfixe dans le nom de l'audit de serveur.
- Pour `FILEPATH`, spécifiez `D:\rdsdbdata\SQLAudit`.
- Pour `MAXSIZE`, spécifiez une taille comprise entre 2 Mo et 50 Mo.
- Ne configurez pas `MAX_ROLLOVER_FILES` ou `MAX_FILES`.
- Ne configurez pas SQL Server pour arrêter l'instance de bases de données s'il ne parvient pas à écrire l'enregistrement d'audit.

Création de spécifications d'audit

Vous créez des spécifications d'audit de serveur et des spécifications d'audit de base de données, de la même manière que vous les créez pour vos serveurs de base de données sur site. Pour plus d'informations sur la création de spécifications d'audit, consultez CREATE SERVER AUDIT SPECIFICATION et CREATE DATABASE AUDIT SPECIFICATION dans la documentation Microsoft SQL Server.

Pour éviter les erreurs, n'utilisez pas `RDS_` comme préfixe dans le nom de la spécification d'audit de base de données ou la spécification d'audit de serveur.

Consultation des journaux d'audit

Vos journaux d'audit sont stockés dans `D:\rdsdbdata\SQLAudit`.

Après que SQL Server a fini d'écrire dans un fichier de journal d'audit (quand le fichier atteint sa limite de taille), Amazon RDS charge le fichier dans votre compartiment S3. Si la rétention est activée, Amazon RDS déplace le fichier vers le dossier de rétention : `D:\rdsdbdata\SQLAudit\transmitted`.

Pour plus d'informations sur la rétention, consultez Ajout de SQL Server Audit aux options d'instance de base de données (p. 708).

Les enregistrements d'audit sont conservés sur l'instance de base de données jusqu'à ce que le fichier de journal soit chargé. Vous pouvez afficher les enregistrements d'audit en exécutant la commande suivante.

```
SELECT   *
 FROM     msdb.dbo.rds_fn_get_audit_file
              ('D:\rdsdbdata\SQLAudit\*.sqlaudit'
              , default
              , default )
```

Vous pouvez utiliser la même commande pour afficher les enregistrements d'audit de votre dossier de rétention en modifiant le filtre en `D:\rdsdbdata\SQLAudit\transmitted\*.sqlaudit`.

```
SELECT   *
 FROM     msdb.dbo.rds_fn_get_audit_file
             ('D:\rdsdbdata\SQLAudit\transmitted\*.sqlaudit'
             , default
             , default )
```

Utilisation de SQL Server Audit avec des instances multi-AZ

Pour les instances multi-AZ, le processus d'envoi de fichiers de journal d'audit à Amazon S3 est similaire au processus utilisé pour les instances mono-AZ. Cependant, il existe quelques différences importantes :

- Les objets de spécification d'audit de base de données sont répliqués vers tous les nœuds.
- Les audits de serveur et les spécifications d'audit de serveur ne sont pas répliqués vers les nœuds secondaires. Vous devez les créer et les modifier manuellement.

Pour capturer des audits de serveur ou une spécification d'audit de serveur depuis les deux nœuds :

1. Créez un audit de serveur ou une spécification d'audit de serveur sur le nœud primaire.
2. Basculez vers le nœud secondaire, puis créez un audit de serveur ou une spécification d'audit de serveur avec les mêmes nom et GUID sur le nœud secondaire. Utilisez le paramètre `AUDIT_GUID` pour spécifier le GUID.

Configuration d'un compartiment S3

Les fichiers journaux d'audit sont chargés automatiquement depuis l'instance de base de données vers votre compartiment S3. Les restrictions suivantes s'appliquent au compartiment S3 que vous utilisez comme cible pour vos fichiers d'audit :

- Il doit se situer dans la même région AWS que l'instance de base de données.
- Il ne doit pas être ouvert au public.
- Le propriétaire du compartiment doit également être le propriétaire du rôle IAM.

La clé cible qui est utilisée pour stocker les données suit ce schéma de dénomination : `bucket-name/key-prefix/instance-name/audit-name/node_file-name.ext`

> **Note**
>
> Vous définissez le nom du compartiment et les valeurs de préfixe de clé avec le paramètre d'option (`S3_BUCKET_ARN`.

Le schéma est composé des éléments suivants :

- **`bucket-name`** – Nom de votre compartiment S3.
- **`key-prefix`** – Préfixe de clé personnalisé que vous souhaitez utiliser pour les journaux d'audit.
- **`instance-name`** – Nom de votre instance Amazon RDS.
- **`audit-name`** – Nom de l'audit.
- **`node`** – Identifiant du nœud constituant la source des journaux d'audit (`node1` or `node2`). Il existe un nœud pour une instance mono-AZ et deux nœuds de réplication pour une instance multi-AZ. Il ne s'agit pas des nœuds primaires et secondaires, car les rôles des nœuds primaires et secondaires au fil du temps. L'identificateur de nœud est une simple étiquette.
  - **`node1`** – Premier nœud de la réplication (une instance mono-AZ ne comporte qu'un seul nœud).

  - **node2** – Deuxième nœud de la réplication (une instance multi-AZ ne comporte deux nœuds).
- **file-name** – Nom du fichier cible. Le nom du fichier est pris tel quel de SQL Server.
- **ext** – Extension du fichier (`zip` ou `sqlaudit`):
  - **zip** – Si la compression est activée (par défaut).
  - **sqlaudit** – Si la compression est désactivée.

Création manuelle d'un rôle IAM pour SQL Server Audit

En règle générale, lorsque vous créez une nouvelle option, AWS Management Console crée le rôle IAM et la stratégie d'approbation IAM pour vous. Cependant, vous pouvez créer manuellement un rôle IAM à utiliser avec les audits SQL Server pour pouvoir le personnaliser avec les exigences supplémentaires que vous pourriez avoir. Pour ce faire, vous créez un rôle IAM et vous déléguez des autorisations pour que le service Amazon RDS puisse utiliser votre compartiment Amazon S3. Lorsque vous créez ce rôle IAM, vous attachez des stratégies d'approbation et d'autorisation. La stratégie d'approbation permet à Amazon RDS d'assumer ce rôle. La stratégie d'autorisation définit les actions que ce rôle peut exécuter. Pour plus d'informations, consultez Création d'un rôle pour déléguer des autorisations à un service AWS dans le Guide de l'utilisateur AWS Identity and Access Management.

Vous pouvez utiliser les exemples de cette section pour créer les stratégies d'approbation et d'autorisation dont vous avez besoin.

Voici un exemple de stratégie d'approbation de rôle pour SQL Server Audit. La stratégie utilise le mandataire de service `rds.amazonaws.com` pour autoriser RDS à écrire dans le compartiment S3. Un mandataire de service est un identifiant utilisé pour accorder des autorisations à un service. Chaque fois que vous autorisez l'accès à `rds.amazonaws.com` de cette manière, vous autorisez RDS à exécuter une action en votre nom. Pour de plus amples information sur les mandataires de service, veuillez consulter Éléments de stratégie JSON : mandataire.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Effect": "Allow",
             "Principal": {
                 "Service": "rds.amazonaws.com"
             },
             "Action": "sts:AssumeRole"
         }
     ]
 }
```

Dans l'exemple suivant de stratégie d'autorisation pour SQL Server Audit, nous spécifions un Amazon Resource Name (ARN) pour le compartiment Amazon S3. Vous pouvez utiliser des ARN pour identifier un compte, un utilisateur ou un rôle spécifique auquel vous souhaitez accorder l'accès. Pour de plus amples informations sur l'utilisation des ARN, veuillez consulter Amazon Resource Names (ARN).

```
{
     "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/key_prefix/*"
        }
    ]
}
```

Note

L'action `s3:ListAllMyBuckets` est requise pour vérifier que le même compte AWS possède à la fois le compartiment S3 et l'instance de base de données SQL Server. L'action répertorie les noms des compartiments du compte.
Les espaces de noms de compartiment S3 sont globaux. Si vous supprimez accidentellement votre compartiment, un autre utilisateur peut créer un compartiment portant le même nom dans un compte différent. Ensuite, les données d'audit SQL Server sont écrites dans le nouveau compartiment.

Prise en charge de SQL Server Analysis Services dans Amazon RDS pour SQL Server

Microsoft SQL Server Analysis Services (SSAS) fait partie de la suite Microsoft Business Intelligence (MSBI). SSAS est un outil de traitement analytique en ligne (OLAP) et d'exploration de données installé dans SQL Server. Vous utilisez SSAS pour analyser des données et vous aider ainsi à prendre des décisions professionnelles. SSAS diffère de la base de données relationnelle SQL Server, car SSAS est optimisé pour les requêtes et les calculs, courants dans un environnement de veille économique. Pour plus d'informations sur SSAS, consultez la documentation Analysis Services de Microsoft.

Amazon RDS pour SQL Server prend en charge l'exécution de SQL Server Analysis Services (SSAS) en mode tabulaire. Vous pouvez activer SSAS sur des instances de base de données existantes ou nouvelles. Il est installé sur la même instance de base de données que votre moteur de base de données.

RDS prend en charge SSAS pour SQL Server éditions Standard et Enterprise sur les versions suivantes :

- SQL Server 2017, version 14.00.3223.3.v1 et ultérieure
- SQL Server 2016, version 13.00.5426.0.v1 et ultérieure

Limites

Les limitations suivantes s'appliquent à l'exécution de SSAS sur RDS pour SQL Server :

- Le mode tabulaire est le seul mode pris en charge pour SSAS.
- Les instances multi-AZ ne sont pas prises en charge.
- Les instances doivent utiliser AWS Directory Service for Microsoft Active Directory (Enterprise Edition) pour l'authentification SSAS.

- Les utilisateurs ne disposent pas d'un accès administrateur au serveur SSAS, mais ils peuvent avoir un accès administrateur au niveau de la base de données.
- Le seul port pris en charge pour accéder à SSAS est le port 2383.
- Vous ne pouvez pas déployer de projets directement. Nous fournissons une procédure stockée fournie par RDS pour cela. Pour plus d'informations, consultez Déploiement de projets SSAS sur Amazon RDS (p. 718).
- Le traitement pendant le déploiement n'est pas pris en charge.
- L'utilisation de fichiers .xmla pour le déploiement n'est pas prise en charge.
- Les fichiers d'entrée du projet SSAS et les fichiers de sortie de la sauvegarde de base de données peuvent se trouver uniquement dans le dossier `D:\S3` de l'instance de base de données.

Activation de SSAS

Utilisez la procédure suivante pour activer SSAS pour votre instance de base de données :

1. Créez un groupe d'options ou choisissez un groupe d'options existant.
2. Ajoutez l'option `SSAS` au groupe d'options.
3. Associez le groupe d'options à l'instance de base de données.
4. Autorisez l'accès entrant au groupe de sécurité VPC pour le port d'écoute SSAS.
5. Activez l'intégration Amazon S3

Création du groupe d'options pour SSAS

Utilisez AWS Management Console ou l'AWS CLI pour créer un groupe d'options correspondant au moteur SQL Server et à la version de l'instance de base de données que vous prévoyez d'utiliser.

> **Note**
>
> Vous pouvez également utiliser un groupe d'options existant s'il convient au moteur et à la version SQL Server.

Console

La procédure de console suivante crée un groupe d'options pour SQL Server Standard Edition 2017.

Pour créer le groupe d'options

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes d'options.
3. Choisissez Créer un groupe.
4. Dans la fenêtre Créer un groupe d'options, procédez comme suit :
   a. Pour Nom, attribuez au groupe d'options un nom unique au sein de votre compte AWS, par exemple **`ssas-se-2017`**. Le nom ne peut contenir que des lettres, des chiffres et des tirets.
   b. Pour Description, saisissez une brève description du groupe d'options, par exemple **`SSAS option group for SQL Server SE 2017`**. La description est utilisée à des fins d'affichage.
   c. Pour Moteur, choisissez sqlserver-se.
   d. Pour Version majeure du moteur, choisissez 14.00.
5. Sélectionnez Créer.

Interface de ligne de commande

L'exemple d'interface de ligne de commande suivant crée un groupe d'options pour SQL Server Standard Edition 2017.

Pour créer le groupe d'options

- Utilisez l'une des commandes suivantes.

  Example

  Pour Linux, macOS ou 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"
```

  Pour 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"
```

Ajout de l'option SSAS au groupe d'options

Ensuite, utilisez AWS Management Console ou l'AWS CLI pour ajouter l'option `SSAS` au groupe d'options.

Console

Pour ajouter l'option SSAS

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Groupes d'options.
3. Choisissez le groupe d'options que vous venez de créer.
4. Sélectionnez Ajouter une option.
5. Sous Option details (Détails de l'option), choisissez SSAS pour Option name (Nom de l'option).
6. Sous Paramètres d'option, entrez une valeur de 10–80 pour Max memory (Mémoire max.).

   Max memory (Mémoire max.) spécifie le seuil supérieur au-delà duquel SSAS commence à libérer de la mémoire de manière plus agressive pour laisser de la place aux requêtes en cours d'exécution et hautement prioritaires. Le nombre correspond à un pourcentage de la mémoire totale de l'instance de base de données. Les valeurs autorisées sont 10–80, et celle par défaut est 45.

   Note

   Le port permettant d'accéder à SSAS, 2383, est prérempli.
7. Pour Groupes de sécurité, choisissez le groupe de sécurité VPC à associer à l'option.
8. Sous Scheduling (Planification), choisissez si vous souhaitez ajouter l'option immédiatement ou lors du créneau de maintenance suivant.
9. Sélectionnez Ajouter une option.

Interface de ligne de commande

Pour ajouter l'option SSAS

1. Créez un fichier JSON, par exemple `ssas-option.json`, avec les paramètres suivants :
   - `OptionGroupName` – Nom du groupe d'options que vous avez créé ou choisi précédemment (`ssas-se-2017` dans l'exemple suivant).
   - `Port` – Port que vous utilisez pour accéder à SSAS. Le seul port pris en charge est 2383.
   - `VpcSecurityGroupMemberships` – Appartenances au groupe de sécurité VPC pour votre instance de base de données RDS.
   - `MAX_MEMORY` – Seuil supérieur au-delà duquel SSAS doit commencer à libérer de la mémoire de manière plus agressive pour laisser de la place aux requêtes en cours d'exécution et hautement prioritaires. Le nombre correspond à un pourcentage de la mémoire totale de l'instance de base de données. Les valeurs autorisées sont 10–80, et celle par défaut est 45.

```
{
"OptionGroupName": "ssas-se-2017",
"OptionsToInclude": [
 {
 "OptionName": "SSAS",
 "Port": 2383,
 "VpcSecurityGroupMemberships" : ["sg-0abcdef123"],
 "OptionSettings": [{"Name" : "MAX_MEMORY","Value" : "60"}]
 }],
"ApplyImmediately": true
}
```

2. Ajoutez l'option `SSAS` au groupe d'options.

   Example

   Pour Linux, macOS ou Unix :

```
aws rds add-option-to-option-group \
    --cli-input-json file://ssas-option.json \
    --apply-immediately
```

   Pour Windows :

```
aws rds add-option-to-option-group ^
    --cli-input-json file://ssas-option.json ^
    --apply-immediately
```

Association du groupe d'options à votre instance de base de données

Vous pouvez utiliser AWS Management Console ou l'AWS CLI pour associer le groupe d'options à votre instance de base de données.

Console

Associez votre groupe d'options à une instance de base de données nouvelle ou existante :

- Pour une nouvelle instance de base de données, associez le groupe d'options à l'instance de base de données lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).

- Pour une instance de base de données existante, modifiez l'instance et associez-lui le nouveau groupe d'options. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

  Note

  Si vous utilisez une instance existante, un domaine Active Directory et un rôle IAM doivent déjà lui être associés. Si vous créez une instance, spécifiez un domaine Active Directory et un rôle IAM existants. Pour plus d'informations, consultez Utilisation de l'authentification Windows avec une instance de base de données Amazon RDS pour SQL Server (p. 676).

Interface de ligne de commande

Vous pouvez associer votre groupe d'options à une instance de base de données nouvelle ou existante.

Note

Si vous utilisez une instance existante, un domaine Active Directory et un rôle IAM doivent déjà lui être associés. Si vous créez une instance, spécifiez un domaine Active Directory et un rôle IAM existants. Pour plus d'informations, consultez Utilisation de l'authentification Windows avec une instance de base de données Amazon RDS pour SQL Server (p. 676).

Pour créer une instance de base de données utilisant le groupe d'options

- Spécifiez le type de moteur de base de données et la version majeure utilisés lors de la création du groupe d'options.

  Example

  Pour Linux, macOS ou 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
```

  Pour 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
```

Pour modifier une instance de base de données afin d'y associer le groupe d'options

- Utilisez l'une des commandes suivantes.

  Example

  Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier myssasinstance \
    --option-group-name ssas-se-2017 \
    --apply-immediately
```

  Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier myssasinstance ^
    --option-group-name ssas-se-2017 ^
    --apply-immediately
```

Autorisation de l'accès entrant à votre groupe de sécurité VPC

Créez une règle entrante pour le port d'écoute SSAS spécifié dans le groupe de sécurité VPC associé à votre instance de base de données. Pour de plus amples informations sur la configuration des groupes de sécurité, veuillez consulter Créer un groupe de sécurité qui autorise l'accès à votre instance de base de données dans votre VPC (p. 66).

Activation de l'intégration S3

Pour télécharger des fichiers de configuration de modèle sur votre hôte pour le déploiement, utilisez l'intégration S3. Pour plus d'informations, consultez Intégration d'un Amazon RDS pour instance de base de données SQL Server avec Amazon S3 (p. 686).

Déploiement de projets SSAS sur Amazon RDS

Sur RDS, vous ne pouvez pas déployer de projets SSAS directement avec SQL Server Management Studio (SSMS). Pour déployer des projets, utilisez une procédure stockée de RDS.

> **Note**
>
> L'utilisation de fichiers .xmla pour le déploiement n'est pas prise en charge.

Avant de déployer des projets, vérifiez les points suivants :

- L'intégration S3 est activée. Pour plus d'informations, consultez Intégration d'un Amazon RDS pour instance de base de données SQL Server avec Amazon S3 (p. 686).
- Le paramètre de configuration `Processing Option` est défini sur `Do Not Process`. Ce paramètre signifie qu'aucun traitement n'est effectué après le déploiement.
- Vous disposez des fichiers *`myssasproject`*`.asdatabase` et *`myssasproject`*`.deploymentoptions`. Ils sont générés automatiquement lorsque vous créez le projet SSAS.

Pour déployer un projet SSAS sur RDS

1. Téléchargez le fichier `.asdatabase` (modèle SSAS) de votre compartiment S3 dans votre instance de base de données, comme illustré dans l'exemple suivant. Pour plus d'informations sur les paramètres

de téléchargement, consultez Téléchargement des fichiers d'un compartiment Amazon S3 vers une instance de base de données SQL Server (p. 693).

```
exec msdb.dbo.rds_download_from_s3
@s3_arn_of_file='arn:aws:s3:::bucket_name/myssasproject.asdatabase',
[@rds_file_path='D:\S3\myssasproject.asdatabase'],
[@overwrite_file=1];
```

2. Téléchargez le fichier `.deploymentoptions` de votre compartiment S3 dans votre instance de base de données.

```
exec msdb.dbo.rds_download_from_s3
@s3_arn_of_file='arn:aws:s3:::bucket_name/myssasproject.deploymentoptions',
[@rds_file_path='D:\S3\myssasproject.deploymentoptions'],
[@overwrite_file=1];
```

3. Déployez le projet.

```
exec msdb.dbo.rds_msbi_task
@task_type='SSAS_DEPLOY_PROJECT',
@file_path='D:\S3\myssasproject.asdatabase';
```

Surveillance de l'état d'une tâche de déploiement

Pour suivre l'état de votre tâche de déploiement (ou de téléchargement), appelez la fonction `rds_fn_task_status`. Deux paramètres sont nécessaires. Le premier paramètre doit toujours être `NULL`, car il ne s'applique pas à SSAS. Le second paramètre accepte l'ID de tâche.

Pour consulter une liste de toutes les tâches, définissez le premier paramètre sur `NULL` et le second sur `0`, comme illustré dans l'exemple suivant.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,0);
```

Pour obtenir une tâche spécifique, définissez le premier paramètre sur `NULL` et le second sur l'ID de tâche, comme illustré dans l'exemple suivant.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,42);
```

La fonction `rds_fn_task_status` retourne les informations suivantes.

Paramètre de sortie	Description
`task_id`	ID de la tâche
`task_type`	Pour SSAS, les tâches peuvent avoir les types suivants : • `SSAS_DEPLOY_PROJECT` • `SSAS_ADD_DB_ADMIN_MEMBER` • `SSAS_BACKUP_DB` • `SSAS_RESTORE_DB`
`database_name`	Non applicable aux tâches SSAS.

Paramètre de sortie	Description
`% complete`	Progression de la tâche sous forme de pourcentage.
`duration (mins)`	Temps consacré à la tâche, en minutes.
`lifecycle`	État de la tâche. Les statuts possibles sont les suivants : • `CREATED` – Après que vous avez appelé une des procédures stockées SSAS, une tâche est créée et le statut est défini sur `CREATED`. • `IN_PROGRESS` – Après le démarrage d'une tâche, le statut est défini sur `IN_PROGRESS`. Le passage du statut `CREATED` à `IN_PROGRESS` peut prendre jusqu'à cinq minutes. • `SUCCESS` – Lorsqu'une tâche est terminée, le statut est défini sur `SUCCESS`. • `ERROR` – Si une tâche échoue, le statut est défini sur `ERROR`. Lisez la colonne `task_info` pour plus d'informations sur l'erreur. • `CANCEL_REQUESTED` – Après que vous avez appelé `rds_cancel_task`, le statut de la tâche est défini sur `CANCEL_REQUESTED`. • `CANCELLED` – Une fois une tâche annulée avec succès, l'état de la tâche est défini sur `CANCELLED`.
`task_info`	Informations supplémentaires sur la tâche. Si une erreur se produit pendant le traitement, cette colonne contient des informations sur l'erreur.
`last_updated`	Date et heure de la dernière mise à jour de l'état de la tâche.
`created_at`	Date et heure de création de la tâche.
`S3_object_arn`	Non applicable aux tâches SSAS.
`overwrite_S3_backup_file`	Non applicable aux tâches SSAS.
`KMS_master_key_arn`	Non applicable aux tâches SSAS.
`filepath`	Non applicable aux tâches SSAS.
`overwrite_file`	Non applicable aux tâches SSAS.
`task_metadata`	Métadonnées associées à la tâche SSAS.

Utilisation de SSAS sur Amazon RDS

Après le déploiement du projet SSAS, vous pouvez traiter directement la base de données OLAP sur SSMS.

Pour utiliser SSAS sur RDS

1. Dans SSMS, connectez-vous à SSAS en utilisant le nom d'utilisateur et le mot de passe du domaine Active Directory.
2. Développez Bases de données. La nouvelle base de données SSAS déployée s'affiche.
3. Développez Connexions, ouvrez le menu contextuel (clic droit) de l'objet de connexion, puis choisissez Propriétés.
4. Dans la chaîne de connexion, remplacez le nom d'utilisateur et le mot de passe par ceux de la base de données SQL source. Cette opération est nécessaire pour le traitement des tables.
5. Ouvrez le menu contextuel (clic droit) de la base de données SSAS que vous avez créée et choisissez Process Database (Traiter la base données).

   Selon la taille des données d'entrée, le traitement peut prendre plusieurs minutes.

Ajout d'un utilisateur de domaine en tant qu'administrateur de base de données

Vous pouvez ajouter un utilisateur de domaine en tant qu'administrateur de base de données SSAS de la manière suivante :

- Un administrateur de base de données peut utiliser SSMS pour créer un rôle avec des privilèges `admin`, puis ajouter des utilisateurs à ce rôle.
- Vous pouvez utiliser la procédure stockée suivante.

```
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';
```

  Les paramètres suivants sont obligatoires :

  - `@task_type` – Type de la tâche MSBI, en l'occurrence `SSAS_ADD_DB_ADMIN_MEMBER`.
  - `@database_name` – Nom de la base de données SSAS à laquelle vous accordez des privilèges d'administrateur.
  - `@ssas_role_name` – Nom du rôle de l'administrateur de la base de données SSAS. Si le rôle n'existe pas déjà, il est créé.
  - `@ssas_role_member` – Utilisateur de la base de données SSAS que vous ajoutez au rôle d'administrateur.

Sauvegarde d'une base de données SSAS

Vous pouvez créer des fichiers de sauvegarde d'une base de données SSAS uniquement dans le dossier `D:\S3` de l'instance de base de données. Pour déplacer les fichiers de sauvegarde vers votre compartiment S3, utilisez Amazon S3.

Vous pouvez sauvegarder une base de données SSAS comme suit :

- Un utilisateur de domaine ayant le rôle `admin` pour une base de données particulière peut utiliser SSMS pour sauvegarder la base de données en question dans le dossier `D:\S3`.

  Pour plus d'informations, consultez Ajout d'un utilisateur de domaine en tant qu'administrateur de base de données (p. 721).
- Vous pouvez utiliser la procédure stockée suivante.

```
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];
```

Les paramètres suivants sont obligatoires :

- `@task_type` – Type de la tâche MSBI, en l'occurrence `SSAS_BACKUP_DB`.
- `@database_name` – Nom de la base de données SSAS que vous sauvegardez.
- `@file_path` – Chemin d'accès au fichier de sauvegarde de la base de données SSAS. L'extension `.abf` est requise.

Les paramètres suivants sont facultatifs :

- `@ssas_apply_compression` – Pour spécifier s'il faut compresser la sauvegarde SSAS. Les valeurs valides sont 1 (Oui) et 0 (Non).
- `@ssas_overwrite_file` – Pour spécifier s'il faut écraser le fichier de sauvegarde SSAS. Les valeurs valides sont 1 (Oui) et 0 (Non).

  Note

  La procédure stockée pour la sauvegarde ne prend pas en charge le chiffrement.

Restauration d'une base de données SSAS

Utilisez la procédure stockée suivante pour restaurer une base de données SSAS à partir d'une sauvegarde.

```
exec msdb.dbo.rds_msbi_task
@task_type='SSAS_RESTORE_DB',
@database_name='mynewssasdb',
@file_path='D:\S3\ssas_db_backup.abf';
```

Les paramètres suivants sont obligatoires :

- `@task_type` – Type de la tâche MSBI, en l'occurrence `SSAS_RESTORE_DB`.
- `@database_name` – Nom de la nouvelle base de données SSAS que vous restaurez.
- `@file_path` – Chemin d'accès au fichier de sauvegarde SSAS.

  Note

  Vous ne pouvez pas restaurer une base de données si une base de données SSAS existante porte le même nom. La procédure stockée pour la restauration ne prend pas en charge les fichiers de sauvegarde chiffrés.

Restauration d'une instance de base de données à une date spécifiée

La restauration à un instant dans le passé ne s'applique pas aux bases de données SSAS. Si vous effectuez ce type de restauration, seules les données SSAS du dernier instantané avant l'heure demandée sont disponibles sur l'instance restaurée.

Pour accéder aux bases de données SSAS actualisées sur une instance de base de données restaurée

1. Sauvegardez vos bases de données SSAS dans le dossier `D:\S3` de l'instance source.

2. Transférez les fichiers de sauvegarde dans le compartiment S3.
3. Transférez les fichiers de sauvegarde du compartiment S3 vers le dossier `D:\S3` de l'instance restaurée.
4. Exécutez la procédure stockée pour restaurer les bases de données SSAS sur l'instance restaurée.

> **Note**
>
> Vous pouvez également traiter à nouveau le projet SSAS pour restaurer les bases de données.

Désactivation de SSAS

Pour désactiver SSAS, supprimez l'option `SSAS` de son groupe d'options. Avant de supprimer l'option `SSAS`, supprimez vos bases de données SSAS.

> **Important**
>
> Nous vous recommandons vivement de sauvegarder vos bases de données SSAS avant de les supprimer et de supprimer l'option `SSAS`.

Console

Pour supprimer l'option SSAS de son groupe d'options

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Groupes d'options.
3. Choisissez le groupe d'options avec l'option `SSAS` (`ssas-se-2017` dans les exemples précédents).
4. Choisissez Supprimer une option.
5. Sous Deletion options (Options de suppression), choisissez SSAS pour Options to delete (Options à supprimer).
6. Sous Appliquer immédiatement, choisissez Oui pour supprimer l'option immédiatement, ou Non pour la supprimer lors du prochain créneau de maintenance.
7. Sélectionnez Supprimer.

Interface de ligne de commande

Pour supprimer l'option SSAS de son groupe d'options

- Utilisez l'une des commandes suivantes.

  Example

  Pour Linux, macOS ou Unix :

```
aws rds remove-option-from-option-group \
    --option-group-name ssas-se-2017 \
    --options SSAS \
    --apply-immediately
```

  Pour Windows :

```
aws rds remove-option-from-option-group ^
    --option-group-name ssas-se-2017 ^
    --options SSAS ^
```

```
    --apply-immediately
```

Prise en charge de SQL Server Integration Services dans Amazon RDS pour SQL Server

Microsoft SQL Server Integration Services (SSIS) est un composant que vous pouvez utiliser pour effectuer un large éventail de tâches de migration de données. SSIS est une plateforme d'intégration de données et d'applications de flux de travail. Elle dispose d'un outil d'entreposage de données utilisé pour l'extraction, la transformation et le chargement des données (ETL). Vous pouvez également utiliser cet outil pour automatiser la maintenance des bases de données SQL Server et les mises à jour des données cube multidimensionnelles.

Les projets SSIS sont organisés en paquets enregistrés en tant que fichiers .dtsx basés sur XML. Les packages peuvent contenir des flux de contrôle et des flux de données. Vous utilisez des flux de données pour représenter les opérations ETL. Après le déploiement, les packages sont stockés dans SQL Server dans la base de données SSISDB. SSISDB est une base de données de traitement des transactions en ligne (OLTP) en mode de récupération complète.

Amazon RDS for SQL Server prend en charge l'exécution de SSIS directement sur une instance de base de données RDS. Vous pouvez activer SSIS sur une instance de base de données existante ou nouvelle. SSIS est installée sur la même instance de base de données que votre moteur de base de données.

RDS prend en charge SSIS pour SQL Server éditions Standard et Enterprise sur les versions suivantes :

- SQL Server 2017, version 14.00.3223.3.v1 et ultérieure
- SQL Server 2016, version 13.00.5426.0.v1 et ultérieure

Limitations et recommandations

Les limitations et recommandations suivantes s'appliquent à l'exécution de SSIS sur RDS for SQL Server :

- L'instance de base de données doit utiliser AWS Managed Microsoft AD pour l'authentification SSIS.
- L'instance de base de données doit avoir un groupe de paramètres associé avec le paramètre `clr enabled` défini sur 1. Pour de plus amples informations, veuillez consulter Modification du paramètre pour SSIS (p. 728).

  Note

  Si vous activez le paramètre `clr enabled` sur SQL Server 2017, vous ne pouvez pas utiliser le Common Language Runtime (CLR) sur votre instance de base de données.
- Les tâches de flux de contrôle suivantes sont prises en charge :
  - Analysis Services exécute tâche DDL
  - Tâche de traitement Analysis Services
  - Tâche d’insertion en bloc
  - Tâche de vérification de l'intégrité de la base de données
  - Tâche de flux de données
  - Tâche de requête d'exploration de données
  - Tâche de profilage des données
  - Tâche d’exécution de package
  - Exécuter la tâche de travail de SQL Server Agent
  - Exécuter une tâche SQL

  - Exécuter la tâche d'instruction T-SQL
  - Notifier la tâche de l'opérateur
  - Tâche de reconstruction de l'index
  - Tâche de réorganisation de l'index
  - Tâche de réduction de la base de données
  - Tâche de transfert de la base de données
  - Tâche de transfert des tâches
  - Tâche de transfert des connexions
  - Tâche de transfert d'objets SQL Server
  - Tâche de mise à jour des statistiques
- Seul le déploiement de projet est pris en charge.
- L'exécution de packages SSIS à l'aide de SQL Server Agent est prise en charge.
- Seule la journalisation basée sur SQL Server est prise en charge.
- Utilisez uniquement le dossier `D:\S3` pour travailler avec des fichiers. Les fichiers placés dans un autre répertoire sont supprimés. Soyez conscient de quelques autres détails de l'emplacement des fichiers :
  - Placez les fichiers d'entrée et de sortie du projet SSIS dans le dossier `D:\S3`.
  - Pour la tâche de flux de données, modifiez l'emplacement de `BLOBTempStoragePath` et de `BufferTempStoragePath` vers un fichier à l'intérieur du dossier `D:\S3`.
  - Assurez-vous que tous les paramètres, variables et expressions utilisés pour les connexions de fichiers pointent vers le dossier `D:\S3`.
  - Sur les instances multi-AZ, les fichiers créés par SSIS dans le dossier `D:\S3` sont supprimés après un basculement. Pour de plus amples informations, veuillez consulter Limitations Multi-AZ pour l'intégration S3 (p. 698).
  - Téléchargez les fichiers créés par SSIS dans le dossier `D:\S3` dans votre compartiment Amazon S3 pour les rendre durables.
- Les transformations de colonne d'importation et d'exportation, et le composant Script sur la tâche de flux de données ne sont pas prises en charge.
- Vous ne pouvez pas activer le vidage sur l'exécution du package SSIS, et vous ne pouvez pas ajouter des prises de données sur les packages SSIS.
- La fonctionnalité augmentation de la taille des instances SSIS n'est pas prise en charge.
- Vous ne pouvez pas déployer de projets directement. Nous fournissons des procédures stockées RDS pour ce faire. Pour plus d'informations, consultez Déploiement d'un projet SSIS (p. 732).
- Créez des fichiers de projet SSIS (.ispac) avec le mode de protection `DoNotSavePasswords` pour le déploiement sur RDS.
- SSIS n'est pas pris en charge sur les instances Always On avec des réplicas en lecture.
- Vous ne pouvez pas sauvegarder la base de données SSISDB associée à l'option `SSIS`.
- L'importation et la restauration de la base de données SSISDB à partir d'autres instances de SSIS ne sont pas prises en charge.

Activation de SSIS

Vous activez SSIS en ajoutant l'option SSIS à votre instance de base de données. Utilisez la procédure suivante :

1. Créez un groupe d'options ou choisissez un groupe d'options existant.
2. Ajoutez l'option `SSIS` au groupe d'options.
3. Créez un nouveau groupe de paramètres ou choisissez un groupe de paramètres existant.
4. Modifiez le groupe de paramètres de manière à définir le paramètre `clr enabled` sur 1.

5. Associez le groupe d'options et le groupe de paramètres à l'instance de base de données.
6. Activez l'intégration Amazon S3

> **Note**
>
> Si une base de données portant le nom SSISDB ou une connexion SSIS réservée existe déjà sur l'instance de base de données, vous ne pouvez pas activer SSIS sur cette dernière.

Création du groupe d'options pour SSIS

Pour utiliser SSIS, créez un groupe d'options ou modifier un groupe d'options correspondant à l'édition et à la version SQL Server de l'instance de base de données que vous prévoyez d'utiliser. Pour ce faire, utilisez AWS Management Console ou l'AWS CLI.

Console

La procédure suivante crée un groupe d'options pour SQL Server Standard Edition 2016.

Pour créer le groupe d'options

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes d'options.
3. Choisissez Create group.
4. Dans la fenêtre Créer un groupe d'options, procédez comme suit :
   a. Pour Nom, attribuez au groupe d'options un nom unique au sein de votre compte AWS, par exemple **`ssis-se-2016`**. Le nom ne peut contenir que des lettres, des chiffres et des tirets.
   b. Pour Description, saisissez une brève description du groupe d'options, par exemple **`SSIS option group for SQL Server SE 2016`**. La description est utilisée à des fins d'affichage.
   c. Pour Moteur, choisissez sqlserver-se.
   d. Pour Version majeure du moteur, choisissez 13.00.
5. Sélectionnez Créer.

Interface de ligne de commande

La procédure suivante crée un groupe d'options pour SQL Server Standard Edition 2016.

Pour créer le groupe d'options

- Exécutez une des commandes suivantes :

  Example

  Pour Linux, macOS ou 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"
```

  Pour 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"
```

Ajout de l'option SSIS au groupe d'options

Ensuite, utilisez la AWS Management Console ou l'AWS CLI pour ajouter l'option `SSIS` à votre groupe d'options.

Console

Pour ajouter l'option SSIS

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Groupes d'options.
3. Choisissez le groupe d'options que vous venez de créer, ssis-se-2016 dans cet exemple.
4. Sélectionnez Ajouter une option.
5. Sous Détails de l'option, choisissez SSIS pour Nom de l'option.
6. Sous Scheduling (Planification), choisissez si vous souhaitez ajouter l'option immédiatement ou lors du créneau de maintenance suivant.
7. Sélectionnez Ajouter une option.

INTERFACE DE LIGNE DE COMMANDE

Pour ajouter l'option SSIS

- Ajoutez l'option `SSIS` au groupe d'options.

  Example

  Pour Linux, macOS ou Unix :

  ```
  aws rds add-option-to-option-group \
      --option-group-name ssis-se-2016 \
      --options OptionName=SSIS \
      --apply-immediately
  ```

  Pour Windows :

  ```
  aws rds add-option-to-option-group ^
      --option-group-name ssis-se-2016 ^
      --options OptionName=SSIS ^
      --apply-immediately
  ```

Création du groupe de paramètres pour SSIS

Créez ou modifiez un groupe de paramètres pour le paramètre `clr enabled` qui correspond à l'édition et à la version de SQL Server l'instance de base de données que vous prévoyez d'utiliser pour SSIS.

Console

La procédure suivante crée un groupe de paramètres pour SQL Server Standard Edition 2016.

Pour créer le groupe de paramètres

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes de paramètres.
3. Choisissez Créer un groupe de paramètres.
4. Dans le volet Créer un groupe de paramètres, faites ce qui suit :
   a. Pour Famille de groupes de paramètres, choisissez sqlserver-se-13.0.
   b. Pour Nom du groupe, saisissez un identifiant pour le groupe de paramètres, tel que **`ssis-sqlserver-se-13`**.
   c. Pour Description, saisissez **`clr enabled parameter group`**.
5. Sélectionnez Créer.

Interface de ligne de commande

La procédure suivante crée un groupe de paramètres pour SQL Server Standard Edition 2016.

Pour créer le groupe de paramètres

- Exécutez une des commandes suivantes :

  Example

  Pour Linux, macOS ou 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"
```

  Pour 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"
```

Modification du paramètre pour SSIS

Modifiez le paramètre `clr enabled` dans le groupe de paramètres qui correspond à l'édition et à la version SQL Server de votre instance de base de données. Pour SSIS, définissez le paramètre `clr enabled` sur 1.

Console

La procédure suivante modifie le groupe de paramètres que vous avez créé pour SQL Server Standard Edition 2016.

Pour modifier le groupe de paramètres

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes de paramètres.

3. Choisissez le groupe de paramètres, tel que ssis-sqlserver-se-13.
4. Sous Paramètres, filtrez la liste des paramètres pour **clr**.
5. Choisissez clr activé.
6. Choisissez Modifier les paramètres.
7. Dans Valeurs, choisissez 1.
8. Sélectionnez Save Changes.

Interface de ligne de commande

La procédure suivante modifie le groupe de paramètres que vous avez créé pour SQL Server Standard Edition 2016.

Pour modifier le groupe de paramètres

- Exécutez une des commandes suivantes :

  Example

  Pour Linux, macOS ou Unix :

```
aws rds modify-db-parameter-group \
    --db-parameter-group-name ssis-sqlserver-se-13 \
    --parameters "ParameterName='clr enabled',ParameterValue=1,ApplyMethod=immediate"
```

  Pour Windows :

```
aws rds modify-db-parameter-group ^
    --db-parameter-group-name ssis-sqlserver-se-13 ^
    --parameters "ParameterName='clr enabled',ParameterValue=1,ApplyMethod=immediate"
```

Association du groupe d'options et du groupe de paramètres à votre instance de base de données

Pour associer le groupe d'options SSIS et le groupe de paramètres à votre instance de base de données, utilisez la AWS Management Console ou l'AWS CLI

> **Note**
>
> Si vous utilisez une instance existante, un domaine Active Directory et un rôle AWS Identity and Access Management (IAM) doivent déjà lui être associés. Si vous créez une instance, spécifiez un domaine Active Directory et un rôle IAM existants. Pour de plus amples informations, veuillez consulter Utilisation de l'authentification Windows avec une instance de base de données Amazon RDS pour SQL Server (p. 676).

Console

Pour terminer l'activation de SSIS, associez votre groupe d'options et votre groupe de paramètres SSIS à une instance de base de données nouvelle ou existante :

- Pour une nouvelle instance de base de données, associez-les lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).
- Pour une instance de base de données existante, associez-les en modifiant l'instance. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Interface de ligne de commande

Vous pouvez associer le groupe d'options et le groupe de paramètres SSIS à une instance de base de données nouvelle ou existante.

Pour créer une instance avec le groupe d'options SSIS et le groupe de paramètres

- Spécifiez le type de moteur de base de données et la version majeure utilisés lors de la création du groupe d'options.

  Example

  Pour Linux, macOS ou 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
```

  Pour 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
```

Pour modifier une instance et associer le groupe d'options et le groupe de paramètres SSIS

- Exécutez une des commandes suivantes :

  Example

  Pour Linux, macOS ou 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
```

Pour 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
```

Activation de l'intégration S3

Pour télécharger les fichiers du projet SSIS (.ispac) sur votre hôte pour le déploiement, utilisez l'intégration de fichiers S3. Pour plus d'informations, consultez Intégration d'un Amazon RDS pour instance de base de données SQL Server avec Amazon S3 (p. 686).

Autorisations administratives sur SSISDB

Lorsque l'instance est créée ou modifiée avec l'option SSIS, le résultat est une base de données SSISDB avec les rôles ssis_admin et ssis_logreader accordés à l'utilisateur principal. L'utilisateur principal dispose des privilèges suivants dans SSISDB :

- modifier le rôle ssis_admin
- modifier le rôle ssis_logreader
- modifier n'importe quel utilisateur

L'utilisateur principal étant un utilisateur authentifié par SQL, vous ne pouvez pas l'utiliser pour exécuter des packages SSIS. L'utilisateur principal peut utiliser ces privilèges pour créer de nouveaux utilisateurs SSISDB et les ajouter aux rôles ssis_admin et ssis_logreader. Cela peut s'avérer utile pour permettre aux utilisateurs de votre domaine d'utiliser SSIS.

Configuration d'un utilisateur authentifié par Windows pour SSIS

L'utilisateur principal peut utiliser l'exemple de code suivant pour configurer une connexion authentifiée par Windows dans SSISDB et accorder les autorisations de procédure requises. Ainsi, l'utilisateur de domaine peut déployer et exécuter des packages SSIS, utiliser des procédures de transfert de fichiers S3, créer des informations d'identification et travailler avec le proxy d'agent SQL Server. Pour de plus amples informations, consultez Informations d'identification (Moteur de base de données) et Créer un proxy d'agent SQL Server dans la documentation Microsoft.

> **Note**
>
> Vous pouvez accorder quelques-unes ou la totalité des autorisations suivantes, selon les besoins, aux utilisateurs authentifiés par Windows.

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
```

Déploiement d'un projet SSIS

Sur RDS, vous ne pouvez pas déployer de projets SSAS directement avec SQL Server Management Studio (SSMS) ou des procédures SSIS. Pour télécharger des fichiers de projet à partir de Amazon S3, pour les déployer ensuite, utilisez les procédures stockées RDS.

Pour exécuter les procédures stockées, connectez-vous en tant qu'utilisateur auquel vous avez accordé des autorisations d'exécution pour les procédures stockées. Pour plus d'informations, consultez Configuration d'un utilisateur authentifié par Windows pour SSIS (p. 731).

Pour déployer le projet SSIS

1. Téléchargez le fichier du projet (.ispac).

```
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. Soumettez la tâche de déploiement en vérifiant ce qui suit :
   - Le dossier est présent dans le catalogue SSIS.
   - Le nom du projet correspond au nom du projet que vous avez utilisé lors du développement du projet SSIS.

```
exec msdb.dbo.rds_msbi_task
@task_type='SSIS_DEPLOY_PROJECT',
@folder_name='DEMO',
@project_name='ssisproject',
@file_path='D:\S3\ssisproject.ispac;
```

Surveillance de l'état d'une tâche de déploiement

Pour suivre l'état de votre tâche de déploiement, appelez la fonction `rds_fn_task_status`. Deux paramètres sont nécessaires. Le premier paramètre doit toujours être `NULL`, car il ne s'applique pas à SSIS. Le second paramètre accepte l'ID de tâche.

Pour consulter une liste de toutes les tâches, définissez le premier paramètre sur `NULL` et le second sur `0`, comme illustré dans l'exemple suivant.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,0);
```

Pour obtenir une tâche spécifique, définissez le premier paramètre sur `NULL` et le second sur l'ID de tâche, comme illustré dans l'exemple suivant.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,42);
```

La fonction `rds_fn_task_status` retourne les informations suivantes.

Paramètre de sortie	Description
`task_id`	ID de la tâche
`task_type`	`SSIS_DEPLOY_PROJECT`
`database_name`	Non applicable aux tâches SSIS.
`% complete`	Progression de la tâche sous forme de pourcentage.
`duration (mins)`	Temps consacré à la tâche, en minutes.
`lifecycle`	État de la tâche. Les statuts possibles sont les suivants : • `CREATED` – Après avoir appelé la procédure stockée `msdb.dbo.rds_msbi_task`, une tâche est créée et son état est défini sur `CREATED`. • `IN_PROGRESS` – Après le démarrage d'une tâche, le statut est défini sur `IN_PROGRESS`. Le passage du statut `CREATED` à `IN_PROGRESS` peut prendre jusqu'à cinq minutes. • `SUCCESS` – Lorsqu'une tâche est terminée, le statut est défini sur `SUCCESS`. • `ERROR` – Si une tâche échoue, le statut est défini sur `ERROR`. Lisez la colonne `task_info` pour plus d'informations sur l'erreur. • `CANCEL_REQUESTED` – Après que vous avez appelé `rds_cancel_task`, le statut de la tâche est défini sur `CANCEL_REQUESTED`. • `CANCELLED` – Une fois une tâche annulée avec succès, l'état de la tâche est défini sur `CANCELLED`.
`task_info`	Informations supplémentaires sur la tâche. Si une erreur se produit pendant le traitement, cette colonne contient des informations sur l'erreur.

Paramètre de sortie	Description
`last_updated`	Date et heure de la dernière mise à jour de l'état de la tâche.
`created_at`	Date et heure de création de la tâche.
`S3_object_arn`	Non applicable aux tâches SSIS.
`overwrite_S3_backup_file`	Non applicable aux tâches SSIS.
`KMS_master_key_arn`	Non applicable aux tâches SSIS.
`filepath`	Non applicable aux tâches SSIS.
`overwrite_file`	Non applicable aux tâches SSIS.
`task_metadata`	Métadonnées associées à la tâche SSIS.

Utilisation de SSIS

Après avoir déployé le projet SSIS dans le catalogue SSIS, vous pouvez exécuter des packages directement à partir de SSMS ou les planifier à l'aide de SQL Server Agent. Vous devez utiliser une connexion authentifiée par Windows pour exécuter les packages SSIS. Pour plus d'informations, consultez Configuration d'un utilisateur authentifié par Windows pour SSIS (p. 731).

Définition des gestionnaires de connexion à la base de données pour les projets SSIS

Lorsque vous utilisez un gestionnaire de connexions, vous pouvez employer les types d'authentification suivants :

- Pour les connexions de base de données locales, vous pouvez utiliser l'authentification SQL ou l'authentification Windows. Pour l'authentification Windows, utilisez *`DB_instance_name`*`.`*`fully_qualified_domain_name`* comme nom de serveur de la chaîne de connexion.

  `myssisinstance.corp-ad.example.com` en est un exemple, où `myssisinstance` est le nom de l'instance de base de données et `corp-ad.example.com` le nom de domaine entièrement qualifié.
- Pour les connexions distantes, utilisez toujours l'authentification SQL.

Création d'un proxy SSIS

Pour pouvoir planifier des packages SSIS à l'aide de SQL Server Agent, créez des informations d'identification SSIS et un proxy SSIS. Exécutez ces procédures en tant qu'utilisateur authentifié par Windows.

Pour créer les informations d'identification SSIS

- Créez les informations d'identification pour le proxy. Pour ce faire, vous pouvez utiliser SSMS ou l'instruction SQL suivante.

```
USE [master]
GO
CREATE CREDENTIAL [SSIS_Credential] WITH IDENTITY = N'mydomain\user_name', SECRET =
 N'mysecret'
```

```
GO
```

> **Note**
>
> `IDENTITY` doit être une connexion authentifiée par domaine. Remplacez *`mysecret`* par le mot de passe de la connexion authentifiée par le domaine.
> Chaque fois que l'hôte principal SSISDB est modifié, modifiez les informations d'identification du proxy SSIS pour permettre au nouvel hôte d'y accéder.

Pour créer le proxy SSIS

1. Utilisez l'instruction SQL suivante pour créer le proxy.

```
USE [msdb]
GO
EXEC msdb.dbo.sp_add_proxy
 @proxy_name=N'SSIS_Proxy',@credential_name=N'SSIS_Credential',@description=N''
GO
```

2. Utilisez l'instruction SQL suivante pour accorder l'accès au proxy à d'autres utilisateurs.

```
USE [msdb]
GO
EXEC msdb.dbo.sp_grant_login_to_proxy
 @proxy_name=N'SSIS_Proxy',@login_name=N'mydomain\user_name'
GO
```

3. Utilisez l'instruction SQL suivante pour donner au sous-système SSIS accès au proxy.

```
USE [msdb]
GO
EXEC msdb.dbo.rds_sqlagent_proxy
 @task_type='GRANT_SUBSYSTEM_ACCESS',@proxy_name='SSIS_Proxy',@proxy_subsystem='SSIS'
GO
```

Pour afficher le proxy et les octrois sur le proxy

1. Utilisez l'instruction SQL suivante pour afficher les bénéficiaires du proxy.

```
USE [msdb]
GO
EXEC sp_help_proxy
GO
```

2. Utilisez l'instruction SQL suivante pour afficher les octrois du sous-système.

```
USE [msdb]
GO
EXEC msdb.dbo.sp_enum_proxy_for_subsystem
GO
```

Planification d'un package SSIS à l'aide de SQL Server Agent

Après avoir créé les informations d'identification et le proxy et accordé l'accès SSIS au proxy, vous pouvez créer un tâche SQL Server Agent pour planifier le package SSIS.

Pour planifier le package SSIS

- Vous pouvez utiliser SSMS ou T-SQL pour créer la tâche SQL Server Agent. L'exemple suivant utilise 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_jobserver @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
```

Révocation de l'accès SSIS à partir du proxy

Vous pouvez révoquer l'accès au sous-système SSIS et supprimer le proxy SSIS à l'aide des procédures stockées suivantes.

Pour révoquer l'accès et supprimer le proxy

1. Révoquez l'accès au sous-système.

```
USE [msdb]
GO
EXEC msdb.dbo.rds_sqlagent_proxy
 @task_type='REVOKE_SUBSYSTEM_ACCESS',@proxy_name='SSIS_Proxy',@proxy_subsystem='SSIS'
GO
```

2. Révoquez les octrois sur le proxy.

```
USE [msdb]
GO
EXEC msdb.dbo.sp_revoke_login_from_proxy
 @proxy_name=N'SSIS_Proxy',@name=N'mydomain\user_name'
GO
```

3. Supprimez le proxy.

```
USE [msdb]
GO
EXEC dbo.sp_delete_proxy @proxy_name = N'SSIS_Proxy'
GO
```

Désactivation de SSIS

Pour désactiver SSIS, supprimez l'option `SSIS` de son groupe d'options.

> **Important**
>
> La suppression de l'option ne supprime pas la base de données SSISDB, vous pouvez donc supprimer l'option en toute sécurité sans perdre les projets SSIS.
> Vous pouvez réactiver l'option `SSIS` après la suppression pour réutiliser les projets SSIS précédemment déployés dans le catalogue SSIS.

Console

La procédure suivante supprime l'option `SSIS`.

Pour supprimer l'option SSIS de son groupe d'options

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Groupes d'options.
3. Choisissez le groupe d'options avec l'option `SSIS` (`ssis-se-2016` dans les exemples précédents).
4. Choisissez Supprimer une option.
5. Sous Options de suppression, choisissez SSIS pour Options à supprimer.
6. Sous Appliquer immédiatement, choisissez Oui pour supprimer l'option immédiatement, ou Non pour la supprimer lors du prochain créneau de maintenance.
7. Sélectionnez Supprimer.

Interface de ligne de commande

La procédure suivante supprime l'option `SSIS`.

Pour supprimer l'option SSIS de son groupe d'options

- Exécutez une des commandes suivantes :

  Example

  Pour Linux, macOS ou Unix :

```
aws rds remove-option-from-option-group \
    --option-group-name ssis-se-2016 \
    --options SSIS \
    --apply-immediately
```

  Pour Windows :

```
aws rds remove-option-from-option-group ^
```

```
    --option-group-name ssis-se-2016 ^
    --options SSIS ^
    --apply-immediately
```

Suppression de la base de données SSISDB

Après avoir supprimé l'option SSIS, la base de données SSISDB n'est pas supprimée. Pour supprimer la base de données SSISDB, utilisez la procédure stockée `rds_drop_ssis_database` après avoir supprimé l'option SSIS.

Pour supprimer la base de données SSIS

- Utilisez la procédure stockée suivante.

```
USE [msdb]
GO
EXEC dbo.rds_drop_ssis_database
GO
```

Après avoir supprimé la base de données SSISDB, si vous réactivez l'option SSIS, vous obtenez un nouveau catalogue SSISDB.

Prise en charge de SQL Server Reporting Services dans Amazon RDS pour SQL Server

Microsoft SQL Server Reporting Services (SSRS) est une application basée sur un serveur utilisée pour la génération et la distribution de rapports. Elle fait partie d'une suite de services SQL Server qui inclut également SQL Server Analysis Services (SSAS) et SQL Server Integration Services (SSIS). SSRS est un service qui repose sur SQL Server. Vous pouvez l'utiliser pour collecter des données provenant de diverses sources de données et les présenter de sorte qu'elles soient facilement compréhensibles et prêtes à être analysées.

Amazon RDS for SQL Server prend en charge l'exécution de SSRS directement sur les instances de base de données RDS. Vous pouvez activer SSRS pour des instances de base de données existantes ou nouvelles.

RDS prend en charge SSRS pour SQL Server éditions Standard et Enterprise sur les versions suivantes :

- SQL Server 2017, version 14.00.3223.3.v1 et ultérieure
- SQL Server 2016, version 13.00.5820.21.v1 et ultérieure

Limitations et recommandations

Les limitations et recommandations suivantes s'appliquent à l'exécution de SSRS sur RDS for SQL Server :

- Les instances doivent utiliser AWS Managed Microsoft AD pour l'authentification auprès d'un portail Web SSRS et d'un serveur Web.
- L'importation et la restauration de bases de données de serveur de rapports à partir d'autres instances de SSRS ne sont pas prises en charge.

  Assurez-vous d'utiliser les bases de données créées lorsque l'option `SSRS` est ajoutée à l'instance de base de données RDS. Pour de plus amples informations, veuillez consulter Bases de données de serveur de rapports (p. 743).

- Vous ne pouvez pas configurer SSRS pour l'écoute sur le port SSL par défaut (443). Les valeurs autorisées sont comprises entre 1150 et 49511, sauf 1234, 1434, 3260, 3343, 3389 et 47001.
- Les abonnements par e-mail ou par partage de fichier Microsoft Windows ne sont pas pris en charge.
- L'utilisation du Gestionnaire de configurations Reporting Services n'est pas prise en charge.
- La création et la modification de rôles n'est pas prise en charge.
- La modification des propriétés du serveur de rapports n'est pas prise en charge.
- Les rôles d'administrateur système et d'utilisateur système ne sont pas accordés.
- Vous ne pouvez pas modifier les affectations de rôle de niveau système via le portail Web.

Activation de SSRS

Utilisez la procédure suivante pour activer SSRS sur votre instance de base de données :

1. Créez un groupe d'options ou choisissez un groupe d'options existant.
2. Ajoutez l'option `SSRS` au groupe d'options.
3. Associez le groupe d'options à l'instance de base de données.
4. Autorisez l'accès entrant au groupe de sécurité VPC (Virtual Private Cloud) pour le port d'écoute SSRS.

Création d'un groupe d'options pour SSRS

Pour utiliser SSRS, créez un groupe d'options correspondant au moteur et à la version SQL Server de l'instance de base de données que vous prévoyez d'utiliser. Pour ce faire, utilisez AWS Management Console ou l'AWS CLI.

> **Note**
>
> Vous pouvez également utiliser un groupe d'options existant s'il convient au moteur et à la version SQL Server.

Console

La procédure suivante crée un groupe d'options pour SQL Server Standard Edition 2017.

Pour créer le groupe d'options

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes d'options.
3. Choisissez Créer un groupe.
4. Dans la fenêtre Créer un groupe d'options, procédez comme suit :
   a. Pour Nom, attribuez au groupe d'options un nom unique au sein de votre compte AWS, par exemple **`ssrs-se-2017`**. Le nom ne peut contenir que des lettres, des chiffres et des tirets.
   b. Pour Description, saisissez une brève description du groupe d'options, par exemple **`SSRS option group for SQL Server SE 2017`**. La description est utilisée à des fins d'affichage.
   c. Pour Moteur, choisissez sqlserver-se.
   d. Pour Version majeure du moteur, choisissez 14.00.
5. Sélectionnez Créer.

Interface de ligne de commande

La procédure suivante crée un groupe d'options pour SQL Server Standard Edition 2017.

Pour créer le groupe d'options

- Exécutez une des commandes suivantes :

Example

Pour Linux, macOS ou 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"
```

Pour 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"
```

Ajout de l'option SSRS à votre groupe d'options

Ensuite, utilisez AWS Management Console ou l'AWS CLI pour ajouter l'option `SSRS` à votre groupe d'options.

Console

Pour ajouter l'option SSRS

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Groupes d'options.
3. Choisissez le groupe d'options que vous venez de créer.
4. Sélectionnez Ajouter une option.
5. Sous Option details (Détails de l'option), choisissez SSRS pour Option name (Nom de l'option).
6. Sous Option settings (Paramètres d'option), procédez comme suit :
   a. Entrez le port que le service SSRS utilisera pour l'écoute. La valeur par défaut est 8443. Pour obtenir la liste des valeurs autorisées, veuillez consulter Limitations et recommandations (p. 738).
   b. Entrez une valeur pour Max memory (Volume de mémoire maximal).

      Lamémoire maximale spécifie le seuil supérieur au-dessus duquel aucune nouvelle demande d'allocation de mémoire n'est accordée aux applications serveur de rapports. Le nombre correspond à un pourcentage de la mémoire totale de l'instance de base de données. Les valeurs autorisées sont comprises entre 10 et 80.
7. Pour Groupes de sécurité, choisissez le groupe de sécurité VPC à associer à l'option. Utilisez le même groupe de sécurité que celui associé à votre instance de base de données.
8. Sous Scheduling (Planification), choisissez si vous souhaitez ajouter l'option immédiatement ou lors du créneau de maintenance suivant.
9. Sélectionnez Ajouter une option.

INTERFACE DE LIGNE DE COMMANDE

Pour ajouter l'option SSRS

1. Créez un fichier JSON, par exemple `ssrs-option.json`, avec les paramètres suivants :
   - `OptionGroupName` – Nom du groupe d'options que vous avez créé ou choisi précédemment (`ssrs-se-2017` dans l'exemple suivant).
   - `Port` – Port que le service SSRS utilisera pour l'écoute. La valeur par défaut est 8443. Pour obtenir la liste des valeurs autorisées, veuillez consulter Limitations et recommandations (p. 738).
   - `VpcSecurityGroupMemberships` – Appartenances au groupe de sécurité VPC pour votre instance de base de données RDS.
   - `MAX_MEMORY` – Seuil supérieur au-dessus duquel aucune nouvelle demande d'attribution de mémoire n'est accordée aux applications de serveur de rapports. Le nombre correspond à un pourcentage de la mémoire totale de l'instance de base de données. Les valeurs autorisées sont comprises entre 10 et 80.

```
{
"OptionGroupName": "ssrs-se-2017",
"OptionsToInclude": [
 {
 "OptionName": "SSRS",
 "Port": 8443,
 "VpcSecurityGroupMemberships": ["sg-0abcdef123"],
 "OptionSettings": [{"Name": "MAX_MEMORY","Value": "60"}]
 }],
"ApplyImmediately": true
}
```

2. Ajoutez l'option `SSRS` au groupe d'options.

   Example

   Pour Linux, macOS ou Unix :

```
aws rds add-option-to-option-group \
    --cli-input-json file://ssrs-option.json \
    --apply-immediately
```

   Pour Windows :

```
aws rds add-option-to-option-group ^
    --cli-input-json file://ssrs-option.json ^
    --apply-immediately
```

Association de votre groupe d'options à votre instance de base de données

Vous pouvez utiliser AWS Management Console ou l'AWS CLI pour associer votre groupe d'options à votre instance de base de données.

Si vous utilisez une instance de base de données existante, un domaine Active Directory et un rôle AWS Identity and Access Management (IAM) doivent déjà lui être associés. Si vous créez une instance, spécifiez un domaine Active Directory et un rôle IAM existants. Pour de plus amples informations, veuillez consulter Utilisation de l'authentification Windows avec une instance de base de données Amazon RDS pour SQL Server (p. 676).

Console

Vous pouvez associer votre groupe d'options à une instance de base de données nouvelle ou existante.

- Pour une nouvelle instance de base de données, associez le groupe d'options lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).
- Pour une instance de base de données existante, modifiez l'instance et associez le nouveau groupe d'options. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Interface de ligne de commande

Vous pouvez associer votre groupe d'options à une instance de base de données nouvelle ou existante.

Pour créer une instance de base de données utilisant votre groupe d'options

- Spécifiez le type de moteur de base de données et la version majeure utilisés lors de la création du groupe d'options.

  Example

  Pour Linux, macOS ou 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
```

  Pour 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
```

Pour modifier une instance de base de données pour utiliser votre groupe d'options

- Exécutez une des commandes suivantes :

Example

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier myssrsinstance \
    --option-group-name ssrs-se-2017 \
    --apply-immediately
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier myssrsinstance ^
    --option-group-name ssrs-se-2017 ^
    --apply-immediately
```

Autorisation de l'accès entrant à votre groupe de sécurité VPC

Pour autoriser l'accès entrant au groupe de sécurité VPC associé à votre instance de base de données, créez une règle entrante pour le port d'écoute SSRS spécifié. Pour de plus amples informations sur la configuration des groupes de sécurité, veuillez consulter Créer un groupe de sécurité qui autorise l'accès à votre instance de base de données dans votre VPC (p. 66).

Bases de données de serveur de rapports

Lorsque votre instance de base de données est associée à l'option SSRS, deux nouvelles bases de données sont créées sur votre instance de base de données : rdsadmin_ReportServer et rdsadmin_ReportServerTempDB. Ces bases de données agissent comme les bases de données ReportServer et ReportServerTempDB. SSRS stocke ses données dans la base de données ReportServer et les met en cache dans la base de données ReportServerTempDB. RDS possède et gère ces bases de données. Elles ne peuvent donc pas faire l’objet d’opérations de base de données telles que ALTER et DROP.

Accès au portail Web SSRS

Utilisez la procédure suivante pour accéder au portail Web SSRS :

1. Activez le protocole SSL (Secure Sockets Layer).
2. Accorder l'accès aux utilisateurs du domaine.
3. Accédez au portail Web à l'aide d'un navigateur et des informations d'identification d'un utilisateur du domaine.

Activation de SSL sur RDS

SSRS utilise le protocole SSL HTTPS pour ses connexions. Pour utiliser ce protocole, importez un certificat SSL dans le système d'exploitation Microsoft Windows sur votre ordinateur client.

Pour de plus amples informations sur les certificats SSL, veuillez consulter Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525). Pour de plus amples informations sur l'utilisation de SSL avec SQL Server, veuillez consulter Utilisation de SSL avec une instance DB Microsoft SQL Server (p. 669).

Octroi de l'accès aux utilisateurs du domaine

Dans une nouvelle activation SSRS, il n'y a pas d'attribution de rôle dans SSRS. Pour donner à un utilisateur ou à un groupe d'utilisateurs du domaine l'accès au portail Web, RDS fournit une procédure stockée.

Pour accorder l'accès à un utilisateur du domaine sur le portail Web

- Utilisez la procédure stockée suivante.

```
exec msdb.dbo.rds_msbi_task
@task_type='SSRS_GRANT_PORTAL_PERMISSION',
@ssrs_group_or_username=N'AD_domain\user';
```

Le rôle système `RDS_SSRS_ROLE` est accordé à l'utilisateur ou au groupe d'utilisateurs du domaine. Les tâches de niveau système suivantes sont accordées à ce rôle :

- Exécuter des définitions de rapport
- Gérer des tâches
- Gérer des calendriers partagés
- Afficher des calendriers partagés

Le rôle de niveau élément `Content Manager` sur le dossier racine est également accordé.

Accès au portail Web

Lorsque la tâche `SSRS_GRANT_PORTAL_PERMISSION` est terminée, vous avez accès au portail à l'aide d'un navigateur Web. L'URL du portail Web a le format suivant.

```
https://rds_endpoint:port/Reports
```

Dans ce format, les points suivants s'appliquent :

- *`rds_endpoint`* – Point de terminaison de l'instance de base de données RDS que vous utilisez avec SSRS.

  Vous trouverez le point de terminaison dans l'onglet Connectivité et sécurité de votre instance de base de données. Pour de plus amples informations, veuillez consulter Connexion à une instance de base de données exécutant le moteur de base de données Microsoft SQL Server (p. 618).
- *`port`* – Port d'écoute pour SSRS que vous définissez dans l'option `SSRS`.

Pour accéder au portail Web

1. Entrez l'URL du portail Web dans votre navigateur.

   ```
   https://myssrsinstance.cg034itsfake.us-east-1.rds.amazonaws.com:8443/Reports
   ```

2. Connectez-vous avec les informations d'identification d'un utilisateur du domaine auquel vous avez accordé l'accès avec la tâche `SSRS_GRANT_PORTAL_PERMISSION`.

Déploiement de rapports sur SSRS

Une fois que vous avez accès au portail web, vous pouvez y déployer des rapports. Vous pouvez utiliser l'outil de chargement dans le portail web pour charger des rapports, ou effectuer le déploiement directement à partir de SQL Server Data Tools (SSDT). Lors du déploiement à partir de SSDT, assurez-vous de ce qui suit :

- L'utilisateur qui a lancé SSDT a accès au portail web SSRS.
- La valeur `TargetServerURL` des propriétés du projet SSRS est définie sur le point de terminaison HTTPS de l'instance de base de données RDS dotée du suffixe `ReportServer`, par exemple :

```
https://myssrsinstance.cg034itsfake.us-east-1.rds.amazonaws.com:8443/ReportServer
```

Révocation des autorisations de niveau système

Le rôle système `RDS_SSRS_ROLE` ne dispose pas des autorisations suffisantes pour supprimer les affectations de rôle de niveau système. Pour supprimer un utilisateur ou un groupe d'utilisateurs de `RDS_SSRS_ROLE`, utilisez la même procédure stockée que celle utilisée pour accorder le rôle, mais faites appel au type de tâche `SSRS_REVOKE_PORTAL_PERMISSION`.

Pour révoquer l'accès d'un utilisateur du domaine pour le portail Web

- Utilisez la procédure stockée suivante.

```
exec msdb.dbo.rds_msbi_task
@task_type='SSRS_REVOKE_PORTAL_PERMISSION',
@ssrs_group_or_username=N'AD_domain\user';
```

Cette procédure supprime l'utilisateur du rôle système `RDS_SSRS_ROLE`. Il supprime également l'utilisateur du rôle de niveau élément `Content Manager`, si cet utilisateur en dispose.

Surveillance du statut d’une tâche

Pour suivre le statut de votre tâche d'octroi ou de révocation, appelez la fonction `rds_fn_task_status`. Deux paramètres sont nécessaires. Le premier paramètre doit toujours être `NULL`, car il ne s'applique pas à SSRS. Le second paramètre accepte l'ID de tâche.

Pour consulter une liste de toutes les tâches, définissez le premier paramètre sur `NULL` et le second sur `0`, comme illustré dans l'exemple suivant.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,0);
```

Pour obtenir une tâche spécifique, définissez le premier paramètre sur `NULL` et le second sur l'ID de tâche, comme illustré dans l'exemple suivant.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,42);
```

La fonction `rds_fn_task_status` retourne les informations suivantes.

Paramètre de sortie	Description
`task_id`	ID de la tâche

Paramètre de sortie	Description
`task_type`	Pour SSRS, les tâches peuvent avoir les types suivants : • `SSRS_GRANT_PORTAL_PERMISSION` • `SSRS_REVOKE_PORTAL_PERMISSION`
`database_name`	Non applicable aux tâches SSRS.
`% complete`	Progression de la tâche sous forme de pourcentage.
`duration (mins)`	Temps consacré à la tâche, en minutes.
`lifecycle`	État de la tâche. Les statuts possibles sont les suivants : • `CREATED` – Après que vous avez appelé une des procédures SSRS stockées, une tâche est créée et le statut est défini sur `CREATED`. • `IN_PROGRESS` – Après le démarrage d'une tâche, le statut est défini sur `IN_PROGRESS`. Le passage du statut `CREATED` à `IN_PROGRESS` peut prendre jusqu'à cinq minutes. • `SUCCESS` – Lorsqu'une tâche est terminée, le statut est défini sur `SUCCESS`. • `ERROR` – Si une tâche échoue, le statut est défini sur `ERROR`. Lisez la colonne `task_info` pour plus d'informations sur l'erreur. • `CANCEL_REQUESTED` – Après que vous avez appelé la procédure stockée `rds_cancel_task`, le statut de la tâche est défini sur `CANCEL_REQUESTED`. • `CANCELLED` – Une fois une tâche annulée avec succès, l'état de la tâche est défini sur `CANCELLED`.
`task_info`	Informations supplémentaires sur la tâche. Si une erreur se produit pendant le traitement, cette colonne contient des informations sur l'erreur.
`last_updated`	Date et heure de la dernière mise à jour de l'état de la tâche.
`created_at`	Date et heure de création de la tâche.
`S3_object_arn`	Non applicable aux tâches SSRS.
`overwrite_S3_backup_file`	Non applicable aux tâches SSRS.
`KMS_master_key_arn`	Non applicable aux tâches SSRS.
`filepath`	Non applicable aux tâches SSRS.
`overwrite_file`	Non applicable aux tâches SSRS.
`task_metadata`	Métadonnées associées à la tâche SSRS.

Désactivation de SSRS

Pour désactiver SSRS, supprimez l'option `SSRS` de son groupe d'options. La suppression de l'option ne supprime pas les bases de données SSRS. Pour de plus amples informations, veuillez consulter Suppression des bases de données SSRS (p. 747).

Vous pouvez réactiver SSRS en ajoutant l'option `SSRS`. Si vous avez également supprimé les bases de données SSRS, la réactivation de SSRS sur la même instance de base de données crée de nouvelles bases de données de serveur de rapports.

Console

Pour supprimer l'option SSRS de son groupe d'options

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Groupes d'options.
3. Choisissez le groupe d'options avec l'option `SSRS` (`ssrs-se-2017` dans les exemples précédents).
4. Choisissez Supprimer une option.
5. Sous Options de suppression, choisissez SSRS pour Options à supprimer.
6. Sous Appliquer immédiatement, choisissez Oui pour supprimer l'option immédiatement, ou Non pour la supprimer lors du prochain créneau de maintenance.
7. Sélectionnez Supprimer.

Interface de ligne de commande

Pour supprimer l'option SSRS de son groupe d'options

- Exécutez une des commandes suivantes :

  Example

  Pour Linux, macOS ou Unix :

```
aws rds remove-option-from-option-group \
    --option-group-name ssrs-se-2017 \
    --options SSRS \
    --apply-immediately
```

  Pour Windows :

```
aws rds remove-option-from-option-group ^
    --option-group-name ssrs-se-2017 ^
    --options SSRS ^
    --apply-immediately
```

Suppression des bases de données SSRS

La suppression de l'option `SSRS` ne supprime pas les bases de données du serveur de rapports. Pour les supprimer, utilisez la procédure stockée suivante.

Pour supprimer les bases de données du serveur de rapports, assurez-vous d'abord de supprimer l'option `SSRS`.

Pour supprimer les bases de données SSRS

- Utilisez la procédure stockée suivante.

```
exec msdb.dbo.rds_drop_ssrs_databases
```

Prise en charge de Microsoft Distributed Transaction Coordinator dans SQL Server

Une transaction distribuée est une transaction de base de données dans laquelle deux hôtes réseau ou plus sont impliqués. Amazon RDS for SQL Server prend en charge les transactions distribuées entre des hôtes, où un hôte peut être un des éléments suivants :

- Instance de base de données RDS for SQL Server
- Hôte SQL Server sur site
- Hôte Amazon EC2 avec SQL Server installé
- Tout autre hôte EC2 ou instance de base de données RDS avec un moteur de base de données prenant en charge les transactions distribuées

Dans RDS, à partir de SQL Server 2012 (versions 11.00.5058.0.v1 et ultérieures), toutes les éditions de SQL Server prennent en charge les transactions distribuées. La prise en charge est fournie via Microsoft Distributed Transaction Coordinator (MSDTC). Pour de plus amples informations sur MSDTC, veuillez consulter Distributed Transaction Coordinator dans la documentation Microsoft.

Limites

Les limitations suivantes s'appliquent à l'utilisation de MSDTC sur RDS for SQL Server :

- MSDTC n'est pas pris en charge sur les instances utilisant la mise en miroir de base de données SQL Server. Pour de plus amples informations, veuillez consulter Transactions - availability groups and database mirroring.
- Le paramètre `in-doubt xact resolution` doit être défini sur 1 ou 2. Pour de plus amples informations, veuillez consulter Modification du paramètre pour MSDTC (p. 752).
- MSDTC exige que tous les noms d'hôtes participant à des transactions distribuées puissent être résolus à l'aide de leurs noms d'ordinateur. RDS gère automatiquement cette fonctionnalité pour les instances jointes au domaine. Toutefois, pour les instances autonomes, assurez-vous de configurer manuellement le serveur DNS.
- Les transactions distribuées qui dépendent de bibliothèques de liens dynamiques clientes (DLL) sur des instances RDS ne sont pas prises en charge.

Activation de MSDTC

Utilisez la procédure suivante pour activer MSDTC pour votre instance de base de données :

1. Créez un groupe d'options ou choisissez un groupe d'options existant.
2. Ajoutez l'option `MSDTC` au groupe d'options.
3. Créez un nouveau groupe de paramètres ou choisissez un groupe de paramètres existant.
4. Modifiez le groupe de paramètres de manière à définir le paramètre `in-doubt xact resolution` sur 1 ou 2.

5. Associez le groupe d'options et le groupe de paramètres à l'instance de base de données.

Création du groupe d'options pour MSDTC

Utilisez AWS Management Console ou l'AWS CLI pour créer un groupe d'options correspondant au moteur SQL Server et à la version de votre instance de base de données.

> **Note**
>
> Vous pouvez également utiliser un groupe d'options existant s'il convient au moteur et à la version SQL Server.

Console

La procédure suivante crée un groupe d'options pour SQL Server Standard Edition 2016.

Pour créer le groupe d'options

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes d'options.
3. Choisissez Créer un groupe.
4. Dans la fenêtre Créer un groupe d'options, procédez comme suit :
   a. Pour Nom, attribuez au groupe d'options un nom unique au sein de votre compte AWS, par exemple **msdtc-se-2016**. Le nom ne peut contenir que des lettres, des chiffres et des tirets.
   b. Pour Description, saisissez une brève description du groupe d'options, par exemple **MSDTC option group for SQL Server SE 2016**. La description est utilisée à des fins d'affichage.
   c. Pour Moteur, choisissez sqlserver-se.
   d. Pour Version majeure du moteur, choisissez 13.00.
5. Sélectionnez Créer.

Interface de ligne de commande

L'exemple suivant crée un groupe d'options pour SQL Server Standard Edition 2016.

Pour créer le groupe d'options

- Utilisez l'une des commandes suivantes.

  Example

  Pour Linux, macOS ou 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"
```

  Pour 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"
```

Ajout de l'option MSDTC au groupe d'options

Ensuite, utilisez AWS Management Console ou l'AWS CLI pour ajouter l'option `MSDTC` au groupe d'options.

Les paramètres d'option suivants sont requis :

- Port – Port que vous utilisez pour accéder à MSDTC. Les valeurs autorisées sont comprises entre 1150 et 49151, sauf 1234, 1434, 3260, 3343, 3389 et 47001. La valeur par défaut est 5000.

  Assurez-vous que le port que vous souhaitez utiliser est activé dans vos règles de pare-feu. Assurez-vous également que ce port est activé dans les règles entrantes et sortantes pour le groupe de sécurité associé à votre instance de base de données. Pour plus d'informations, consultez Impossible de se connecter à l'instance de base de données Amazon RDS (p. 1639).
- Groupes de sécurité – Appartenances au groupe de sécurité de base de données ou VPC pour votre instance de base de données RDS.
- Type d'authentification – Mode d'authentification entre les hôtes. Les types d'authentification suivants sont pris en charge :
  - Mutuelle – Les instances RDS sont mutuellement authentifiées à l'aide d'une authentification intégrée. Si cette option est sélectionnée, toutes les instances associées à ce groupe d'options doivent être jointes au domaine.
  - Aucun(e) – Aucune authentification n'est effectuée entre les hôtes. Nous ne recommandons pas d'utiliser ce mode dans les environnements de production.
- Taille du journal des transactions – Taille du journal des transactions MSDTC. Les valeurs autorisées sont comprises entre 4 et 1 024 Mo. La taille par défaut est 4 Mo.

Les paramètres d'option suivants sont facultatifs :

- Activer les connexions entrantes – Indique si vous souhaitez autoriser les connexions MSDTC entrantes aux instances associées à ce groupe d'options.
- Activer les connexions sortantes – Indique si vous souhaitez autoriser les connexions MSDTC sortantes à partir des instances associées à ce groupe d'options.
- Activer XA – Indique si vous souhaitez autoriser les transactions XA. Pour de plus amples informations sur le protocole XA, veuillez consulter XA Specification.

  > **Note**
  >
  > L'utilisation de bibliothèques à liens dynamiques XA personnalisées n'est pas prise en charge.
- Activer SNA LU – Indique si le protocole SNA LU doit être utilisé pour les transactions distribuées. Pour de plus amples informations sur la prise en charge du protocole SNA LU, veuillez consulter Managing IBM CICS LU 6.2 Transactions dans la documentation Microsoft.

Console

Pour ajouter l'option MSDTC

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Groupes d'options.
3. Choisissez le groupe d'options que vous venez de créer.
4. Sélectionnez Ajouter une option.

5. Sous Détails de l'option, choisissez MSDTC pour Nom de l'option.
6. Sous Paramètres des options :
   a. Pour Port, entrez le numéro de port pour accéder à MSDTC. La valeur par défaut est 5000.
   b. Pour Groupes de sécurité, choisissez le groupe de sécurité de base de données ou de VPC à associer à l'option.
   c. Pour Type d'authentification, choisissez Mutuelle ou Aucun(e).
   d. Pour Taille du journal des transactions, entrez une valeur comprise entre 4 et 1 024. La valeur par défaut est 4.
7. Sous Configuration supplémentaire, procédez comme suit :
   a. Pour Connexions, choisissez, selon vos besoins, Activer les connexions entrantes et Activer les connexions sortantes.
   b. Pour Protocoles autorisés, choisissez, selon vos besoins, Activer XA et Activer SNA LU.
8. Sous Scheduling (Planification), choisissez si vous souhaitez ajouter l'option immédiatement ou lors du créneau de maintenance suivant.
9. Sélectionnez Ajouter une option.

   Pour ajouter cette option, aucun redémarrage n'est requis.

INTERFACE DE LIGNE DE COMMANDE

Pour ajouter l'option MSDTC

1. Créez un fichier JSON, par exemple `msdtc-option.json`, avec les paramètres requis suivants :

```
{
"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. Ajoutez l'option `MSDTC` au groupe d'options.

   #### Example

   Pour Linux, macOS ou Unix :

```
aws rds add-option-to-option-group \
    --cli-input-json file://msdtc-option.json \
    --apply-immediately
```

   Pour Windows :

```
aws rds add-option-to-option-group ^
    --cli-input-json file://msdtc-option.json ^
    --apply-immediately
```

   Aucun redémarrage n'est requis.

Création du groupe de paramètres pour MSDTC

Créez ou modifiez un groupe de paramètres pour le paramètre `in-doubt xact resolution` qui correspond à l'édition et à la version de SQL Server de votre instance de base de données.

Console

L'exemple suivant crée un groupe de paramètres pour SQL Server Standard Edition 2016.

Pour créer le groupe de paramètres

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes de paramètres.
3. Choisissez Créer un groupe de paramètres.
4. Dans le volet Créer un groupe de paramètres, faites ce qui suit :
   a. Pour Famille de groupes de paramètres, choisissez sqlserver-se-13.0.
   b. Pour Nom du groupe, entrez un identifiant pour le groupe de paramètres, tel que **`msdtc-sqlserver-se-13`**.
   c. Pour Description, entrez **`in-doubt xact resolution`**.
5. Sélectionnez Créer.

Interface de ligne de commande

L'exemple suivant crée un groupe de paramètres pour SQL Server Standard Edition 2016.

Pour créer le groupe de paramètres

- Utilisez l'une des commandes suivantes.

  Example

  Pour Linux, macOS ou 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"
```

  Pour 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"
```

Modification du paramètre pour MSDTC

Modifiez le paramètre `in-doubt xact resolution` dans le groupe de paramètres qui correspond à l'édition et à la version SQL Server de votre instance de base de données.

Pour MSDTC, définissez le paramètre `in-doubt xact resolution` sur l'une des options suivantes :

- `1 – Presume commit`. Toute transaction MSDTC incertaine est présumée avoir été validée.

- `2 – Presume abort`. Toute transaction MSDTC incertaine est présumée avoir été arrêtée.

Pour de plus amples informations, veuillez consulter in-doubt xact resolution Server Configuration Option dans la documentation Microsoft.

Console

L'exemple suivant modifie le groupe de paramètres que vous avez créé pour SQL Server Standard Edition 2016.

Pour modifier le groupe de paramètres

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Groupes de paramètres.
3. Choisissez le groupe de paramètres, tel que msdtc-sqlserver-se-13.
4. Sous Paramètres, filtrez la liste des paramètres pour **`xact`**.
5. Choisissez in-doubt xact resolution.
6. Choisissez Modifier les paramètres.
7. Entrez **`1`** ou **`2`**.
8. Sélectionnez Save Changes.

Interface de ligne de commande

L'exemple suivant modifie le groupe de paramètres que vous avez créé pour SQL Server Standard Edition 2016.

Pour modifier le groupe de paramètres

- Utilisez l'une des commandes suivantes.

  Example

  Pour Linux, macOS ou 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"
```

  Pour 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"
```

Association du groupe d'options et du groupe de paramètres à l'instance de base de données

Vous pouvez utiliser AWS Management Console ou l’AWS CLI pour associer le groupe d'options et le groupe de paramètres MSDTC à l'instance de base de données.

Console

Vous pouvez associer le groupe d'options et le groupe de paramètres MSDTC à une instance de base de données nouvelle ou existante.

- Pour une nouvelle instance de base de données, associez-les lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).
- Pour une instance de base de données existante, associez-les en modifiant l'instance. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

  Note

  Si vous utilisez une instance de base de données existante jointe au domaine, un domaine Active Directory et un rôle AWS Identity and Access Management (IAM) doivent déjà lui être associés. Si vous créez une nouvelle instance jointe au domaine, spécifiez un domaine Active Directory et un rôle IAM existants. Pour de plus amples informations, veuillez consulter Utilisation de l'authentification Windows avec une instance de base de données Amazon RDS pour SQL Server (p. 676).

Interface de ligne de commande

Vous pouvez associer le groupe d'options et le groupe de paramètres MSDTC à une instance de base de données nouvelle ou existante.

Note

Si vous utilisez une instance de base de données jointe au domaine existante, un domaine Active Directory et un rôle IAM doivent déjà lui être associés. Si vous créez une nouvelle instance jointe au domaine, spécifiez un domaine Active Directory et un rôle IAM existants. Pour plus d'informations, consultez Utilisation de l'authentification Windows avec une instance de base de données Amazon RDS pour SQL Server (p. 676).

Pour créer une instance DB avec le groupe d'options et le groupe de paramètres MSDTC

- Spécifiez le type de moteur de base de données et la version majeure utilisés lors de la création du groupe d'options.

  Example

  Pour Linux, macOS ou 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
```

  Pour 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
```

Pour modifier une instance de base de données et associer le groupe d'options et le groupe de paramètres MSDTC

- Utilisez l'une des commandes suivantes.

  Example

  Pour Linux, macOS ou 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
```

  Pour 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
```

Utilisation des transactions distribuées

Dans Amazon RDS for SQL Server, vous exécutez des transactions distribuées de la même manière que les transactions distribuées exécutées sur site :

- Utilisation des transactions `System.Transactions` .NET framework susceptibles d'être promues, ce qui optimise les transactions distribuées en reportant leur création jusqu'à ce qu'elles soient nécessaires.

  Dans ce cas, la promotion est automatique et ne nécessite aucune intervention de votre part. S'il n'y a qu'un gestionnaire de ressources dans la transaction, aucune promotion n'est effectuée. Pour de plus amples informations sur les portées des transactions implicites, veuillez consulter Implementing an Implicit Transaction using Transaction Scope dans la documentation Microsoft.

  Les transactions susceptibles d'être promues sont prises en charge avec ces implémentations .NET :

  - À partir de ADO.NET 2.0, `System.Data.SqlClient` prend en charge les transactions susceptibles d'être promues avec SQL Server. Pour de plus amples informations, veuillez consulter System.Transactions Integration with SQL Server dans la documentation Microsoft.
  - ODP.NET prend en charge `System.Transactions`. Une transaction locale est créée pour la première connexion ouverte dans la portée `TransactionsScope` à Oracle Database 11g version 1 (version 11.1) et ultérieures. Lorsqu'une deuxième connexion est ouverte, cette transaction est

automatiquement promue en tant que transaction distribuée. Pour de plus amples informations sur la prise en charge des transactions distribuées dans ODP.NET, veuillez consulter Microsoft Distributed Transaction Coordinator Integration dans la documentation Microsoft.

- Utilisation de l'instruction `BEGIN DISTRIBUTED TRANSACTION`. Pour de plus amples informations, veuillez consulter BEGIN DISTRIBUTE TRANSACTION (Transact-SQL) dans la documentation Microsoft.

Utilisation du suivi des transactions

RDS prend en charge le contrôle des suivis de transaction MSDTC et leur téléchargement à partir de l'instance de base de données RDS pour le dépannage. Vous pouvez contrôler les sessions de suivi de transaction en exécutant la procédure stockée RDS suivante.

```
exec msdb.dbo.rds_msdtc_transaction_tracing 'trace_action',
[@traceall='0|1'],
[@traceaborted='0|1'],
[@tracelong='0|1'];
```

Les paramètres suivants sont obligatoires :

- `trace_action` – Action de suivi. Il peut être `START`, `STOP` ou `STATUS`.

Les paramètres suivants sont facultatifs :

- `@traceall` – La valeur 1 permet de suivre toutes les transactions distribuées. La valeur par défaut est 0.
- `@traceaborted` – La valeur 1 permet de suivre les transactions distribuées annulées. La valeur par défaut est 0.
- `@tracelong` – La valeur 1 permet de suivre les transactions distribuées de longue durée. La valeur par défaut est 0.

Example de l'action de suivi START

Pour démarrer une nouvelle session de suivi des transactions, exécutez l'exemple d'instruction suivant.

```
exec msdb.dbo.rds_msdtc_transaction_tracing 'START',
@traceall='0',
@traceaborted='1',
@tracelong='1';
```

> **Note**
>
> Une seule session de suivi des transactions peut être active à la fois. Si une nouvelle commande `START` de session de suivi est émise alors qu'une session de suivi est active, une erreur est renvoyée et la session de suivi active reste inchangée.

Example de l'action de suivi STOP

Pour arrêter une session de suivi des transactions, exécutez l'instruction suivante.

```
exec msdb.dbo.rds_msdtc_transaction_tracing 'STOP'
```

Cette instruction arrête la session active de suivi des transactions et enregistre les données de suivi des transactions dans le répertoire de journal de l'instance de base de données RDS. La première ligne de la sortie contient le résultat global, et les lignes suivantes indiquent les détails de l'opération.

Vous trouverez ci-après un exemple d'arrêt de session de suivi réussi.

```
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\dtctrace.log:
 OS version    10.0.14393  (Currently running on 6.2.9200)
 Start Time    <timestamp>
 End Time      <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
```

Vous pouvez utiliser les informations détaillées pour rechercher le nom du fichier journal généré. Pour plus d'informations sur le téléchargement de fichiers journaux à partir de l'instance de base de données RDS, veuillez consulter Amazon RDS Fichiers journaux de base de données (p. 490).

Les journaux de session de suivi sont conservés sur l'instance pendant 35 jours. Les journaux de session de suivi plus anciens sont automatiquement supprimés.

Example de l'action de suivi STATUS

Pour suivre le statut d'une session de suivi des transactions, exécutez l'instruction suivante.

```
exec msdb.dbo.rds_msdtc_transaction_tracing 'STATUS'
```

Cette instruction affiche les éléments suivants sous forme de lignes séparées dans l'ensemble de résultats.

```
OK
SessionStatus: <Started|Stopped>
TraceAll: <True|False>
TraceAborted: <True|False>
TraceLongLived: <True|False>
```

La première ligne indique le résultat global de l'opération : `OK` ou `ERROR` avec des détails, le cas échéant. Les lignes suivantes indiquent des détails sur le statut de la session de suivi :

- `SessionStatus`, les valeurs suivantes sont possibles :
  - `Started` si une session de suivi est en cours d'exécution.
  - `Stopped` si aucune session de suivi n'est en cours d'exécution.
- Les indicateurs de session de suivi peuvent être `True` ou `False` en fonction de la façon dont ils ont été définis dans la commande `START`.

Modification de l'option MSDTC

Après avoir activé l'option `MSDTC`, vous pouvez modifier ses paramètres. Pour de plus amples informations sur la modification des paramètres d'option, veuillez consulter Modification d'un paramètre d'option (p. 219).

> **Note**
>
> Certaines modifications apportées aux paramètres d'option MSDTC nécessitent le redémarrage du service MSDTC. Cette exigence peut affecter les transactions distribuées en cours d'exécution.

Désactivation de MSDTC

Pour désactiver MSDTC, supprimez l'option `MSDTC` de son groupe d'options.

Console

Pour supprimer l'option MSDTC de son groupe d'options

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Groupes d'options.
3. Choisissez le groupe d'options avec l'option `MSDTC` (`msdtc-se-2016` dans les exemples précédents).
4. Choisissez Supprimer une option.
5. Sous Options de suppression, choisissez MSDTC pour Options à supprimer.
6. Sous Appliquer immédiatement, choisissez Oui pour supprimer l'option immédiatement, ou Non pour la supprimer lors du prochain créneau de maintenance.
7. Sélectionnez Supprimer.

Interface de ligne de commande

Pour supprimer l'option MSDTC de son groupe d'options

- Utilisez l'une des commandes suivantes.

  Example

  Pour Linux, macOS ou Unix :

```
aws rds remove-option-from-option-group \
    --option-group-name msdtc-se-2016 \
    --options MSDTC \
    --apply-immediately
```

  Pour Windows :

```
aws rds remove-option-from-option-group ^
    --option-group-name msdtc-se-2016 ^
    --options MSDTC ^
    --apply-immediately
```

Dépannage de MSDTC pour RDS SQL Server

Dans certains cas, vous pouvez avoir des difficultés à établir une connexion entre MSDTC s'exécutant sur un ordinateur client et le service MSDTC s'exécutant sur une instance de base de données RDS SQL Server. Dans ce cas, assurez-vous que :

- Les règles entrantes pour le groupe de sécurité associé à l'instance de base de données sont configurées correctement. Pour plus d'informations, consultez Impossible de se connecter à l'instance de base de données Amazon RDS (p. 1639).
- Votre ordinateur client est configuré correctement.
- Les règles de pare-feu MSDTC sur votre ordinateur client sont activées.

Pour configurer l'ordinateur client

1. Ouvrez Component Services (Services de composants).

   Ou, dans Server Manager (Gestionnaire de serveur), choisissez Tools (Outils), puis Component Services (Services de composants).
2. Développez successivement Component Services (Services de composants), Computers (Ordinateurs), My Computer (Mon ordinateur) et Distributed Transaction Coordinator (Coordinateur de transactions distribuées).
3. Ouvrez le menu contextuel (clic droit) pour Local DTC (DTC local) et choisissez Properties (Propriétés).
4. Choisissez l'onglet Security (Sécurité).
5. Choisissez toutes les options suivantes :
   - Network DTC Access (Accès DTC réseau)
   - Allow Inbound (Autoriser le trafic entrant)
   - Allow Outbound (Autoriser le trafic sortant)
6. Assurez-vous que le mode d'authentification correct est choisi :
   - Mutual Authentication Required (Authentification mutuelle requise) – La machine cliente est jointe au même domaine que les autres nœuds participant à une transaction distribuée, ou une relation d'approbation est configurée entre les domaines.
   - No Authentication Required (Aucune authentification requise) – Tous les autres cas.
7. Choisissez OK pour enregistrer vos modifications.
8. Si vous êtes invité à redémarrer le service, choisissez Oui.

Pour activer les règles de pare-feu MSDTC

1. Ouvrez le pare-feu Windows, puis choisissez Paramètres avancés.

   Ou, dans Gestionnaire de serveur, choisissez Outils, puis Pare-feu Windows avec fonctions avancées de sécurité.

   Note

   En fonction de votre système d'exploitation, le Pare-feu Windows peut s'appeler « Pare-feu Windows Defender ».
2. Choisissez Règles entrantes dans le volet de gauche.
3. Activez, si ce n’est pas déjà le cas, les règles de pare-feu suivantes :
   - Coordinateur de transactions distribuées (RPC)
   - Coordinateur de transactions distribuées (RPC-EPMAP)
   - Coordinateur de transactions distribuées (TCP-Entrée)
4. Fermez le pare-feu Windows.

Tâches DBA courantes pour Microsoft SQL Server

Cette section décrit les implémentations spécifiques à Amazon RDS de certaines tâches d'administration de base de données courantes pour les instances de base de données exécutant le moteur de base de données Microsoft SQL Server. Pour offrir une expérience de service géré, Amazon RDS ne fournit pas l'accès shell aux instances de bases de données et limite l'accès à certaines tables et procédures système qui requièrent des privilèges avancés.

Note

Lors de l'utilisation d'une instance de base de données SQL Server, vous pouvez exécuter des scripts pour modifier une base de données nouvellement créée, mais vous ne pouvez pas modifier la base de données [model], celle utilisée comme modèle pour les nouvelles bases de données.

Rubriques

- Accès à la base de données tempdb sur les instances de base de données Microsoft SQL Server sur Amazon RDS (p. 760)
- Analyse de la charge de travail d'une base de données sur une instance de base de données Amazon RDS avec l'Assistant Paramétrage SQL Server (p. 762)
- Classements et jeux de caractères pour Microsoft SQL Server (p. 766)
- Détermination d'un modèle de récupération pour votre base de données Microsoft SQL Server (p. 768)
- Détermination de l'heure du dernier basculement (p. 769)
- Désactivation des insertions rapides pendant le chargement par lots (p. 770)
- Suppression d'une base de données Microsoft SQL Server (p. 770)
- Modification du nom d'une base de données Microsoft SQL Server dans un déploiement Multi-AZ (p. 771)
- Réinitialisation du mot de passe du rôle db_owner (p. 771)
- Restauration des instances de bases de données résiliées faute de licence (p. 771)
- Passage d'une base de données Microsoft SQL Server de l'état OFFLINE à l'état ONLINE (p. 772)
- Utilisation de la capture de données modifiées (p. 772)
- Utilisation de SQL Server Agent (p. 775)
- Utilisation des journaux Microsoft SQL Server (p. 776)
- Utilisation des fichiers de trace et de vidage (p. 777)

Accès à la base de données tempdb sur les instances de base de données Microsoft SQL Server sur Amazon RDS

Vous pouvez accéder à la base de données `tempdb` sur vos instances de base de données Microsoft SQL Server sur Amazon RDS. Vous pouvez exécuter le code sur `tempdb` à l'aide de Transact-SQL via Microsoft SQL Server Management Studio (SSMS) ou via toute autre application cliente SQL standard. Pour plus d'informations sur la connexion à votre instance de base de données, consultez Connexion à une instance de base de données exécutant le moteur de base de données Microsoft SQL Server (p. 618).

L'utilisateur principal pour votre instance de base de données bénéficie d'un accès `CONTROL` à `tempdb` afin qu'il puisse modifier les options de la base de données `tempdb`. L'utilisateur principal n'est pas le propriétaire de la base de données `tempdb`. Si nécessaire, l'utilisateur principal peut accorder un accès `CONTROL` à d'autres utilisateurs afin qu'ils puissent eux aussi modifier les options de la base de données `tempdb`.

Note

Vous ne pouvez pas exécuter de commandes DBCC (Database Console) sur la base de données `tempdb`.

Modification des options de la base de données tempdb

Vous pouvez modifier les options de base de données sur la base de données `tempdb` sur vos instances de base de données Amazon RDS. Pour de plus amples informations sur les options qui peuvent être modifiées, veuillez consulter Base de données tempdb dans la documentation Microsoft.

Les options de base de données telles que les options de taille maximale des fichiers sont persistantes une fois que vous redémarrez votre instance de base de données. Vous pouvez modifier les options de base de données pour optimiser les performances lors de l'importation des données et pour éviter le manque d'espace de stockage.

Optimisation des performances lors de l'importation de données

Afin d'optimiser les performances lors de l'importation de grandes quantités de données dans votre instance de base de données, définissez les propriétés `SIZE` et `FILEGROWTH` de la base de données tempdb sur des grands chiffres. Pour de plus amples informations sur la façon d'optimiser `tempdb`, veuillez consulter Optimisation des performances de la base de données tempdb dans la documentation Microsoft.

L'exemple suivant illustre la définition de la taille sur 100 Go et la croissance des fichiers sur 10 pour cent.

```
alter database[tempdb] modify file (NAME = N'templog', SIZE=100GB, FILEGROWTH = 10%)
```

Prévention des problèmes de stockage

Pour éviter que la base de données `tempdb` utilise tout l'espace disque disponible, définissez la propriété `MAXSIZE`. L'exemple suivant illustre la définition de la propriété sur 2 048 Mo.

```
alter database [tempdb] modify file (NAME = N'templog', MAXSIZE = 2048MB)
```

Réduction de la base de données tempdb

Il existe deux façons de réduire la base de données `tempdb` sur votre instance de base de données Amazon RDS. Vous pouvez utiliser la procédure `rds_shrink_tempdbfile` ou vous pouvez définir la propriété `SIZE`.

Utilisation de la procédure rds_shrink_tempdbfile

Vous pouvez utiliser la procédure Amazon RDS `msdb.dbo.rds_shrink_tempdbfile` pour réduire la base de données `tempdb`. Vous pouvez uniquement appeler `rds_shrink_tempdbfile` si vous disposez de l'accès `CONTROL` à `tempdb`. Lorsque vous appelez `rds_shrink_tempdbfile`, il n'y a aucun temps d'arrêt pour votre instance de base de données.

La procédure `rds_shrink_tempdbfile` possède les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`@temp_filename`	SYSNAME	—	obligatoire	Le nom logique du fichier à réduire.
`@target_size`	int	null	facultatif	La nouvelle taille du fichier en mégaoctets.

L'exemple suivant permet d'obtenir les noms des fichiers de la base de données `tempdb`.

```
use tempdb;
```

```
GO

select name, * from sys.sysfiles;
GO
```

L'exemple suivant réduit un fichier de base de données `tempdb` nommé `test_file` et demande une nouvelle taille de `10` mégaoctets :

```
exec msdb.dbo.rds_shrink_tempdbfile @temp_filename = N'test_file', @target_size = 10;
```

Configuration de la propriété SIZE

Vous pouvez également réduire la base de données `tempdb` en configurant la propriété `SIZE` et en redémarrant votre instance de base de données. Pour plus d'informations sur le redémarrage de votre instance de base de données, consultez Redémarrage d'une instance de base de données (p. 272).

L'exemple suivant illustre la définition de la propriété `SIZE` sur 1 024 Mo.

```
alter database [tempdb] modify file (NAME = N'templog', SIZE = 1024MB)
```

Considérations sur les déploiements multi-AZ

Si votre instance de base de données Amazon RDS est un déploiement multi-AZ pour Microsoft SQL Server avec mise en miroir de la base de données ou Always On, certains points sont à prendre en compte.

La base de données `tempdb` ne peut pas être répliquée. Aucune des données que vous stockez sur votre instance principale n'est répliquée sur votre instance secondaire.

Si vous modifiez les options de base de données sur la base de données `tempdb`, vous pouvez capturer ces modifications sur l'instance secondaire en utilisant l'une des méthodes suivantes :

- Tout d'abord, modifiez votre instance de base de données et désactivez le déploiement multi-AZ, puis modifier tempdb, puis enfin réactivez le déploiement multi-AZ. Cette méthode n'entraîne aucun temps d'arrêt.

  Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).
- Tout d'abord, modifiez `tempdb` dans l'instance principale d'origine, puis exécutez un basculement manuel et enfin modifiez `tempdb` dans la nouvelle instance principale. Cette méthode implique un temps d'arrêt.

  Pour plus d'informations, consultez Redémarrage d'une instance de base de données (p. 272).

Analyse de la charge de travail d'une base de données sur une instance de base de données Amazon RDS avec l'Assistant Paramétrage SQL Server

L'Assistant Paramétrage du moteur de base de données est une application cliente fournie par Microsoft qui analyse la charge de travail de la base de données et recommande un ensemble optimal d'index pour vos bases de données Microsoft SQL Server en fonction des types de requêtes que vous exécutez. Comme SQL Server Management Studio, vous exécutez l'Assistant Paramétrage à partir d'un ordinateur client qui se connecte à votre instance de base de données Amazon RDS exécutant SQL Server.

L'ordinateur client peut être un ordinateur local que vous exécutez sur site au sein de votre propre réseau ou une instance Amazon EC2 Windows qui s'exécute dans la même région que votre instance de base de données Amazon RDS.

Cette section montre comment capturer une charge de travail pour que l'Assistant Paramétrage l'analyse. Il s'agit du processus privilégié pour capturer une charge de travail parce que Amazon RDS limite l'accès de l'hôte à l'instance SQL Server. La documentation complète sur l'Assistant de réglage est disponible sur MSDN.

Pour utiliser l'Assistant Paramétrage, vous devez lui fournir ce qu'on appelle une charge de travail. Une charge de travail est un ensemble d'instructions Transact-SQL qui s'exécutent sur une base de données ou des bases de données que vous voulez régler. L'Assistant Paramétrage du moteur de base de données utilise les fichiers trace, les tables de trace, les scripts Transact-SQL ou les fichiers XML comme entrées de charge de travail lors du réglage des bases de données. Lors de l'utilisation de Amazon RDS, une charge de travail peut être un fichier sur un ordinateur client ou un tableau de base de données sur une instance de base de données Amazon RDS SQL Server accessible à votre ordinateur client. Le fichier ou la table doit contenir des requêtes sur les bases de données que vous voulez régler dans un format adapté à la relecture.

Pour que l'Assistant Paramétrage soit le plus efficace, une charge de travail doit être aussi réaliste que possible. Vous pouvez générer un fichier de charge de travail ou une table en exécutant une trace sur votre instance de base de données. Pendant l'exécution d'une trace, vous pouvez simuler une charge sur votre instance de base de données ou exécuter vos applications avec une charge normale.

Il existe deux types de trace : côté client et côté serveur. Une trace côté client est plus facile à configurer et vous pouvez observer les événements de trace capturés en temps réel dans SQL Server Profiler. Une trace côté serveur est plus complexe à configurer et nécessite quelque script Transact-SQL. De plus, comme la trace est écrite dans un fichier de l'instance de base de données Amazon RDS, l'espace de stockage est utilisé par la trace. Il importe de tracer la quantité d'espace de stockage qu'une trace côté serveur utilise, parce que l'instance de base de données peut entrer dans un état de stockage complet et n'être plus disponible si elle se trouve à court d'espace de stockage.

Pour une trace côté client, quand une quantité suffisante de données de trace a été capturée dans SQL Server Profiler, vous pouvez générer le fichier de charge de travail en enregistrant la trace sur un fichier de votre ordinateur local ou dans une table de base de données d'une instance de base de données accessible à votre ordinateur client. Le principal désavantage de l'utilisation d'une trace côté client est que la trace peut ne pas capturer toutes les requêtes quand elle est soumise à de lourdes charges. Cela pourrait affaiblir l'efficacité de l'analyse exécutée par l'Assistant Paramétrage du moteur de base de données. Si vous devez exécuter une trace soumise à des charges massives et que vous voulez vous assurer qu'elle capture chaque requête pendant une session de trace, vous devez utiliser une trace côté serveur.

Pour une trace côté serveur, vous devez obtenir les fichiers de trace de l'instance de base de données en un fichier de charge de travail adapté ou vous pouvez enregistrer la trace sur une table de l'instance de base de données une fois la trace terminée. Vous pouvez utiliser SQL Server Profiler pour enregistrer la trace sur un fichier de votre ordinateur local ou faire en sorte que l'Assistant Paramétrage lise à partir de la table de trace sur l'instance de base de données.

Exécution d'une trace côté client sur une instance de base de données SQL Server

Pour exécuter une trace côté client sur une instance de base de données SQL Server

1. Démarrez SQL Server Profiler. Il est installé dans le dossier Outils de performance de votre dossier d'instances SQL Server. Vous devez charger ou définir un modèle de définition de trace pour démarrer une trace côté client.
2. Dans le menu du fichier SQL Server Profiler, choisissez New Trace (Nouvelle trace). Dans la boîte de dialogue Connect to Server (Se connecter au serveur), entrez le point de terminaison de l'instance de

base de données, le port, l'identifiant principal et le mot de passe de la base de données sur laquelle vous souhaitez exécuter une trace.

3. Dans la boîte de dialogue Propriétés de la trace, entrez un nom de trace et choisissez un modèle de définition de trace. Un modèle par défaut, TSQL_Replay, est fourni avec l'application. Vous pouvez modifier ce modèle pour définir votre trace. Modifiez les événements et les informations relatives aux événements sous l'onglet Sélection des événements de la boîte de dialogue Propriétés de la trace. Pour plus d'informations sur les modèles de définition de trace et l'utilisation de SQL Server Profiler pour spécifier une trace côté client, consultez la documentation dans MSDN.
4. Démarrez la trace côté client et observez les requêtes SQL en temps réel tandis qu'elles s'exécutent sur votre instance de base de données.
5. Sélectionnez Stop Trace (Arrêter la trace) dans le menu Fichier lorsque vous avez terminé la trace. Enregistrez les résultats comme fichier ou comme table de trace sur votre instance de base de données.

Exécution d'une trace côté serveur sur une instance de base de données SQL Server

L'écriture de scripts pour créer une trace côté serveur peut être complexe et au-delà de la portée de ce document. Cette section contient des scripts que vous pouvez utiliser comme exemples. Comme pour une trace côté client, l'objectif est de créer un fichier de charge de travail ou une table de trace que vous pouvez ouvrir à l'aide de l'Assistant Paramétrage du moteur de base de données.

L'exemple abrégé suivant est un script qui démarre une trace côté serveur et capture les détails dans un fichier de charge de travail. La trace s'enregistre initialement sur le fichier RDSTrace.trc du répertoire D:\RDSDBDATA\Log et se réinitialise tous les 100 Mo, si bien que les fichiers de trace suivants se nomment 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
```

L'exemple suivant illustre un script qui arrête une trace. Notez qu'une trace créée par le précédent script continue à s'exécuter jusqu'à ce que vous arrêtiez explicitement la trace ou que le processus ne dispose plus d'espace disque suffisant.

```
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
```

Vous pouvez enregistrer les résultats de la trace côté serveur sur une table de base de données et utiliser celle-ci comme charge de travail pour l'Assistant Paramétrage à l'aide de la fonction fn_trace_gettable. Les commandes suivantes chargent les résultats de tous les fichiers nommés RDSTrace.trc dans le répertoire D:\rdsdbdata\Log, y compris tous les fichiers de substitution comme RDSTrace_1.trc, dans une table nommée RDSTrace de la base de données active.

```
SELECT * INTO RDSTrace
FROM fn_trace_gettable('D:\rdsdbdata\Log\RDSTrace.trc', default);
```

Pour enregistrer un fichier de substitution spécifique dans une table, par exemple le fichier RDSTrace_1.trc, spécifiez le nom du fichier de substitution et remplacez le dernier paramètre par défaut de fn_trace_gettable par 1.

```
SELECT * INTO RDSTrace_1
FROM fn_trace_gettable('D:\rdsdbdata\Log\RDSTrace_1.trc', 1);
```

Exécution de l'Assistant Paramétrage avec une trace

Une fois que vous créez une trace, comme fichier local ou comme table de base de données, vous pouvez exécuter l'Assistant Paramétrage sur votre instance de base de données. Microsoft propose une documentation relative à l'utilisation de l'Assistant de réglage du moteur de base de données dans MSDN. L'utilisation de l'Assistant Paramétrage avec Amazon RDS repose sur le même processus que l'utilisation d'une instance SQL Server autonome et distante. Vous pouvez utiliser l'interface utilisateur de l'Assistant Paramétrage sur votre ordinateur client ou choisir l'utilitaire dta.exe à partir de la ligne de commande. Dans les deux cas, vous devez vous connecter à l'instance de base de données Amazon RDS à l'aide du point de terminaison de l'instance de base de données, et fournir votre nom d'utilisateur maître et votre mot de passe utilisateur maître lors de l'utilisation de l'Assistant Paramétrage.

L'exemple de code suivant illustre l'utilisation de l'utilitaire de ligne de commande dta.exe sur une instance de base de données Amazon RDS avec le point de terminaison **`dta.cnazcmklsdei.us-east-1.rds.amazonaws.com`**. L'exemple inclut l'identifiant principal **`admin`** et le mot de passe d'utilisateur principal **`test`**. L'exemple de base de données à régler se nomme **`RDSDTA`** et la charge de travail entrante est un fichier trace sur l'ordinateur local nommé **`C:\RDSTrace.trc`**. L'exemple de code de ligne de commande spécifie également une session de trace nommée **`RDSTrace1`**, ainsi que les fichiers de sortie sur l'ordinateur local nommés **`RDSTrace.sql`** pour le script de sortie SQL, **`RDSTrace.txt`** pour un fichier résultat et **`RDSTrace.xml`** pour un fichier XML de l'analyse. Il existe aussi une table d'erreur spécifiée sur la base de données RDSDTA et nommée **`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
```

Voici le même exemple de code de ligne de commande, à ceci près que la charge de travail en entrée est une table de l'instance Amazon RDS distante nommée **`RDSTrace`** qui se trouve sur la base de données **`RDSDTA`**.

```
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
```

La liste complète des paramètres de ligne de commande de l'utilitaire dta se trouve dans MSDN.

Classements et jeux de caractères pour Microsoft SQL Server

SQL Server prend en charge les classements à différents niveaux. Vous définissez le classement de serveur par défaut lorsque vous créez l'instance de base de données. Vous pouvez remplacer le classement au niveau de la base de données, de la table ou de la colonne.

Rubriques

- Classement de niveau serveur pour Microsoft SQL Server (p. 766)
- Classement au niveau de la base de données pour Microsoft SQL Server (p. 768)

Classement de niveau serveur pour Microsoft SQL Server

Lorsque vous créez une instance de base de données Microsoft SQL Server, vous pouvez définir le classement de serveur que vous souhaitez utiliser. Si vous ne choisissez pas un autre classement, le classement de serveur sera défini par défaut sur SQL_Latin1_General_CP1_CI_AS. Le classement de serveur est appliqué par défaut à toutes les bases de données et à tous les objets de base de données.

> Note
>
> Vous ne pouvez pas modifier le classement lorsque vous effectuez une restauration à partir d'un instantané de base de données.

Amazon RDS prend actuellement en charge les classements de serveur suivants :

Classement (Collation)	Description
Chinese_PRC_CI_AS	Chinois - RPC, insensible à la casse, sensible aux accents, insensible au type de kana, insensible à la largeur
Chinese_Taiwan_Stroke_CI_AS	Chinois de Taiwan, insensible à la casse, sensible aux accents, insensible au type de kana, insensible à la largeur
Finnish_Swedish_CI_AS	Finnois, suédois et suédois (Finlande), insensible à la casse, sensible aux accents, sensible aux caractères Kana et insensible à la largeur.
French_CI_AS	French, insensible à la casse, sensible aux accents, insensible au type de kana, insensible à la largeur
Hebrew_BIN	Hebrew, tri binaire
Japanese_CI_AS	Japanese, insensible à la casse, sensible aux accents, insensible au type de kana, insensible à la largeur
Korean_Wansung_CI_AS	Korean-Wansung, insensible à la casse, sensible aux accents, insensible au type de kana, insensible à la largeur
Latin1_General_100_BIN	Latin1-General-100, tri binaire
Latin1_General_100_BIN2	Latin1-General-100, tri de comparaison de points de code binaire

Classement (Collation)	Description
Latin1_General_100_CI_AS	Latin1-General-100, insensible à la casse, sensible aux accents, insensible au type de kana, insensible à la largeur
Latin1_General_BIN	Latin1-General, tri binaire
Latin1_General_CI_AI	Latin1-General, insensible à la casse, insensible aux accents, insensible au type de kana, insensible à la largeur
Latin1_General_CI_AS	Latin1-General, insensible à la casse, sensible aux accents, insensible au type de kana, insensible à la largeur
Latin1_General_CS_AS	Latin1-General, sensible à la casse, sensible aux accents, insensible au type de kana, insensible à la largeur
Modern_Spanish_CI_AS	Modern-Spanish, insensible à la casse, sensible aux accents, insensible au type de kana, insensible à la largeur
SQL_Latin1_General_CP1_CI_AI	Latin1-General, insensible à la casse, insensible aux accents, insensible au type de kana, insensible à la largeur pour les données Unicode, l'ordre de tri SQL Server 54 sur la page de codes 1252 pour les données non Unicode
SQL_Latin1_General_CP1_CI_AS (par défaut)	Latin1-General, insensible à la casse, sensible aux accents, insensible au type de kana, insensible à la largeur pour les données Unicode, ordre de tri SQL Server 52 sur la page de codes 1252 pour les données non Unicode
SQL_Latin1_General_CP1_CS_AS	Latin1-General, sensible à la casse, sensible aux accents, insensible au type de kana, insensible à la largeur pour les données Unicode, l'ordre de tri SQL Server 51 sur la page de codes 1252 pour les données non Unicode
SQL_Latin1_General_CP437_CI_AI	Latin1-General, insensible à la casse, insensible aux accents, insensible au type de kana, insensible à la largeur pour les données Unicode, ordre de tri SQL Server 34 sur la page de codes 437 pour les données non Unicode
SQL_Latin1_General_CP850_BIN2	Latin1-General, tri de comparaison des points de code binaire pour les données Unicode, l'ordre de tri SQL Server 40 sur la page de codes 850 pour les données non Unicode
SQL_Latin1_General_CP850_CI_AS	Latin1-General, insensible à la casse, sensible aux accents, insensible au type de kana, insensible à la largeur pour les données Unicode, ordre de tri SQL Server 42 sur la page de codes 850 pour les données non Unicode

Pour choisir la classement :

- Si vous utilisez la console Amazon RDS, lors de la création d'une nouvelle instance de base de données, choisissez Additional configuration (Configuration supplémentaire), puis choisissez le classement dans le menu Collation (Classement) sous Database options (Options de base de données). Pour de plus amples informations, veuillez consulter Création d'une instance de base de données Amazon RDS (p. 146).
- Si vous utilisez l'AWS CLI, utilisez l'option `--character-set-name` avec la commande `create-db-instance`. Pour de plus amples informations, veuillez consulter create-db-instance.
- Si vous utilisez l'API Amazon RDS, utilisez le paramètre `CharacterSetName` avec l'opération `CreateDBInstance`. Pour de plus amples informations, veuillez consulter CreateDBInstance.

Classement au niveau de la base de données pour Microsoft SQL Server

Vous pouvez modifier la classement par défaut au niveau base de données, table ou colonne, en remplaçant le classement de la création d'une nouvelle base de données ou d'un objet de base de données. Par exemple, si votre classement de serveur par défaut est SQL_Latin1_General_CP1_CI_AS, vous pouvez le remplacer par Mohawk_100_CI_AS pour la prise en charge du classement Mohawk. Même les arguments d'une requête peuvent être l'objet d'un cast de type afin d'utiliser un classement différent si nécessaire.

Par exemple, la requête suivante modifie le classement par défaut de la colonne AccountName en 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];
```

Le moteur de base de données Microsoft SQL Server prend en charge Unicode à l'aide des types de données intégrés NCHAR, NVARCHAR et NTEXT. Par exemple, si vous avez besoin du support CJC, utilisez ces types de données Unicode pour le stockage des caractères et remplacer le classement de serveur par défaut lors de la création de vos bases de données et tables. Voici plusieurs liens depuis Microsoft couvrant le classement et le support Unicode pour SQL Server :

- Working with Collations (Utilisation des collectes)
- Collation and International Terminology (Collecte et terminologie internationale)
- Using SQL Server Collations (Utilisation de collectes SQL Server)
- International Considerations for Databases and Database Engine Applications (Considérations internationales pour les bases de données et les applications de moteur de base de données)

Détermination d'un modèle de récupération pour votre base de données Microsoft SQL Server

Dans Amazon RDS, le modèle de récupération, la période de conservation et le statut de base de données sont liés.

Il est important de comprendre les conséquences avant de modifier l'un de ces paramètres. Chaque paramètre peut affecter les autres. Exemples :

- Si vous remplacez le modèle de récupération d'une base de données par le modèle SIMPLE ou BULK_LOGGED alors que la conservation des sauvegardes est activée, Amazon RDS rétablit le modèle de récupération FULL dans les cinq minutes qui suivent. Cela entraîne également la prise d'un instantané de l'instance de base de données par RDS.
- Si vous définissez la conservation des sauvegardes sur `0` jour(s), RDS définit le modèle de récupération sur SIMPLE.
- Si vous remplacez le modèle de récupération d'une base de données SIMPLE par une autre option alors que la conservation des sauvegardes est définie sur `0` jour(s), RDS rétablit le modèle de récupération SIMPLE.

> **Important**
>
> Ne changez jamais le modèle de récupération sur des instances multi-AZ, même s'il semble que vous pouvez le faire (par exemple, en utilisant ALTER DATABASE). La conservation des sauvegardes et donc le mode de récupération FULL sont nécessaires pour l'option multi-AZ. Si vous modifiez le modèle de récupération, RDS le rétablit immédiatement sur FULL.
> Cette réinitialisation automatique oblige RDS à reconstruire complètement le miroir. Au cours de cette reconstruction, la disponibilité de la base de données est dégradée pendant environ 30 à 90 minutes jusqu'à ce que le miroir soit prêt pour le basculement. L'instance de base de données connaît également une dégradation de performances de la même façon que lors d'une conversion du mode mono-AZ au mode multi-AZ. La durée pendant laquelle les performances sont dégradées dépend de la taille de stockage de base de données (plus la base de données stockée est grande, plus la dégradation est longue).

Pour de plus amples informations sur les modèles de récupération SQL Server, veuillez consulter Modes de récupération (SQL Server) dans la documentation Microsoft.

Détermination de l’heure du dernier basculement

Pour déterminer l’heure du dernier basculement, utilisez la procédure stockée suivante :

```
execute msdb.dbo.rds_failover_time;
```

Cette procédure renvoie les informations suivantes.

Paramètre de sortie	Description
errorlog_available_from	Affiche l'heure à partir de laquelle les journaux d'erreurs sont disponibles dans le répertoire des journaux.
recent_failover_time	Affiche l’heure du dernier basculement si elle est disponible à partir des journaux d'erreurs. Sinon, la valeur affichée est `null`.

> **Note**
>
> La procédure stockée recherche l’heure de basculement la plus récente dans tous les journaux d'erreurs SQL Server disponibles dans le répertoire des journaux. Si les messages de basculement ont été remplacés par SQL Server, la procédure ne récupère pas l’heure de basculement.

Example de Aucun basculement récent

Cet exemple illustre la sortie lorsqu'il n'y a pas de basculement récent dans les journaux d'erreurs. Aucun basculement ne s'est produit depuis le 29/04/2020 à 23:59:00.01.

errorlog_available_from	recent_failover_time
2020-04-29 23:59:00.0100000	null

Example de Basculement récent

Cet exemple illustre la sortie lorsqu'un basculement récent est détecté dans les journaux d'erreurs. Le basculement le plus récent a eu lieu le 05/05/2020 à 18:57:51.89.

errorlog_available_from	recent_failover_time
2020-04-29 23:59:00.0100000	2020-05-05 18:57:51.8900000

Désactivation des insertions rapides pendant le chargement par lots

À partir de SQL Server 2016, les insertions rapides sont activées par défaut. Les insertions rapides tirent parti d'une journalisation minimale quand la base de données est en mode de récupération simple ou utilisant les journaux de transactions pour optimiser les performances d'insertion. Avec les insertions rapides, chaque lot de chargement en masse acquiert de nouvelles extensions en ignorant la recherche d'allocation des extensions existantes avec l'espace libre disponible pour optimiser les performances d'insertion.

Avec les insertions rapides, les chargements en masse de lots de petite taille peuvent aboutir à une plus grande quantité d'espace inutilisé consommée par les objets. S'il n'est pas possible d'augmenter la taille de lot, l'activation de cet indicateur de trace 692 peut contribuer à réduire l'espace réservé inutilisé, mais au détriment des performances. L'activation de cet indicateur de trace désactive les insertions rapides lors du chargement en masse de données dans un segment de mémoire ou un index cluster.

Vous activez l'indicateur de trace 692 en tant que paramètre de démarrage à l'aide de groupes de paramètres de base de données. Pour plus d'informations, consultez Utilisation de groupes de paramètres de base de données (p. 225).

L'indicateur de trace 692 est pris en charge pour Amazon RDS sur SQL Server 2016 et versions ultérieures. Pour de plus amples informations sur les indicateurs de trace, veuillez consulter DBCC TRACEON - Trace Flags dans la documentation Microsoft.

Suppression d'une base de données Microsoft SQL Server

Vous pouvez supprimer la base de données d'une instance de base de données Amazon RDS exécutant Microsoft SQL Server dans un déploiement Multi-AZ ou à zone de disponibilité unique. Pour supprimer la base de données, utilisez la commande suivante :

```
--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**
>
> Utilisez des apostrophes droites dans la commande. Tout autre type de guillemet entraînera une erreur.

Après cette procédure de suppression de la base de données, Amazon RDS supprime toutes les connexions existantes à cette dernière, ainsi que son historique de sauvegarde.

Modification du nom d'une base de données Microsoft SQL Server dans un déploiement Multi-AZ

Pour renommer une instance de base de données Microsoft SQL Server qui utilise un déploiement Multi-AZ, procédez comme suit :

1. Commencez par désactiver Multi-AZ pour l'instance de base de données.
2. Renommez la base de données en exécutant `rdsadmin.dbo.rds_modify_db_name`.
3. Ensuite, activez la mise en miroir multi-AZ ou l'option Groupes de disponibilité AlwaysOn pour l'instance de base de données, afin de rétablir son état d'origine.

Pour plus d'informations, consultez Ajout d'un déploiement multi-AZ à une instance de base de données Microsoft SQL Server (p. 665).

> **Note**
>
> Si votre instance n'utilise pas le mode multi-AZ, vous n'avez pas besoin de modifier d'autres paramètres avant ou après l'exécution de `rdsadmin.dbo.rds_modify_db_name`.

Exemple : dans l'exemple suivant, la procédure stockée `rdsadmin.dbo.rds_modify_db_name` change le nom d'une base de données de **`MOO`** à **`ZAR`**. Cela revient à exécuter l'instruction `DDL ALTER DATABASE [MOO] MODIFY NAME = [ZAR]`.

```
EXEC rdsadmin.dbo.rds_modify_db_name N'MOO', N'ZAR'
GO
```

Réinitialisation du mot de passe du rôle `db_owner`

Si vous vous êtes vous-même bloqué l'accès au rôle `db_owner` sur votre base de données Microsoft SQL Server, vous pouvez réinitialiser le mot de passe du rôle `db_owner` en modifiant le mot de passe maître de l'instance de base de données. En modifiant le mot de passe maître de l'instance de base de données, vous pouvez reconquérir l'accès à l'instance de base de données, accéder aux bases de données à l'aide du mot de passe modifié pour le rôle `db_owner` et restaurer les privilèges pour le rôle `db_owner` qui peuvent avoir été malencontreusement révoqués. Vous pouvez modifier le mot de passe d'une instance de base de données à l'aide de la console Amazon RDS, de la commande modify-db-instance de l'AWS CLI ou de l'opération ModifyDBInstance. Pour de plus amples informations sur la modification d'une instance de base de données, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

Restauration des instances de bases de données résiliées faute de licence

Microsoft a demandé à ce que certains clients Amazon RDS n'ayant pas signalé leurs informations Microsoft License Mobility résilient leur instance de base de données. Amazon RDS prend des instantanés

de ces instances de base de données et vous pouvez restituer à partir de l'instantané vers une nouvelles instance de base de données qui dispose d'un modèle License Included (License incluse).

Vous pouvez effectuer la restauration à partir d'un instantané de Standard Edition vers Standard Edition ou Enterprise Edition.

Vous pouvez effectuer la restauration à partir d'un instantané d'Enterprise Edition vers Standard Edition ou Enterprise Edition.

Pour restaurer à partir d'un instantané SQL Server après que Amazon RDS a créé un instantané final de votre instance :

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Snapshots (Instantanés).
3. Choisissez l'instantané de l'instance de base de données SQL Server. Amazon RDS crée un instantané final de votre instance de base de données. Le nom de l'instantané de l'instance terminée est au format `instance_name-final-snapshot`. Par exemple, si votre instance de base de données s'appelait **`mytest.cdxgahslksma.us-east-1.rds.com`**, l'instantané final s'appellerait **`mytest-final-snapshot`** et serait situé dans la même région AWS que l'instance de base de données d'origine.
4. Pour Actions, choisissez Restore Snapshot (Restaurer l'instantané).

   La fenêtre Restore DB Instance (Restituer l'instance de base de données) s'affiche.
5. Pour Modèle de licence, sélectionnez licence incluse.
6. Sélectionnez le moteur de base de données SQL Server que vous voulez utiliser.
7. Pour DB Instance Identifier (Identifiant d'instance DB), entrez le nom de l'instance de base de données restaurée.
8. Choisissez Restore DB Instance.

Pour plus d'informations sur la restauration à partir d'un instantané, consultez Restauration à partir d'un instantané de base de données (p. 329).

Passage d'une base de données Microsoft SQL Server de l'état OFFLINE à l'état ONLINE

Vous pouvez faire passer votre base de données Microsoft SQL Server sur une instance de base de données Amazon RDS de l'état `OFFLINE` à l'état `ONLINE`.

Méthode SQL Server	Méthode Amazon RDS
ALTER DATABASE *db_name* SET ONLINE;	EXEC rdsadmin.dbo.rds_set_database_online *db_name*

Utilisation de la capture de données modifiées

Amazon RDS prend en charge la capture de données modifiées (CDC) pour vos instances de base de données s'exécutant sur Microsoft SQL Server. CDC capture les modifications apportées aux données de vos tables. CDC stocke les métadonnées relatives à chaque modification et vous pouvez y accéder ultérieurement. Pour plus d'informations sur le fonctionnement de CDC, consultez Capture de données modifiées dans la documentation Microsoft.

Pour utiliser la fonction CDC avec vos instances de base de données Amazon RDS, vous devez tout d'abord l'activer au niveau de la base de données en exécutant `msdb.dbo.rds_cdc_enable_db`. Vous devez avoir des droits d'utilisateur principal pour pouvoir activer CDC dans l'instance de base de données Amazon RDS. Une fois la fonction CDC activée, tout utilisateur `db_owner` de cette base de données peut activer ou désactiver CDC sur les tables de cette base de données.

> **Important**
>
> Pendant les restaurations, la fonction CDC est désactivée. L'ensemble des métadonnées associées est automatiquement supprimé de la base de données. Cela s'applique aux restaurations d'instantané, aux restaurations à un instant dans le passé et aux restaurations SQL Server Native depuis S3. Après avoir exécuté l'un de ces types de restaurations, vous pouvez réactiver CDC et respécifier les tables à suivre.

Pour activer CDC pour une instance de base de données, exécutez la procédure stockée `msdb.dbo.rds_cdc_enable_db`.

```
exec msdb.dbo.rds_cdc_enable_db 'database_name'
```

Pour désactiver le CDC pour une instance de base de données, exécutez la procédure stockée `msdb.dbo.rds_cdc_disable_db`.

```
exec msdb.dbo.rds_cdc_disable_db 'database_name'
```

Rubriques

- Suivi des tables avec CDC (p. 773)
- Tâches CDC (p. 774)
- Capture de données modifiées (CDC) pour les instances multi-AZ (p. 774)

Suivi des tables avec CDC

Une fois que CDC est activé sur la base de données, vous pouvez démarrer le suivi de tables spécifiques. Vous pouvez choisir les tableaux à suivre en exécutant 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'
;
```

Pour afficher la configuration CDC de vos tableaux, exécutez 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'
```

```
;
```

Pour plus d'informations sur les tables, fonctions et procédures stockées CDC dans la documentation SQL Server, consultez les rubriques suivantes :

- Procédures stockées CDC (Transact-SQL)
- Fonctions CDC (Transact-SQL)
- Tableaux CDC (Transact-SQL)

Tâches CDC

Quand vous activez CDC, SQL Server crée les tâches CDC. Les propriétaires de base de données (`db_owner`) peuvent afficher, créer, modifier et supprimer les tâches CDC. Cependant, le compte système RDS en est propriétaire. Par conséquent, les tâches ne sont pas visibles des vues natives, des procédures ou de SQL Server Management Studio.

Pour contrôler le comportement de CDC dans une base de données, utilisez les procédures SQL Server natives telles que sp_cdc_enable_table et sp_cdc_start_job . Pour modifier les paramètres des tâches CDC, comme `maxtrans` et `maxscans`, vous pouvez utiliser sp_cdc_change_job..

Pour obtenir plus d'informations sur les tâches CDC, vous pouvez interroger les vues de gestion dynamiques suivantes :

- sys.dm_cdc_errors
- sys.dm_cdc_log_scan_sessions
- sysjobs
- sysjobhistory

Capture de données modifiées (CDC) pour les instances multi-AZ

Si vous utilisez CDC sur une instance multi-AZ, assurez-vous que la configuration de la tâche CDC du miroir correspond à celle du mandataire. Les tâches CDC sont mappées au `database_id`. Si les ID de base de données du réplica secondaire sont différents de ceux du mandataire, les tâches ne seront pas associées à la base de données appropriée. Pour éviter toute erreur après le basculement, RDS supprimer et recrée les tâches sur le nouveau mandataire. Les tâches recréées utilisent les paramètres que le mandataire a enregistrés avant le basculement.

Même si ce processus s'exécute rapidement, il est toujours possible que les tâches CDC puissent s'exécuter avant que RDS puisse les corriger. Voici trois moyens de contraindre les paramètres à être cohérents entre les réplicas principaux et secondaires :

- Utilisez les mêmes paramètres de tâche pour toutes les bases de données pour lesquelles CDC est activé.
- Avant de modifier la configuration des tâches CDC, convertissez l'instance multi-AZ en mono-AZ.
- Transférez manuellement les paramètres chaque fois que vous les modifiez sur le principal.

Pour afficher et définir les paramètres CDC utilisés pour recréer les tâches CDC après un basculement, utilisez `rds_show_configuration` et `rds_set_configuration`.

L'exemple suivant renvoie la valeur définie pour cdc_capture_maxtrans. Pour tout paramètre défini sur RDS_DEFAULT, RDS configure automatiquement la valeur.

```
-- Show configuration for each parameter on either primary and secondary replicas.
```

```
exec rdsadmin.dbo.rds_show_configuration 'cdc_capture_maxtrans'
```

Pour définir la configuration sur le réplica secondaire, exécutez `rdsadmin.dbo.rds_set_configuration`. Cette procédure définit les valeurs de paramètre pour toutes les bases de données du serveur secondaire. Ces paramètres ne sont utilisés qu'après un basculement. L'exemple suivant définit le `maxtrans` de toutes les tâches de capture CDC sur *1000* :

```
--To set values on secondary. These are used after failover.
exec rdsadmin..rds_set_configuration 'cdc_capture_maxtrans' , 1000
```

Pour définir les paramètres de tâche CDC sur le principal, utilisez plutôt sys.sp_cdc_change_job.

Utilisation de SQL Server Agent

Avec Amazon RDS, vous pouvez utiliser SQL Server Agent sur une instance de base de données exécutant Microsoft SQL Server Standard, Web Edition ou Enterprise Edition. SQL Server Agent est un service Microsoft Windows qui exécute des tâches administratives planifiées, appelées travaux. Vous pouvez utiliser SQL Server Agent pour exécuter les travaux T-SQL jobs afin de reconstruire les index, d'exécuter les contrôles de corruption et de regrouper les données dans une instance de base de données SQL Server.

SQL Server Agent peut exécuter un travail en fonction d'une planification, en réponse à un événement spécifique, ou à la demande. Pour plus d'informations, consultez SQL Server Agent dans la documentation SQL Server. Vous devez éviter de planifier l'exécution de travaux pendant les fenêtres de maintenance et de sauvegarde pour votre instance de base de données, parce que ces processus de maintenance et de sauvegarde qui sont lancés par AWS pourraient interrompre le travail ou entraîner son annulation. Comme Amazon RDS sauvegarde votre instance de base de données, vous n'utilisez pas SQL Server Agent pour créer des sauvegardes.

Pour afficher l'historique d'un travail SQL Server Agent dans SQL Server Management Studio, vous ouvrez l'Explorateur d'objet, cliquez avec le bouton droit sur le travail, puis cliquez sur Afficher l'historique.

Comme SQL Server Agent s'exécute sur un hôte géré dans une instance de base de données, certaines actions ne sont pas prises en charge. L'exécution de travaux de réplication et de scripts de ligne de commande à l'aide d'ActiveX, du shell de commande Windows ou de Windows PowerShell n'est pas prise en charge. De plus, vous ne pouvez pas démarrer, arrêter ou redémarrer manuellement SQL Server Agent parce que son fonctionnement est géré par l'hôte. Les notifications par e-mail via SQL Server Agent ne sont pas disponibles à partir d'une instance de base de données.

Lorsque vous créez une instance de base de données SQL Server, le nom d'utilisateur maître est inscrit dans le rôle SQLAgentUserRole. Pour ajouter un utilisateur/une connexion supplémentaire afin d'utiliser SQL Server Agent, vous devez vous connecter comme utilisateur maître et exécuter les actions suivantes.

1. Créez une autre connexion de niveau serveur à l'aide de la commande `CREATE LOGIN`.
2. Créez un utilisateur dans msdb avec la commande `CREATE USER`, puis liez cet utilisateur à la connexion que vous avez créée à l'étape précédente.
3. Ajoutez l'utilisateur au rôle SQLAgentUserRole avec la procédure stockée système `sp_addrolemember`.

Par exemple, supposons que votre identifiant principal soit **`admin`** et que vous souhaitez accorder l'accès à SQL Server Agent à un utilisateur nommé **`theirname`** avec le mot de passe **`theirpassword`**. Vous vous connectez à l'aide du nom d'utilisateur maître et exécutez les commandes suivantes.

```
--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];
```

Pour supprimer un travail SQL Server Agent, exécutez l'instruction T-SQL suivante.

```
EXEC msdb..sp_delete_job @job_name = 'job_name';
```

Note

N'utilisez pas l'interface utilisateur dans SQL Server Management Console (SSMS) pour supprimer un travail SQL Server Agent. Si vous le faites, vous obtenez un message d'erreur similaire au suivant :

```
The EXECUTE permission was denied on the object 'xp_regread', database
 'mssqlsystemresource', schema 'sys'.
```

Cette erreur survient parce que, en tant que service managé, RDS est empêché d'exécuter les procédures qui accèdent au registre Windows. Lorsque vous utilisez SSMS pour supprimer la tâche, celui-ci essaie d'exécuter un processus (`xp_regread`) que RDS n'est pas autorisé à employer.

Utilisation des journaux Microsoft SQL Server

Vous pouvez utiliser la console Amazon RDS pour afficher, consulter et télécharger les journaux SQL Server Agent et les journaux d'erreurs Microsoft SQL Server.

Consultation des fichiers journaux

Si vous affichez un journal dans la console Amazon RDS, vous pouvez voir son contenu tel qu'il est à ce moment-là. L'observation d'un journal dans la console l'ouvre dans un état dynamique de telle sorte que vous puissiez voir ses mises à jour pratiquement en temps réel.

Seul le dernier journal est actif pour pouvoir être observé. Par exemple, supposons que les journaux affichent les informations suivantes :

Name	Last Written	Size			
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

Seul log/ERROR, comme le journal le plus récent est en mise à jour active. Vous pouvez choisir d'en observer d'autres, mais ils sont statiques et ne sont pas mis à jour.

Archivage des fichiers journaux

La console Amazon RDS affiche les journaux de la semaine écoulée jusqu'au même. Vous pouvez télécharger et archiver les journaux pour les garder comme référence au-delà de cette date. Une solution

pour archiver les journaux consiste à les charger dans un compartimentAmazon S3. Pour savoir comment configurer un compartiment Amazon S3 et comment charger un fichier, consultez Bases Amazon S3 dans le Guide de démarrage Amazon Simple Storage Service, puis cliquez sur Mise en route.

Affichage des journaux des erreurs et des agents

Pour consulter les journaux des erreurs et de l'agent Microsoft SQL Server, utilisez la procédure stockée Amazon RDS `rds_read_error_log` avec les paramètres suivants :

- **`@index`** – version du journal à récupérer. La valeur par défaut est 0, qui permet de récupérer le journal des erreurs actuel. Spécifiez 1 pour récupérer le journal précédent, spécifiez 2 pour récupérer celui d'avant, et ainsi de suite.
- **`@type`** – type de journal à récupérer. Spécifiez 1 pour récupérer un journal des erreurs. Spécifiez 2 pour récupérer un journal de l'agent.

Example

L'exemple suivant demande le journal des erreurs actuel.

```
EXEC rdsadmin.dbo.rds_read_error_log @index = 0, @type = 1;
```

Utilisation des fichiers de trace et de vidage

Cette section décrit l'utilisation des fichiers de trace et des fichiers de vidage pour vos instances de base de données Amazon RDS exécutant Microsoft SQL Server.

Génération d'une requête de trace SQL

```
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
```

Affichage d'une trace ouverte

```
select * from ::fn_trace_getinfo(default)
```

Affichage du contenu d'une trace

```
select * from ::fn_trace_gettable('D:\rdsdbdata\log\rdstest.trc', default)
```

Configuration de la période de rétention pour les fichiers de trace et de vidage

Les fichiers de trace et de vidage peuvent s'accumuler et consommer de l'espace sur le disque. Par défaut, Amazon RDS purge les fichiers de trace et de vidage de plus de sept jours.

Pour consulter la période actuelle de rétention des fichiers de trace et de vidage, utilisez la procédure `rds_show_configuration`, comme illustré dans l'exemple suivant.

```
exec rdsadmin..rds_show_configuration;
```

Pour modifier la période de rétention des fichiers de trace, utilisez la procédure `rds_set_configuration` et définissez `tracefile retention` en minutes. L'exemple ci-dessous définit la période de rétention des fichiers de trace à 24 heures.

```
exec rdsadmin..rds_set_configuration 'tracefile retention', 1440;
```

Pour modifier la période de rétention des fichiers de vidage, utilisez la procédure `rds_set_configuration` et définissez `dumpfile retention` en minutes. L'exemple ci-dessous définit la période de rétention des fichiers de vidage à 3 jours.

```
exec rdsadmin..rds_set_configuration 'dumpfile retention', 4320;
```

Pour des raisons de sécurité, vous ne pouvez pas supprimer un fichier de trace ou de vidage spécifique sur une instance de base de données SQL Server. Pour supprimer tous les fichiers de trace ou de vidage inutilisés, définissez la période de rétention des fichiers à 0.

MySQL sur Amazon RDS

Amazon RDS prend en charge les instances de base de données qui exécutent plusieurs versions de MySQL. Vous pouvez utiliser les versions majeures suivantes :

- MySQL 8.0
- MySQL 5.7
- MySQL 5.6
- MySQL 5.5

Pour plus d'informations sur la prise en charge des versions mineures, consultez Versions de MySQL sur Amazon RDS (p. 782).

Vous utilisez d'abord les interfaces ou les outils de gestion Amazon RDS pour créer une instance de base de données MySQL Amazon RDS. Vous pouvez ensuite redimensionner l'instance de base de données, autoriser les connexions à l'instance de base de données, créer et restaurer à partir de sauvegardes ou d'instantanés, créer des secondaires multi-AZ, créer des réplicas en lecture et superviser les performances de l'instance de base de données. Vous utilisez les applications et les utilitaires MySQL standard pour stocker les données de l'instance de base de données et y accéder.

Amazon RDS pour MySQL est conforme à de nombreuses normes du secteur. Par exemple, vous pouvez utiliser Amazon RDS pour les bases de données MySQL afin de créer des applications conformes à HIPAA et de stocker des informations liées à la santé, y compris des informations de santé protégées (PHI, Protected Health Information) dans le cadre d'un accord de partenariat (AAA) avec AWS. Amazon RDS pour MySQL satisfait également les exigences de sécurité du Programme de gestion de risque et d'autorisation fédérale (FedRAMP) et a reçu une autorisation provisoire P-ATO du conseil d'autorisation commun du FedRAMP au niveau de la base de références FedRAMP HIGH au sein de la région AWS GovCloud (USA Ouest). Pour de plus amples informations sur les normes de conformité prises en charge, veuillez consulter Conformité du Cloud AWS.

Pour plus d'informations sur les fonctions de chaque version MySQL, consultez The Main Features of MySQL dans la documentation MySQL.

Tâches courantes de gestion pour MySQL sur Amazon RDS

Vous trouverez ci-dessous les tâches courantes de gestion que vous exécutez avec une instance de base de données Amazon RDS MySQL, avec des liens vers la documentation appropriée relative à chaque tâche.

Type de tâche	Documentation
Comprendre Amazon RDS Comprendre les principaux composants d'Amazon RDS, y compris les instances de base de données, les régions AWS, les zones de disponibilité, les groupes de sécurité, les groupes de paramètres et les groupes d'options.	Qu'est-ce que Amazon Relational Database Service (Amazon RDS) ? (p. 1)

Type de tâche	Documentation
Configuration d'Amazon RDS pour la première utilisation Configurez Amazon RDS de sorte à pouvoir créer des instances de bases de données MySQL dans Amazon Web Services (AWS).	Configuration pour Amazon RDS (p. 62)
Présentation des instances de bases de données d'Amazon RDS Créez des instances de serveur MySQL virtuelles qui s'exécutent dans AWS. Étant donné que les instances de bases de données sont les blocs de construction d'Amazon RDS, nous vous recommandons de bien comprendre leurs principes.	Instances de base de données Amazon RDS (p. 5)
Création d'une instance de base de données de production Créer une instance de base de données à des fins de production. Créer une instance implique de choisir une classe d'instance de base de données dotée d'une puissance de traitement et de capacités de mémoire appropriées, et de choisir un type de stockage qui prenne en charge la manière que vous envisagez d'utiliser votre base de données.	Classes d'instances de base de données (p. 6) Types de stockage Amazon RDS (p. 30) Création d'une instance de base de données Amazon RDS (p. 146)
Gestion de la sécurité de votre instance de base de données Par défaut, les instances de bases de données sont créées avec un pare-feu qui empêche d'y accéder. Vous devez créer un groupe de sécurité avec les adresses IP et la configuration réseau voulues pour accéder à l'instance de base de données. Vous pouvez également utiliser des stratégies AWS Identity and Access Management (IAM) pour attribuer des autorisations déterminant qui peut gérer les ressources RDS.	Sécurité dans Amazon RDS (p. 1518) Gestion de l'accès à l'aide de stratégies (p. 1539) Contrôle d'accès par groupe de sécurité (p. 1590) Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611)
Connexion à votre instance de base de données Connectez-vous à votre instance de base de données à l'aide d'une application client SQL standard telle que l'utilitaire de ligne de commande MySQL ou MySQL Workbench.	Connexion à une instance de base de données exécutant le moteur de base de données MySQL (p. 793)

Type de tâche	Documentation
Configuration d'une haute disponibilité pour une instance de base de données de production Assurez un haut niveau de disponibilité grâce à une réplication de secours synchrone dans une autre zone de disponibilité, au basculement automatique, à la tolérance aux pannes pour les instances de base de données à l'aide de déploiements multi-AZ et aux réplicas en lecture.	Haute disponibilité (multi-AZ) pour Amazon RDS (p. 43)
Configuration d'une instance de base de données dans un Amazon Virtual Private Cloud Configurez un Virtual Private Cloud (VPC) dans le service Amazon VPC. Un Amazon VPC est un réseau virtuel logiquement isolé des autres réseaux virtuels dans AWS.	Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611) Utilisation d'une instance de base de données dans un VPC (p. 1620)
Configuration de fonctionnalités et de paramètres de base de données MySQL spécifiques Configurez des paramètres de base de données MySQL spécifiques avec un groupe de paramètres pouvant être associé à plusieurs instances de bases de données. Vous pouvez également configurer des caractéristiques de base de données MySQL spécifiques avec un groupe d'options pouvant être associé à plusieurs instances de bases de données.	Utilisation de groupes de paramètres de base de données (p. 225) Utilisation de groupes d'options (p. 209) Options pour les instances de base de données MySQL (p. 873)
Modification d'une instance de base de données exécutant le moteur de base de données MySQL Modifiez les paramètres d'une instance de base de données pour accomplir des tâches telles que l'ajout de stockage supplémentaire ou la modification de la classe d'instance.	Modification d'une instance de base de données Amazon RDS (p. 243)
Configuration de la sauvegarde et de la restauration des bases de données Configurez la sauvegarde automatique de votre instance de base de données. Vous pouvez également sauvegarder et restaurer vos bases de données manuellement à l'aide de fichiers de sauvegarde complets.	Utilisation des sauvegardes (p. 317) Sauvegarde et restauration d'une instance de base de données Amazon RDS (p. 317)

Type de tâche	Documentation
Importation et exportation de données Importez des données d'autres instances de bases de données RDS MySQL, d'instances MySQL s'exécutant à l'extérieur d'Amazon RDS et d'autres types de sources de données et exportez les données vers des instances MySQL s'exécutant à l'extérieur d'Amazon RDS.	Restauration d'une sauvegarde dans une instance de base de données MySQL Amazon RDS (p. 821)
Surveillance d'une instance de base de données MySQL Surveillez votre instance de base de données RDS MySQL à l'aide de métriques RDS Amazon CloudWatch, d'événements et de Surveillance améliorée. Affichez des fichiers journaux pour votre instance de base de données RDS MySQL.	Surveillance d'une instance de base de données Amazon RDS (p. 373) Affichage des métriques d'instances de base de données (p. 384) Affichage d'événements Amazon RDS (p. 486) Amazon RDS Fichiers journaux de base de données (p. 490) Fichiers journaux de base de données MySQL (p. 506)
Réplication de vos données Créez un réplica en lecture MySQL, dans la même région AWS ou dans une région différente. Vous pouvez utiliser des réplicas en lecture pour l'équilibrage de charge, la reprise après sinistre et le traitement de charges de travail très intenses en lecture des bases de données, telles que l'analyse et la création de rapports.	Utilisation des réplicas en lecture (p. 275) Réplication avec une instance MySQL ou MariaDB s'exécutant à l'extérieur d'Amazon RDS (p. 863)

Vous pouvez également consulter plusieurs sections contenant des informations utiles sur l'utilisation des instances de base de données MySQL Amazon RDS :

- Tâches DBA courantes pour les instances de base de données MySQL (p. 881)
- Options pour les instances de base de données MySQL (p. 873)
- Référence SQL de MySQL sur Amazon RDS (p. 899)

Versions de MySQL sur Amazon RDS

Les numéros de versions de MySQL sont organisés selon la version = X.Y.Z. Dans la terminologie Amazon RDS, X.Y représente la version majeure et Z le numéro de la version mineure. Pour les implémentations Amazon RDS, un changement de version sera considéré majeur si le numéro de version majeure change—par exemple, en allant de la version 5.6 à 5.7. Un changement de version sera considéré mineur seulement si le numéro de version mineure change—par exemple, en allant de la version 5.7.16 à 5.7.21.

Amazon RDS prend actuellement en charge les versions suivantes de MySQL :

Version majeure	Version mineure
MySQL 8.0	• 8.0.21 • 8.0.20 • 8.0.19 • 8.0.17 • 8.0.16 • 8.0.15 • 8.0.13 • 8.0.11
MySQL 5.7	• 5.7.31 • 5.7.30 • 5.7.28 • 5.7.26 • 5.7.25 • 5.7.24 • 5.7.23 • 5.7.22 • 5.7.21 • 5.7.19 • 5.7.17 • 5.7.16
MySQL 5.6	• 5.6.48 • 5.6.46 • 5.6.44 • 5.6.43 • 5.6.41 • 5.6.40 • 5.6.39 • 5.6.37 • 5.6.35 • 5.6.34
MySQL 5.5	• 5.5.61 • 5.5.59 • 5.5.57 • 5.5.54 • 5.5.53 • 5.5.46

Vous pouvez spécifier n'importe quelle version MySQL actuellement prise en charge lorsque vous créez une instance de base de données. Vous pouvez spécifier la version majeure (par exemple MySQL 5.7), puis toute version mineure prise en charge pour la version majeure spécifiée. Si aucune version n'est spécifiée, Amazon RDS utilise par défaut une version prise en charge, généralement la plus récente. Si une version majeure est spécifiée, mais qu'une version mineure ne l'est pas, Amazon RDS utilise par défaut une version récente de la version majeure que vous avez spécifiée. Pour afficher la liste des versions

prises en charge, ainsi que celles par défaut pour des instances de base de données nouvellement créées, utilisez la commande `describe-db-engine-versions` de l'AWS CLI.

La version par défaut de MySQL peut varier selon la région AWS. Pour créer une instance de base de données avec une version mineure spécifique, spécifiez la version mineure lors de la création de l'instance de base de données. Vous pouvez déterminer la version secondaire par défaut d'une région AWS à l'aide de la commande AWS CLI suivante :

```
aws rds describe-db-engine-versions --default-only --engine mysql --engine-version major-
engine-version --region region --query "*[].{Engine:Engine,EngineVersion:EngineVersion}" --
output text
```

Remplacez *`major-engine-version`* par la version majeure du moteur et *`region`* par la région AWS. Par exemple, la commande AWS CLI suivante renvoie la version mineure du moteur MySQL par défaut pour la version majeure 5.7 et la région AWS USA Ouest (Oregon) (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
```

Avec Amazon RDS, vous contrôlez à quel moment vous mettez à niveau votre instance MySQL vers une nouvelle version majeure prise en charge par Amazon RDS. Vous pouvez maintenir la compatibilité avec des versions MySQL spécifiques, tester de nouvelles versions avec votre application avant le déploiement en production et effectuer des mises à niveau de versions majeures aux moments qui correspondent le mieux à votre calendrier.

Lorsque la mise à niveau automatique de versions mineures est activée, votre instance de base de données sera automatiquement mise à niveau vers de nouvelles versions mineures MySQL, celles-ci étant prises en charge par Amazon RDS. Ces correctifs sont appliqués pendant le créneau de maintenance planifié. Vous pouvez modifier une instance de base de données pour activer ou désactiver les mises à niveau automatiques des versions mineures.

Si vous refusez les mises à niveau automatiques planifiées, vous pouvez procéder manuellement à une mise à niveau vers une version mineure prise en charge en suivant la même procédure que pour une mise à jour de la version majeure. Pour plus d'informations, consultez Mise à niveau d'une version du moteur d'une instance de base de données (p. 267).

Amazon RDS prend actuellement en charge les mises à niveau de version majeure de la version 5.5 à 5.6 de MySQL, de la version 5.6 à 5.7 de MySQL et de la version 5.7 à la version 8.0. Étant donné que les mises à niveau de version majeures impliquent quelques risques de compatibilité, elles ne sont pas appliquées automatiquement et vous devez donc faire une demande de modification de l'instance de base de données. Vous devez tester soigneusement toute mise à niveau avant de procéder à la mise à niveau de vos instances de production. Pour plus d'informations sur la mise à niveau d'une instance de base de données MySQL, consultez Mise à niveau du moteur de base de données MySQL (p. 804).

Vous pouvez tester une instance de base de données par rapport à une nouvelle version avant la mise à niveau. Pour ce faire, créez un instantané de base de données de votre instance de base de données existante, restaurez à partir de l'instantané de base de données pour créer une instance de base de données et lancez une mise à niveau de version pour la nouvelle instance de base de données. Vous pouvez ensuite procéder en toute sécurité à une expérimentation sur le clone mis à niveau de votre instance de base de données avant de décider de mettre à niveau ou pas votre instance de base de données d'origine.

Pour de plus amples informations sur la stratégie d'obsolescence Amazon RDS pour MySQL, veuillez consulter FAQ Amazon RDS.

Fonctions MySQL non prises en charge par Amazon RDS

Amazon RDS ne prend pas en charge actuellement les fonctions MySQL suivantes :

- Plug-in d'authentification
- Erreur de journalisation dans le journal système
- Plug-in de réplication de groupe
- Chiffrement d'espace de tables InnoDB
- Plug-in d'audit MariaDB (non pris en charge pour la version Amazon RDS MySQL 8.0 uniquement)

  Le plug-in d'audit MariaDB est pris en charge pour les versions Amazon RDS 5.5, 5.6 et 5.7)
- Plug-in de niveau de sécurité du mot de passe
- Variables système persistantes
- Filtres de réplication
- Réplication semi-synchrone
- Espace de table transportable
- Plug-in X

> **Note**
>
> Les identifiants de transaction globaux sont pris en charge pour les versions MySQL 5.7.23 et les versions MySQL 5.7 ultérieures. Les identifiants de transaction globaux ne sont pas pris en charge pour les versions Amazon RDS MySQL 5.5, 5.6 ou 8.0.
> L'authentification de base de données IAM n'est pas prise en charge pour MySQL 5.6, 5.7 et 8.0.
> L'authentification de base de données IAM n'est pas prise en charge pour MySQL 5.5.
> Amazon RDS Performance Insights est pris en charge pour MySQL 5.6, 5.7 et 8.0. Amazon RDS Performance Insights n'est pas pris en charge pour MySQL 5.5.

Pour offrir une expérience de service géré, Amazon RDS ne fournit pas l'accès shell aux instances de base de données. Il restreint également l'accès à certaines tables et procédures système qui nécessitent des privilèges avancés. Amazon RDS prend en charge l'accès aux bases de données sur une instance de base de données en utilisant toute application client SQL standard. Amazon RDS ne permet pas d'accès d'hôte direct à une instance de base de données via Telnet, Secure Shell (SSH) ou une connexion Bureau à distance de Windows. Lorsque vous créez une instance de base de données, le rôle db_owner vous est attribué pour toutes les bases de données sur cette instance, et vous disposez de toutes les autorisations au niveau de la base de données, sauf celles qui sont utilisées pour les sauvegardes. Amazon RDS gère les sauvegardes pour vous.

Moteurs de stockage pris en charge pour MySQL sur Amazon RDS

Bien que MySQL prend en charge plusieurs moteurs de stockage avec diverses capacités, ceux-ci ne sont pas tous optimisés pour la récupération et la durabilité des données. Amazon RDS prend entièrement en charge le moteur de stockage InnoDB pour les instances de base de données MySQL. Les fonctions Amazon RDS telles que la restauration Point-In-Time et la restauration d'instantané nécessitent un moteur de stockage récupérable et sont pris en charge pour le moteur de stockage InnoDB uniquement. Vous devez exécuter une instance de MySQL 5.6, ou version ultérieure, pour utiliser l'interface `memcached` InnoDB. Pour plus d'informations, consultez Prise en charge memcached MySQL (p. 877).

Le Federated Storage Engine n'est pour l'instant pas pris en charge par Amazon RDS pour MySQL.

Pour les schémas créés par l'utilisateur, le moteur de stockage MyISAM ne prend pas en charge une récupération fiable et peut causer la perte ou la corruption des données quand MySQL est redémarré après une récupération, empêchant la restauration à un instant dans le passé et la restauration d'instantané de fonctionner comme prévu. Néanmoins, si vous choisissez tout de même d'utiliser MyISAM avec Amazon RDS, les instantanés peuvent être utiles dans certaines conditions.

> Note
>
> Les tables système du schéma `mysql` peuvent être dans le stockage MyISAM.

Si vous souhaitez convertir des tables MyISAM existantes en tables InnoDB, vous pouvez utiliser la commande `ALTER TABLE` (par exemple, `alter table TABLE_NAME engine=innodb;`). N'oubliez pas que MyISAM et InnoDB ont des forces et des faiblesses différentes, vous devriez donc commencer par évaluer de façon exhaustive l'impact de ce basculement sur vos applications.

MySQL 5.1 n'est plus pris en charge dans Amazon RDS. Cependant, vous pouvez restaurer des instantanés MySQL 5.1 existants. Lorsque vous restaurez un instantané MySQL 5.1, l'instance est automatiquement mise à niveau vers MySQL 5.5.

MySQL Security sur Amazon RDS

La sécurité des instances de bases de données Amazon RDS MySQL est gérée à trois niveaux :

- AWS Identity and Access Management contrôle les personnes autorisées à exécuter des actions de gestion Amazon RDS sur les instances de base de données. Lorsque vous vous connectez à AWS à l'aide des informations d'identification IAM, votre compte IAM doit disposer des stratégies IAM qui accordent les autorisations requises pour exécuter les opérations de gestion Amazon RDS. Pour plus d'informations, consultez Identity and Access Management dans Amazon RDS (p. 1536).
- Lorsque vous créez une instance de base de données, vous utilisez un groupe de sécurité VPC ou un groupe de sécurité DB pour contrôler les appareils et les instances Amazon EC2 qui peuvent ouvrir des connexions au point de terminaison et au port de l'instance de base de données. Ces connexions peuvent être effectuées à l'aide du protocole SSL (Secure Socket Layer). En outre, les règles de pare-feu de votre entreprise peuvent contrôler si les appareils en cours d'exécution dans votre entreprise peuvent ouvrir des connexions à l'instance de base de données.
- Pour authentifier la connexion et les autorisations d'une instance de base de données MySQL, vous pouvez adopter l'une des approches suivantes, ou les combiner.

  Vous pouvez adopter la même approche qu'avec une instance autonome de MySQL. Les commandes telles que `CREATE USER`, `RENAME USER`, `GRANT`, `REVOKE` et `SET PASSWORD` fonctionnent de la même façon que dans les bases de données sur site, comme le fait la modification directe des tables du schéma de base de données. Pour de plus amples informations, veuillez consulter Access Control and Account Management dans la documentation MySQL.

  Vous pouvez également utiliser l'authentification de base de données IAM. L'authentification de base de données IAM vous permet de vous authentifier sur votre instance de base de données à l'aide d'un utilisateur IAM ou d'un rôle IAM et d'un jeton d'authentification. Un jeton d'authentification est une valeur unique qui est générée à l'aide du processus de signature Signature Version 4. L'authentification de base de données IAM vous permet d'utiliser les mêmes informations d'identification pour contrôler l'accès à vos ressources AWS et à vos bases de données. Pour plus d'informations, consultez Authentification de base de données IAM pour MySQL et PostgreSQL (p. 1554).

Lorsque vous créez une instance de base de données Amazon RDS, l'utilisateur principal a les privilèges par défaut suivants :

- `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 (MySQL 5.6 and later)`
- `select`
- `show databases`
- `show view`
- `trigger`
- `update`

> **Note**
>
> Bien qu'il soit possible de supprimer l'utilisateur maître sur l'instance de base de données, il n'est pas recommandé de le faire. Pour recréer l'utilisateur maître, utilisez l'opération d'API RDS ModifyDBInstance ou la commande d'AWS CLI modify-db-instance et spécifiez un nouveau mot de passe d'identifiant principal avec le paramètre approprié. Si l'utilisateur maître n'existe pas dans l'instance, il est créé avec le mot de passe spécifié.

Pour fournir des services de gestion à chaque instance de base de données, l'utilisateur `rdsadmin` est créé lors de la création de l'instance de base de données. Les tentatives de supprimer, renommer et modifier le mot de passe du compte `rdsadmin`, ou d'en modifier les privilèges, génèrent une erreur.

Pour autoriser la gestion de l'instance de base de données, les commandes standard `kill` et `kill_query` ont fait l'objet de restrictions. Les commandes Amazon RDS `rds_kill` et `rds_kill_query` sont fournies pour vous permettre de mettre fin aux requêtes ou aux sessions utilisateur sur les instances de base de données.

Utilisation du plug-in de validation de mot de passe

MySQL fournit le plug-in `validate_password` pour assurer une sécurité améliorée. Le plug-in applique des stratégies de mot de passe à l'aide de paramètres du groupe de paramètres de base de données

pour votre instance de base de données MySQL. Le plug-in est pris en charge pour les instances de base de données exécutant MySQL version 5.6, 5.7 et 8.0. Pour de plus amples informations sur le plug-in `validate_password`, veuillez consulter Plug-in de validation de mot de passe dans la documentation MySQL.

Pour activer le plug-in validate_password pour une instance de base de données MySQL

1. Connectez-vous à votre instance de base de données MySQL et exécutez la commande suivante.

```
INSTALL PLUGIN validate_password SONAME 'validate_password.so';
```

2. Configurez les paramètres du plug-in dans le groupe de paramètres de base de données utilisé par l'instance de base de données.

   Pour de plus amples informations sur les paramètres, veuillez consulter Password Validation Plugin Options and Variables dans la documentation MySQL.

   Pour plus d'informations sur la modification des paramètres d'instance de base de données, consultez Modification de paramètres dans un groupe de paramètres de bases de données (p. 229).

Après avoir installé et activé le plug-in `password_validate`, réinitialisez les mots de passe existants conformément à vos nouvelles stratégies de validation.

Amazon RDS ne valide pas les mots de passe. L'instance de base de données MySQL DB effectue la validation de mot de passe. Si vous définissez un mot de passe utilisateur avec l'AWS Management Console, la commande d'AWS CLI `modify-db-instance` ou l'action d'API RDS `ModifyDBInstance`, la modification peut aboutir même si le nouveau mot de passe ne répond pas à vos stratégies de mot de passe. Cependant, un nouveau mot de passe est défini dans l'instance de base de données MySQL uniquement s'il satisfait les stratégies de mot de passe. Dans ce cas, Amazon RDS enregistre l'événement suivant.

```
"RDS-EVENT-0067" - An attempt to reset the master password for the DB instance has failed.
```

Pour plus d'informations sur les événements Amazon RDS, consultez Utilisation de la notification d'événement Amazon RDS (p. 467)

Utilisation de SSL avec une instance de base de données MySQL

Amazon RDS prend en charge les connexions SSL avec les instances de base de données exécutant le moteur de base de données MySQL.

Amazon RDS crée un certificat SSL et l'installe sur l'instance de base de données quand Amazon RDS alloue l'instance. Ces certificats sont signés par une autorité de certification. Le certificat SSL inclut le point de terminaison de l'instance de base de données en tant que nom commun du certificat SSL pour assurer une protection contre les attaques par usurpation.

Un certificat SSL créé par Amazon RDS est l'entité racine approuvée et doit fonctionner dans la plupart des cas, mais il peut échouer si votre application n'accepte pas les chaînes de certificats. Si votre application

n'accepte pas les chaînes de certificats, vous devrez peut-être utiliser un certificat intermédiaire pour vous connecter à votre région AWS. Par exemple, vous devez utiliser un certificat intermédiaire pour vous connecter à la région AWS GovCloud (USA Ouest) à l'aide de SSL.

Pour de plus amples informations sur le téléchargement de certificats, veuillez consulter Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525). Pour en savoir plus sur l'utilisation de SSL avec MySQL, consultez Mise à jour des applications pour se connecter aux instances de bases de données MySQL à l'aide des nouveaux certificats SSL/TLS (p. 799).

MySQL utilise yaSSL pour les connexions sécurisées dans les versions suivantes :

- MySQL version 5.7.19 et versions 5.7 antérieures
- MySQL version 5.6.37 et versions 5.6 antérieures
- MySQL version 5.5.57 et versions 5.5 antérieures

MySQL utilise OpenSSL pour les connexions sécurisées dans les versions suivantes :

- MySQL version 8.0
- MySQL version 5.7.21 et versions 5.7 ultérieures
- MySQL version 5.6.39 et versions 5.6 ultérieures
- MySQL version 5.5.59 et versions 5.5 ultérieures

Amazon RDS pour MySQL prend en charge les versions 1.0, 1.1 et 1.2 du protocole TLS (Transport Layer Security). Le tableau suivant affiche la prise en charge du protocole TLS pour les versions MySQL.

Version MySQL	TLS 1.0	TLS 1.1	TLS 1.2
MySQL 8.0	Pris en charge	Pris en charge	Pris en charge
MySQL 5.7	Pris en charge	Pris en charge	Pris en charge pour MySQL 5.7.21 et versions ultérieures
MySQL 5.6	Pris en charge	Pris en charge pour MySQL 5.6.46 et versions ultérieures	Pris en charge pour MySQL 5.6.46 et versions ultérieures
MySQL 5.5	Pris en charge	Non pris en charge	Non pris en charge

Pour chiffrer les connexions à l'aide du client `mysql` par défaut, lancez le client mysql à l'aide du paramètre `--ssl-ca` pour référencer la clé publique, comme illustré dans l'exemple suivant.

L'exemple suivant montre comment lancer le client à l'aide du paramètre `--ssl-ca` pour MySQL 5.7 ou version ultérieure.

```
mysql -h myinstance.c9akciq32.rds-us-east-1.amazonaws.com
--ssl-ca=[full path]rds-combined-ca-bundle.pem --ssl-mode=VERIFY_IDENTITY
```

L'exemple suivant montre comment lancer le client à l'aide du paramètre `--ssl-ca` pour MySQL 5.6 ou version antérieure.

```
mysql -h myinstance.c9akciq32.rds-us-east-1.amazonaws.com
--ssl-ca=[full path]rds-combined-ca-bundle.pem --ssl-verify-server-cert
```

Vous pouvez exiger des connexions SSL pour des comptes d'utilisateur spécifiques. Par exemple, vous pouvez utiliser l'une des instructions suivantes, selon votre version MySQL, pour exiger des connexions SSL sur le compte utilisateur `encrypted_user`.

Pour MySQL 5.7 et les versions ultérieures, utilisez la déclaration suivante.

```
ALTER USER 'encrypted_user'@'%' REQUIRE SSL;
```

Pour MySQL 5.6 et les versions antérieures, utilisez la déclaration suivante.

```
GRANT USAGE ON *.* TO 'encrypted_user'@'%' REQUIRE SSL;
```

Pour de plus amples informations sur les connexions SSL avec MySQL, veuillez consulter la section sur l'utilisation de connexions chiffrées dans la documentation MySQL.

Utilisation de memcached et d'autres options avec MySQL

La plupart des moteurs de base de données Amazon RDS prennent en charge des groupes d'options qui vous permettent de sélectionner des fonctions supplémentaires pour votre instance de base de données. Les instances de bases de données sur MySQL version 5.6 et versions ultérieures prennent en charge l'option `memcached`, un cache simple basée sur les clés. Pour plus d'informations sur `memcached` et d'autres options, consultez Options pour les instances de base de données MySQL (p. 873). Pour plus d'informations sur l'utilisation de groupes d'options, consultez Utilisation de groupes d'options (p. 209).

Préparation du cache InnoDB

La préparation du cache InnoDB peut fournir des gains de performances pour votre instance de base de données MySQL en enregistrant l'état actuel du pool de mémoires tampons lorsque l'instance de base de données est arrêtée, puis en rechargeant le pool de mémoires tampons à partir des informations enregistrées au démarrage de l'instance de base de données. Cette approche contourne la nécessité de « préparer » le pool de mémoires tampons à partir d'une utilisation normale de la base de données et précharge à la place le pool de mémoires tampons avec les pages des requêtes courantes connues. Le fichier qui stocke les informations du pool de tampons enregistré stocke uniquement les métadonnées pour les pages qui sont dans le pool de mémoires tampons et pas les pages elles-mêmes. Par conséquent, le fichier ne nécessite pas un important espace de stockage. La taille du fichier représente environ 0,2 pour cent de la taille du cache. Par exemple, pour un cache 64 Gio, la taille du fichier de préparation de cache est de 128 Mio. Pour de plus amples informations sur la préparation du cache InnoDB, veuillez consulter Saving and Restoring the Buffer Pool State dans la documentation MySQL.

MySQL sur Amazon RDS prend en charge la préparation de cache InnoDB pour MySQL version 5.6 et ultérieure. Pour activer la préparation du cache InnoDB, définissez les paramètres `innodb_buffer_pool_dump_at_shutdown` et `innodb_buffer_pool_load_at_startup` avec la valeur 1 dans le groupe de paramètres de votre instance de base de données. La modification de ces valeurs dans un groupe de paramètres affecte toutes les instances de bases de données MySQL qui utilisent ce groupe de paramètres. Pour activer la préparation du cache InnoDB pour des instances de bases de données MySQL spécifiques, vous devrez peut-être créer un groupe de paramètres pour ces instances. Pour plus d'informations sur les groupes de paramètres, consultez Utilisation de groupes de paramètres de base de données (p. 225).

La préparation du cache InnoDB fournit principalement une amélioration des performances pour les instances de bases de données qui utilisent le stockage standard. Si vous utilisez le stockage PIOPS, vous ne constatez généralement pas d'amélioration significative des performances.

> **Important**
>
> Si votre instance de base de données MySQL ne se ferme pas normalement, comme lors d'un basculement, l'état du pool de mémoires tampons n'est pas enregistré sur le disque. Dans ce cas, MySQL charge n'importe quel fichier du pool de mémoires tampons disponible au redémarrage de l'instance de base de données. Il n'en résulte aucun dommage, mais le pool de tampons restauré peut ne pas refléter l'état le plus récent du pool de tampons avant le redémarrage. Pour vous assurer d'avoir un état récent du pool de mémoires tampons disponible afin de préparer le cache InnoDB au démarrage, il est recommandé que vous vidiez régulièrement le pool de mémoires tampons « à la demande ». Vous pouvez vider ou charger le pool de mémoires tampons à la demande si votre instance de base de données exécute MySQL version 5.6.19 ou ultérieure.
> Vous pouvez créer un événement pour vider le pool de mémoires tampons automatiquement et à intervalles réguliers. Par exemple, l'instruction suivante crée un événement nommé `periodic_buffer_pool_dump` qui vide le pool de mémoires tampons toutes les heures.
>
> ```
> CREATE EVENT periodic_buffer_pool_dump
> ON SCHEDULE EVERY 1 HOUR
> DO CALL mysql.rds_innodb_buffer_pool_dump_now();
> ```
>
> Pour de plus amples informations sur les événements MySQL, veuillez consulter Syntaxe d'événement dans la documentation MySQL.

Vidage et chargement du pool de tampons à la demande

Pour MySQL version 5.6.19 et ultérieure, vous pouvez enregistrer et charger le cache InnoDB « à la demande ».

- Pour vider l'état actuel du pool de mémoires tampons sur le disque, appelez la procédure stockée mysql.rds_innodb_buffer_pool_dump_now (p. 920).
- Pour charger l'état enregistré du pool de mémoires tampons à partir du disque, appelez la procédure stockée mysql.rds_innodb_buffer_pool_load_now (p. 920).
- Pour annuler une opération de chargement en cours, appelez la procédure stockée mysql.rds_innodb_buffer_pool_load_abort (p. 920).

Fuseau horaire local pour les instances de bases de données MySQL

Par défaut, le fuseau horaire d'une instance de base de données MySQL RDS est le fuseau UTC (temps universel). Vous pouvez à la place définir le fuseau horaire de votre instance de base de données sur le fuseau horaire local de votre application.

Pour définir le fuseau horaire local d'une instance de base de données, définissez le paramètre `time_zone` du groupe de paramètres de votre instance de base de données avec l'une des valeurs prises en charge et répertoriées plus bas dans cette section. Lorsque vous définissez le paramètre `time_zone` d'un groupe de paramètres, toutes les instances de base de données et tous les réplicas en lecture qui ont recours à ce groupe de paramètres sont modifiés de façon à utiliser le nouveau

fuseau horaire local. Pour plus d'informations sur la définition des paramètres d'un groupe de paramètres, consultez Utilisation de groupes de paramètres de base de données (p. 225).

Une fois que vous avez défini le fuseau horaire local, toutes les nouvelles connexions à la base de données reflètent la modification. Si des connexions à votre base de données sont ouvertes lorsque vous modifiez le fuseau horaire local, la mise à jour du fuseau horaire local n'apparaît pas tant que vous n'avez pas fermé la connexion et n'en avez pas ouvert une nouvelle.

Vous pouvez définir un fuseau horaire local différent pour une instance de base de données et un ou plusieurs de ses réplicas en lecture. Pour ce faire, utilisez un autre groupe de paramètres pour l'instance de base de données et les réplicas, et définissez le paramètre `time_zone` de chaque groupe de paramètres avec un autre fuseau horaire local.

Si la réplication s'effectue entre les régions AWS, l'instance de base de données source et le réplica en lecture utilisent des groupes de paramètres différents (les groupes de paramètres sont propres à chaque région AWS). Pour que chaque instance utilise le même fuseau horaire local, vous devez définir le paramètre `time_zone` dans les groupes de paramètres de l'instance et du réplica en lecture.

Lorsque vous restaurez une instance de base de données à partir d'un instantané de base de données, le fuseau horaire local a la valeur UTC. Vous pouvez mettre à jour le fuseau horaire sur votre fuseau horaire local une fois la restauration terminée. Si vous restaurez une instance de base de données à un instant dans le passé, le fuseau horaire local de l'instance de base de données restaurée est le paramètre de fuseau horaire du groupe de paramètres de l'instance de base de données restaurée.

Vous pouvez définir votre fuseau horaire local avec l'une des valeurs suivantes.

`Africa/Cairo`	`Asia/Bangkok`	`Australia/Darwin`
`Africa/Casablanca`	`Asia/Beirut`	`Australia/Hobart`
`Africa/Harare`	`Asia/Calcutta`	`Australia/Perth`
`Africa/Monrovia`	`Asia/Damascus`	`Australia/Sydney`
`Africa/Nairobi`	`Asia/Dhaka`	`Brazil/East`
`Africa/Tripoli`	`Asia/Irkutsk`	`Canada/Newfoundland`
`Africa/Windhoek`	`Asia/Jerusalem`	`Canada/Saskatchewan`
`America/Araguaina`	`Asia/Kabul`	`Europe/Amsterdam`
`America/Asuncion`	`Asia/Karachi`	`Europe/Athens`
`America/Bogota`	`Asia/Kathmandu`	`Europe/Dublin`
`America/Caracas`	`Asia/Krasnoyarsk`	`Europe/Helsinki`
`America/Chihuahua`	`Asia/Magadan`	`Europe/Istanbul`
`America/Cuiaba`	`Asia/Muscat`	`Europe/Kaliningrad`
`America/Denver`	`Asia/Novosibirsk`	`Europe/Moscow`
`America/Fortaleza`	`Asia/Riyadh`	`Europe/Paris`
`America/Guatemala`	`Asia/Seoul`	`Europe/Prague`
`America/Halifax`	`Asia/Shanghai`	`Europe/Sarajevo`
`America/Manaus`	`Asia/Singapore`	`Pacific/Auckland`

America/Matamoros	Asia/Taipei	Pacific/Fiji
America/Monterrey	Asia/Tehran	Pacific/Guam
America/Montevideo	Asia/Tokyo	Pacific/Honolulu
America/Phoenix	Asia/Ulaanbaatar	Pacific/Samoa
America/Santiago	Asia/Vladivostok	US/Alaska
America/Tijuana	Asia/Yakutsk	US/Central
Asia/Amman	Asia/Yerevan	US/Eastern
Asia/Ashgabat	Atlantic/Azores	US/East-Indiana
Asia/Baghdad	Australia/Adelaide	US/Pacific
Asia/Baku	Australia/Brisbane	UTC

Limites et problèmes connus pour MySQL sur Amazon RDS

Il existe des limites et des problèmes connus liés à l'utilisation de MySQL sur Amazon RDS. Pour plus d'informations, consultez Limites et problèmes connus pour MySQL sur Amazon RDS (p. 896).

Connexion à une instance de base de données exécutant le moteur de base de données MySQL

Avant de vous connecter à une instance de base de données qui exécute le moteur de base de données MySQL, vous devez créer une instance de base de données. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146). Après qu'Amazon RDS a provisionné votre instance de base de données, vous pouvez utiliser n'importe quelle application cliente MySQL standard pour vous connecter à l'instance. Dans la chaîne de connexion, vous spécifiez l'adresse DNS du point de terminaison de l'instance de base de données comme paramètre de l'hôte, et le numéro de port du point de terminaison de l'instance de base de données comme paramètre du port.

Pour vous authentifier sur votre instance de base de données RDS, vous pouvez utiliser l'une des méthodes d'authentification pour MySQL et l'authentification de base de données IAM.

- Pour en savoir plus sur l'authentification sur MySQL à l'aide de l'une des méthodes d'authentification pour MySQL, consultez Méthode d'authentification dans la documentation MySQL.
- Pour en savoir plus sur l'authentification sur MySQL à l'aide de l'authentification de base de données IAM, consultez Authentification de base de données IAM pour MySQL et PostgreSQL (p. 1554).

Vous pouvez utiliser la AWS Management Console, la commande describe-db-instances de l'interface AWS CLI ou l'opération d'API Amazon RDS DescribeDBInstances pour répertorier les détails d'une instance de base de données Amazon RDS, notamment son point de terminaison.

Pour rechercher le point de terminaison d'une instance de base de données MySQL dans la AWS Management Console :

1. Ouvrez la console RDS et choisissez Bases de données pour afficher une liste de vos instances de bases de données.
2. Choisissez le nom de l'instance de base de données MySQL pour afficher ses détails.
3. Dans l'onglet Connectivity & security (Connectivité et sécurité), copiez le point de terminaison. Notez également le numéro du port. Vous avez besoin du point de terminaison et du numéro de port pour vous connecter à l'instance de base de données.

Si la valeur d'un point de terminaison est `mysql-instance1.123456789012.us-east-1.rds.amazonaws.com` et que la valeur de port est `3306`, vous spécifiez les valeurs suivantes dans une chaîne de connexion MySQL :

- Pour un hôte ou nom d'hôte, spécifiez `mysql-instance1.123456789012.us-east-1.rds.amazonaws.com`
- Pour un port, spécifiez `3306`

Vous pouvez vous connecter à une instance de base de données MySQL Amazon RDS en utilisant des outils tels que l'utilitaire de ligne de commande MySQL. Pour de plus amples informations sur l'utilisation du client MySQL, veuillez consulter mysql - The MySQL Command-Line Client dans la documentation MySQL. MySQL Workbench est une application basée sur l'interface utilisateur graphique que vous pouvez utiliser pour la connexion. Pour de plus amples informations, veuillez consulter la page Télécharger MySQL Workbench. Pour de plus amples informations sur l'installation de MySQL (y compris le client MySQL), veuillez consulter Installing and Upgrading MySQL.

Pour se connecter à une instance de base de données hors de son Amazon VPC, l'instance de base de données doit être accessible au public, l'accès doit être accordé en utilisant les règles entrantes du groupe de sécurité de l'instance de base de données et d'autres exigences doivent être respectées. Pour de plus amples informations, veuillez consulter Impossible de se connecter à l'instance de base de données Amazon RDS (p. 1639).

Vous pouvez utiliser le chiffrement SSL sur les connexions à une instance de base de données MySQL Amazon RDS. Pour plus d'informations, consultez Utilisation de SSL avec une instance de base de données MySQL (p. 788). Si vous utilisez l'authentification de base de données IAM, vous devez utiliser une connexion SSL. Pour plus d'informations, consultez Authentification de base de données IAM pour MySQL et PostgreSQL (p. 1554).

Vous pouvez également vous connecter à une instance de base de données à partir d'un serveur Web. Pour plus d'informations, consultez Didacticiel : Créer un serveur web et une instance de base de données Amazon RDS (p. 109).

> **Note**
>
> Pour de plus amples informations sur la connexion à une instance de base de données MariaDB, veuillez consulter Connexion à une instance de base de données exécutant le moteur de base de données MariaDB (p. 556).

Connexion depuis le client MySQL

Pour se connecter à une instance de base de données grâce au client MySQL, saisissez la commande suivante dans une invite de commande afin de vous connecter à une instance de base de données en utilisant le client MySQL. Pour le paramètre -h, remplacez le nom DNS (point de terminaison) de votre instance de base de données. Pour le paramètre -P, remplacez le port pour votre instance de base de données. Pour le paramètre -u, remplacez le nom d'utilisateur d'un utilisateur de base de données valide, par exemple l'utilisateur principal. Entrez le mot de passe de l'utilisateur principal quand vous y êtes invité.

```
mysql -h mysql-instance1.123456789012.us-east-1.rds.amazonaws.com -P 3306 -u mymasteruser -
p
```

Après avoir entré le mot de passe pour l'utilisateur, le résultat suivant doit normalement s'afficher.

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 350
Server version: 5.6.40-log MySQL Community Server (GPL)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

Connexion à SSL

Amazon RDS crée un certificat SSL pour votre instance de base de données lorsque l'instance est créée. Si vous activez la vérification du certificat SSL, ce dernier inclut le point de terminaison de l'instance de base de données en tant que nom commun du certificat SSL pour assurer une protection contre les attaques par usurpation. Pour vous connecter à votre instance de base de données à l'aide de SSL, vous

pouvez utiliser l'authentification de mot de passe native ou l'authentification de base de données IAM. Pour vous connecter à votre instance de base de données à l'aide de l'authentification de base de données IAM, consultez Authentification de base de données IAM pour MySQL et PostgreSQL (p. 1554). Pour vous connecter à votre instance de base de données à l'aide de l'authentification de mot de passe native, vous pouvez procéder comme suit :

Pour se connecter à une instance de base de données avec SSL en utilisant le client MySQL

1. Téléchargez un certificat racine valide pour toutes les régions AWS.

   Pour de plus amples informations sur le téléchargement de certificats, veuillez consulter Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).
2. Saisissez la commande suivante dans une invite de commande pour vous connecter à une instance de base de données avec SSL en utilisant le client MySQL. Pour le paramètre -h, remplacez le nom DNS (point de terminaison) de votre instance de base de données. Pour le paramètre --ssl-ca, remplacez le nom de fichier du certificat SSL par le nom approprié. Pour le paramètre -P, remplacez le port pour votre instance de base de données. Pour le paramètre -u, remplacez le nom d'utilisateur d'un utilisateur de base de données valide, par exemple l'utilisateur principal. Entrez le mot de passe de l'utilisateur principal quand vous y êtes invité.

   ```
   mysql -h mysql-instance1.123456789012.us-east-1.rds.amazonaws.com --ssl-ca=rds-ca-2015-root.pem -P 3306 -u mymasteruser -p
   ```
3. Vous pouvez exiger que la connexion SSL vérifie le point de terminaison de l'instance de base de données par rapport au point de terminaison dans le certificat SSL.

   Pour MySQL 5.7 et version ultérieure :

   ```
   mysql -h mysql-instance1.123456789012.us-east-1.rds.amazonaws.com --ssl-ca=rds-ca-2015-root.pem --ssl-mode=VERIFY_IDENTITY -P 3306 -u mymasteruser -p
   ```

   Pour MySQL 5.6 et version antérieure :

   ```
   mysql -h mysql-instance1.123456789012.us-east-1.rds.amazonaws.com --ssl-ca=rds-ca-2015-root.pem --ssl-verify-server-cert -P 3306 -u mymasteruser -p
   ```
4. Entrez le mot de passe de l'utilisateur principal quand vous y êtes invité.

Vous verrez des résultats similaires à ce qui suit.

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 350
Server version: 5.6.40-log MySQL Community Server (GPL)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

Connexion depuis MySQL Workbench

Pour se connecter depuis MySQL Workbench

1. Téléchargez et installez MySQL Workbench depuis Télécharger MySQL Workbench.
2. Ouvrez MySQL Workbench.

3. Dans Base de données, choisissez Gérer les connexions.
4. Dans la fenêtre Gérer les connexions du serveur, choisissez Nouveau.
5. Dans la fenêtre Se connecter à la base de données, entrez les informations suivantes :
   - Connexion stockée – Entrez un nom pour la connexion, par exemple **`MyDB`**.
   - Nom d'hôte – Entrez le point de terminaison de l'instance de base de données.
   - Port – Entrez le port utilisé par l'instance de base de données.
   - Nom d'utilisateur – Entrez le nom d'utilisateur d'un utilisateur de base de données valide, par exemple l'utilisateur principal.
   - Mot de passe – Facultatif. Choisissez Stocker dans le coffre, puis entrez et enregistrez le mot de passe de l'utilisateur.

   La fenêtre ressemble à ce qui suit :

Vous pouvez utiliser les fonctionnalités de MySQL Workbench pour personnaliser les connexions. Par exemple, vous pouvez utiliser l'onglet SSL pour configurer les connexions SSL. Pour de plus amples informations sur l'utilisation de MySQL Workbench, veuillez consulter le manuel MySQL Workbench.

6. Facultatif. Vous pouvez choisir Tester la connexion pour vous assurer que la connexion à l'instance de base de données est réussie.
7. Choisissez Fermer.
8. Dans Base de données, choisissez Se connecter à la base de données.
9. Dans Connexion stockée, choisissez votre connexion.
10. Choisissez OK.

Dépannage des connexions à votre instance de base de données MySQL

Les deux causes les plus courantes d'échec de connexion à une nouvelle instance de base de données sont :

- L'instance de base de données a été créée grâce à un groupe de sécurité qui interdit les connexions depuis l'appareil ou l'instance Amazon EC2 où l'application ou l'utilitaire MySQL s'exécute. Si l'instance de base de données a été créée à l'intérieur d'un VPC, elle doit avoir un groupe de sécurité VPC qui autorise les connexions. Pour plus d'informations, consultez VPC Amazon Virtual Private Cloud et Amazon RDS (p. 1610).

  Vous pouvez ajouter ou modifier une règle entrante dans le groupe de sécurité. Pour Source, choisissez Mon IP. Cela autorise à accéder à l'instance de base de données à partir de l'adresse IP détectée dans votre navigateur.

  Si l'instance de base de données a été créée à l'extérieur d'un VPC, elle doit avoir un groupe de sécurité de bases de données qui autorise les connexions.

- L'instance de base de données a été créée à l'aide du port par défaut 3306, et votre entreprise dispose de règles de pare-feu bloquant les connexions à ce port depuis les appareils de votre réseau d'entreprise. Pour corriger le problème, recréez l'instance avec un port différent.

Pour de plus amples informations sur les problèmes de connexion, veuillez consulter Impossible de se connecter à l'instance de base de données Amazon RDS (p. 1639).

Mise à jour des applications pour se connecter aux instances de bases de données MySQL à l'aide des nouveaux certificats SSL/TLS

Le 19 septembre 2019, Amazon RDS a publié de nouveaux certificats de l'autorité de certification (CA) à connecter à vos instances de bases de données RDS à l'aide du protocole Secure Socket Layer ou Transport Layer Security (SSL/TLS). Vous trouverez ci-après des informations sur la mise à jour de vos applications afin d'utiliser les nouveaux certificats.

Cette rubrique peut vous aider à déterminer si des applications clientes utilisent un protocole SSL/TLS pour se connecter à vos instances de bases de données. Si tel est le cas, il vous est alors possible de vérifier si ces applications nécessitent une vérification du certificat pour se connecter.

> **Note**
>
> Certaines applications sont configurées pour se connecter aux instances de bases de données MySQL uniquement si la vérification du certificat sur le serveur s'effectue avec succès. Pour ces applications, vous devez mettre à jour les magasins d'approbations des applications clientes afin d'inclure les nouveaux certificats de l'autorité de certification.
> Vous pouvez spécifier les modes SSL suivants : `disabled`, `preferred` et `required`. Lorsque vous utilisez le mode SSL `preferred` et que le certificat d'autorité de certification n'existe pas ou n'est pas à jour, le comportement suivant s'applique :
>
> - Pour les versions mineures plus récentes de MySQL, la connexion n'utilise plus SSL et s'établit toujours avec succès.
>
> Étant donné que ces versions ultérieures utilisent le protocole OpenSSL, un certificat de serveur expiré n'empêche pas l'établissement des connexions, sauf si le mode SSL `required` est spécifié.
>
> Les versions mineures de MySQL suivantes utilisent le protocole OpenSSL :
> - Toutes les versions 8.0 de MySQL
> - MySQL 5.7.21 et versions ultérieures de MySQL 5.7
> - MySQL 5.6.39 et versions ultérieures de MySQL 5.6
> - MySQL 5.5.59 et versions ultérieures de MySQL 5.5
> - Pour les versions mineures plus anciennes de MySQL, une erreur est renvoyée.
>
> Étant donné que ces versions plus anciennes utilisent le protocole yaSSL, la vérification du certificat est strictement appliquée et la connexion échoue.
>
> Les versions mineures de MySQL suivantes utilisent le protocole yaSSL :
> - MySQL 5.7.19 et versions antérieures de MySQL 5.7
> - MySQL 5.6.37 et versions antérieures de MySQL 5.6
> - MySQL 5.5.57 et versions antérieures de MySQL 5.5

Une fois que vous avez mis à jour les certificats de l'autorité de certification dans les magasins d'approbations des applications clientes, vous pouvez soumettre les certificats de vos instances de bases de données à une rotation. Nous vous recommandons vivement de tester ces procédures dans un environnement de développement ou intermédiaire avant de les implémenter dans vos environnements de production.

Pour de plus amples informations sur la rotation de certificats, veuillez consulter Rotation de votre certificat SSL/TLS (p. 1527). Pour en savoir plus sur le téléchargement de certificats, consultez Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525). Pour de plus amples informations sur l'utilisation des protocoles SSL/TLS avec les instances de bases de données MySQL, veuillez consulter Utilisation de SSL avec une instance de base de données MySQL (p. 788).

Rubriques

- Contrôle de la connexion des applications aux instances de bases de données MySQL avec le protocole SSL (p. 800)
- Contrôle de la nécessité d'une vérification du certificat du client pour qu'il puisse se connecter (p. 801)
- Mise à jour du magasin d'approbations de votre application (p. 802)
- Exemple de code Java pour l'établissement de connexions SSL (p. 803)

Contrôle de la connexion des applications aux instances de bases de données MySQL avec le protocole SSL

Si vous utilisez Amazon RDS pour MySQL version 5.7 ou 8.0 et que le schéma de performance est activé, exécutez la requête suivante pour vérifier si les connexions utilisent le protocole SSL ou TLS. Pour de plus amples informations sur l'activation du schéma de performance, veuillez consulter Performance Schema Quick Start dans la documentation MySQL.

```
mysql> SELECT id, user, host, connection_type
       FROM performance_schema.threads pst
       INNER JOIN information_schema.processlist isp
       ON pst.processlist_id = isp.id;
```

Dans cet exemple de sortie, vous pouvez voir que votre propre session (`admin`) et une application connectée sous le nom de `webapp1` utilisent toutes deux 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)
```

Si vous utilisez Amazon RDS pour MySQL version 5.5 ou 5.6, vous ne pouvez pas déterminer depuis le côté serveur si les applications se connectent avec ou sans SSL. Pour ces versions, vous pouvez déterminer si le protocole SSL est utilisé en examinant la méthode de connexion de l'application. Vous

trouverez de plus amples informations sur l'examen de la configuration de la connexion cliente dans la section suivante.

Contrôle de la nécessité d'une vérification du certificat du client pour qu'il puisse se connecter

Vous pouvez vérifier si les clients JDBC et les clients MySQL requièrent une vérification du certificat pour pouvoir se connecter.

JDBC

L'exemple suivant avec MySQL Connector/J 8.0 illustre une façon de vérifier les propriétés de connexion JDBC d'une application afin de déterminer si les connexions nécessitent un certificat valide pour réussir. Pour de plus amples informations sur l'ensemble des options de connexion JDBC pour MySQL, veuillez consulter Configuration Properties dans la documentation MySQL.

Lorsque vous utilisez MySQL Connector/J 8.0, une connexion SSL nécessite la vérification du certificat de l'autorité de certification sur le serveur si vos propriétés de connexion ont `sslMode` défini sur `VERIFY_CA` ou `VERIFY_IDENTITY`, comme illustré dans l'exemple suivant.

```
Properties properties = new Properties();
properties.setProperty("sslMode", "VERIFY_IDENTITY");
properties.put("user", DB_USER);
properties.put("password", DB_PASSWORD);
```

> **Note**
>
> Si vous utilisez MySQL Java Connector v5.1.38 ou version ultérieure, ou MySQL Java Connector v8.0.9 ou version ultérieure, pour vous connecter à vos bases de données, même si vous n'avez pas explicitement configuré vos applications de manière à utiliser SSL/TLS lors de la connexion à vos bases de données, ces pilotes clients utilisent par défaut SSL/TLS. En outre, lors de l'utilisation de SSL/TLS, ils effectuent une vérification partielle du certificat et ne parviennent pas à se connecter si le certificat du serveur de base de données est expiré.

MySQL

Les exemples suivants avec le client MySQL montrent deux façons de vérifier la connexion MySQL d'un script pour déterminer si les connexions nécessitent un certificat valide pour réussir. Pour de plus amples informations sur l'ensemble des options de connexion avec le client MySQL, veuillez consulter Client-Side Configuration for Encrypted Connections dans la documentation MySQL.

Lorsque vous utilisez MySQL 5.7 or MySQL 8.0, une connexion SSL nécessite la vérification du certificat de l'autorité de certification sur le serveur si pour l'option `--ssl-mode`, vous spécifiez `VERIFY_CA` ou `VERIFY_IDENTITY`, comme illustré dans l'exemple suivant.

```
mysql -h mysql-database.rds.amazonaws.com -uadmin -ppassword --ssl-ca=/tmp/ssl-cert.pem --
ssl-mode=VERIFY_CA
```

Lorsque vous utilisez le client MySQL 5.6, une connexion SSL nécessite la vérification du certificat de l'autorité de certification sur le serveur si vous spécifiez l'option `--ssl-verify-server-cert`, comme illustré dans l'exemple suivant.

```
mysql -h mysql-database.rds.amazonaws.com -uadmin -ppassword --ssl-ca=/tmp/ssl-cert.pem --
ssl-verify-server-cert
```

Mise à jour du magasin d'approbations de votre application

Pour de plus amples informations sur la mise à jour du magasin d'approbations des applications MySQL, veuillez consulter Installing SSL Certificates dans la documentation MySQL.

> **Note**
>
> Lors de la mise à jour du magasin d'approbations, vous pouvez conserver les certificats plus anciens en complément de l'ajout des nouveaux certificats.

Mise à jour du magasin d'approbations de votre application pour JDBC

Vous pouvez mettre à jour le magasin d'approbations pour les applications qui utilisent JDBC dans le cadre de connexions SSL/TLS.

Pour mettre à jour le magasin d'approbations pour les applications JDBC

1. Téléchargez le certificat racine 2019 qui fonctionne pour toutes les régions AWS et placez le fichier dans le répertoire du magasin d'approbations.

   Pour plus d'informations sur le téléchargement du certificat racine, consultez Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).
2. Convertissez le certificat au format .der à l'aide de la commande suivante.

   ```
   openssl x509 -outform der -in rds-ca-2019-root.pem -out rds-ca-2019-root.der
   ```

   Remplacez le nom du fichier par celui du fichier téléchargé.
3. Importez le certificat dans le magasin de clés à l'aide de la commande suivante.

   ```
   keytool -import -alias rds-root -keystore clientkeystore -file rds-ca-2019-root.der
   ```
4. Vérifiez que le magasin de clés a été mis à jour avec succès.

   ```
   keytool -list -v -keystore clientkeystore.jks
   ```

   Entrez le mot de passe du magasin de clés lorsque vous y êtes invité.

   La sortie doit contenir les lignes suivantes :

```
rds-root,date, trustedCertEntry,
Certificate fingerprint (SHA1):
 D4:0D:DB:29:E3:75:0D:FF:A6:71:C3:14:0B:BF:5F:47:8D:1C:80:96
# This fingerprint should match the output from the below command
openssl x509 -fingerprint -in rds-ca-2019-root.pem -noout
```

Si vous utilisez le pilote JDBC mysql dans une application, définissez les propriétés suivantes dans l'application.

```
System.setProperty("javax.net.ssl.trustStore", certs);
System.setProperty("javax.net.ssl.trustStorePassword", "password");
```

Lorsque vous démarrez l'application, définissez les propriétés suivantes.

```
java -Djavax.net.ssl.trustStore=/path_to_truststore/MyTruststore.jks -
Djavax.net.ssl.trustStorePassword=my_truststore_password com.companyName.MyApplication
```

Exemple de code Java pour l'établissement de connexions SSL

L'exemple de code suivant montre comment configurer la connexion SSL qui valide le certificat sur le serveur à l'aide de 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

Une fois que vous avez déterminé que vos connexions de base de données utilisent un protocole SSL/TLS et que vous avez mis à jour le magasin d'approbations de votre application, vous pouvez mettre à jour votre base de données de sorte qu'elle utilise les certificats rds-ca-2019. Pour obtenir des instructions, veuillez consulter l'étape 3 dans Mise à jour de votre certificat CA en modifiant votre instance de base de données (p. 1528).

Mise à niveau du moteur de base de données MySQL

Lorsque Amazon RDS prend en charge une nouvelle version d'un moteur de base de données, vous pouvez mettre à niveau vos instances de base de données vers cette nouvelle version. Il existe deux types de mises à niveau pour les instances de base de données MySQL : les mises à niveau de version majeure et les mises à niveau de version mineure.

Les mises à niveau de version majeure peuvent contenir des modifications de base de données qui ne sont pas rétrocompatibles avec les applications existantes. En conséquence, vous devez effectuer manuellement les mises à niveau de version majeure de vos instances de base de données. Vous pouvez lancer une mise à niveau de version majeure en modifiant votre instance de base de données. Cependant, avant d'effectuer une mise à niveau de version majeure, nous vous recommandons de suivre les instructions décrites dans Mises à niveau de version majeure pour MySQL (p. 806).

En revanche, une mise à niveau de version mineure contient uniquement des modifications rétrocompatibles avec les applications existantes. Vous pouvez lancer manuellement une mise à niveau de version mineure en modifiant votre instance de base de données. Vous pouvez également activer l'option Mise à niveau automatique des versions mineures lorsque vous créez ou modifiez une instance de base de données. Dans ce cas, votre instance de base de données est automatiquement mise à niveau une fois que Amazon RDS a testé et approuvé la nouvelle version. Pour de plus amples informations sur la mise à niveau, veuillez consulter Mise à niveau d'une version du moteur d'une instance de base de données (p. 267).

Si votre instance de base de données MySQL utilise des réplicas en lecture, vous devez mettre à niveau tous les réplicas en lecture avant de mettre à niveau l'instance source. Si votre instance de base de données se trouve dans un déploiement Multi-AZ, les deux réplicas, principal et de secours, sont mis à niveau. Votre instance de base de données n'est pas disponible tant que la mise à niveau n'est pas terminée.

Rubriques

- Présentation de la mise à niveau (p. 805)
- Mises à niveau de version majeure pour MySQL (p. 806)
- Test d'une mise à niveau (p. 809)
- Mise à niveau d'une instance de base de données MySQL (p. 810)
- Mises à niveau automatiques des versions mineures pour MySQL (p. 810)
- Mise à niveau d'une base de données MySQL avec des temps d'arrêt réduits (p. 812)

Présentation de la mise à niveau

Lorsque vous utilisez AWS Management Console pour mettre à niveau une instance de base de données, les cibles de mise à niveau valides pour l'instance de base de données sont affichées. Vous pouvez également utiliser la commande AWS CLI suivante pour identifier les cibles de mise à niveau valides pour une instance de base de données :

Pour Linux, macOS ou Unix :

```
aws rds describe-db-engine-versions \
  --engine mysql \
  --engine-version version-number \
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

Pour Windows :

```
aws rds describe-db-engine-versions ^
  --engine mysql ^
  --engine-version version-number ^
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

Par exemple, pour identifier les cibles de mise à niveau valides pour une instance de base de données MySQL version 5.6.43, exécutez la commande AWS CLI suivante :

Pour Linux, macOS ou Unix :

```
aws rds describe-db-engine-versions \
  --engine mysql \
  --engine-version 5.6.43 \
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

Pour Windows :

```
aws rds describe-db-engine-versions ^
  --engine mysql ^
  --engine-version 5.6.43 ^
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

Amazon RDS prend deux instantanés de base de données au cours du processus de mise à niveau. Le premier instantané de base de données porte sur l'instance de base de données avant que toute modification de mise à niveau soit apportée. Si la mise à niveau ne fonctionne pas pour vos bases de données, vous pouvez restaurer cet instantané pour créer une instance de base de données exécutant l'ancienne version. Le second instantané de base de données est pris à la fin de la mise à niveau.

> **Note**
>
> Amazon RDS ne prend des instantanés de base de données que si vous avez défini la période de rétention des sauvegardes de votre instance de base de données sur un nombre supérieur à 0. Pour modifier la période de rétention des sauvegardes, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Une fois la mise à niveau terminée, vous ne pouvez pas rétablir la version précédente du moteur de base de données. Si vous souhaitez revenir à la version précédente, restaurez le premier instantané de base de données pris pour créer une nouvelle instance de base de données.

Vous contrôlez à quel moment vous mettez à niveau votre instance de base de données vers une nouvelle version prise en charge par Amazon RDS. Ce niveau de contrôle vous aide à maintenir la compatibilité avec des versions de base de données spécifiques et à tester les nouvelles versions avec votre application avant un déploiement en production. Lorsque vous êtes prêt, vous pouvez effectuer des mises à niveau de version aux moments qui conviennent le mieux à votre planning.

Si votre instance DB utilise la réplication en lecture, vous devez mettre à niveau tous les réplicas en lecture avant de mettre à niveau l'instance source.

Si votre instance de base de données se trouve dans un déploiement multi-AZ, les deux instances de base de données principale et de secours sont mises à niveau. Les instances de base de données principales et de secours sont mises à niveau en même temps, et vous êtes confronté à une panne jusqu'à ce que la mise à niveau soit terminée. La durée de la panne varie selon votre moteur de base de données, la version du moteur et la taille de votre instance de base de données.

Mises à niveau de version majeure pour MySQL

Amazon RDS prend en charge les mises à niveau sur place des versions majeures suivantes du moteur de base de données MySQL :

- MySQL 5.5 vers MySQL 5.6
- MySQL 5.6 vers MySQL 5.7
- MySQL 5.7 vers MySQL 8.0

> **Note**
>
> Vous pouvez uniquement créer des instances de base de données MySQL version 5.7 et 8.0 avec les classes d'instance de base de données de la génération actuelle et de la dernière génération, en plus de la classe d'instance de base de données de la génération précédente db.m3.
> Dans certains cas, vous souhaiterez mettre à niveau une instance de base de données MySQL version 5.6 en cours d'exécution sur une classe d'instance de base de données de génération précédente (autre que db.m3) vers une instance de base de données MySQL version 5.7. Dans ce cas, commencez par modifier l'instance de base de données afin d'utiliser une classe d'instance de base de données de génération actuelle ou de dernière génération. Ensuite, vous pouvez modifier l'instance de base de données pour utiliser le moteur de base de données MySQL version 5.7. Pour de plus amples informations sur les classes d'instance de base de données Amazon RDS, veuillez consulter Classes d'instances de base de données (p. 6).

Rubriques

- Présentation des mises à niveau de version majeure MySQL (p. 807)

- Les mises à niveau vers MySQL version 5.7 peuvent être lentes (p. 807)
- Vérifications préalables aux mises à jour de MySQL 5.7 vers 8.0 (p. 808)

Présentation des mises à niveau de version majeure MySQL

Les mises à niveau de versions majeures peuvent contenir des modifications de base de données qui ne sont pas rétrocompatibles avec les applications existantes. En conséquence, Amazon RDS n'applique pas automatiquement les mises à niveau de version majeure. Vous devez modifier manuellement votre instance de base de données. Nous vous recommandons de tester soigneusement toute mise à niveau avant de l'appliquer à vos instances de production.

Pour effectuer une mise à niveau de version majeure d'une instance de base de données MySQL version 5.5 sur Amazon RDS vers MySQL version 5.6 ou ultérieure, commencez par effectuer toutes les mises à jour disponibles du système d'exploitation. Une fois les mises à jour du système d'exploitation terminées, mettez à niveau chaque version majeure : 5.5 vers 5.6, puis 5.6 vers 5.7, puis 5.7 vers 8.0. Les instances de base de données MySQL créées avant le 24 avril 2014 affichent une mise à jour de système d'exploitation disponible jusqu'à ce que celle-ci soit appliquée. Pour de plus amples informations sur les mises à jour du système d'exploitation, veuillez consulter Application des mises à jour pour une instance de base de données (p. 262).

Au cours d'une mise à niveau de version majeure de MySQL, Amazon RDS exécute le fichier binaire MySQL `mysql_upgrade` pour mettre à niveau les tables, si nécessaire. Amazon RDS vide également les tables `slow_log` et `general_log` pendant une mise à niveau de version majeure. Pour conserver les informations de journal, enregistrez le contenu du journal avant la mise à niveau de version majeure.

Les mises à niveau des versions majeures de MySQL durent généralement environ 10 minutes. Certaines mises à niveau peuvent durer plus longtemps en raison de la taille de la classe d'instance de base de données ou parce que l'instance ne suit pas certaines directives opérationnelles indiquées dans Bonnes pratiques relatives à Amazon RDS. (p. 135). Si vous effectuez une mise à niveau d'une instance de base de données à partir de la console Amazon RDS, le statut de l'instance de base de données indique quand la mise niveau est terminée. Si vous effectuez une mise à niveau à l'aide de l'AWS Command Line Interface (AWS CLI), utilisez la commande describe-db-instances et vérifiez la valeur de `Status`.

Les mises à niveau vers MySQL version 5.7 peuvent être lentes

MySQL version 5.6.4 a introduit un nouveau format de date et d'heure pour les colonnes `datetime`, `time` et `timestamp`, qui autorise les expressions fractionnaires dans les valeurs de date et d'heure. Lors de la mise à niveau d'une instance de base de données vers MySQL version 5.7, MySQL force la conversion de tous les types de colonne de date et d'heure dans le nouveau format.

Étant donné que cette conversion recrée vos tables, cela peut prendre beaucoup de temps pour terminer la mise à niveau de l'instance de base de données. La conversion forcée se produit pour toutes les instances de base de données qui exécutent une version MySQL antérieure à la version 5.6.4. Elle se produit également pour les instances de base de données qui ont été mises à niveau à partir d'une version de MySQL antérieure à la version 5.6.4 vers une version autre que 5.7.

Si votre instance de base de données exécute une version de MySQL antérieure à la version 5.6.4 ou a été mise à niveau à partir d'une version antérieure à la version 5.6.4, nous recommandons d'effectuer une étape supplémentaire. Dans ce cas, nous vous recommandons de convertir les colonnes `datetime`, `time` et `timestamp` de votre base de données avant de mettre à niveau votre instance de base de données vers MySQL version 5.7. Cette conversion peut considérablement réduire le temps nécessaire pour mettre à niveau l'instance de base de données vers MySQL version 5.7. Pour mettre à niveau les colonnes de date et d'heure vers le nouveau format, vous devez émettre la commande `ALTER TABLE <table_name> FORCE;` pour chaque table qui contient des colonnes de date ou d'heure. Comme la modification d'une table la verrouille en lecture seule, il est recommandé d'effectuer cette mise à jour pendant une fenêtre de maintenance.

Pour trouver toutes les tables de votre base de données qui comportent des colonnes `datetime`, `time` ou `timestamp`, et créer une commande `ALTER TABLE <table_name> FORCE;` pour chaque table, utilisez la requête suivante.

```
SELECT DISTINCT CONCAT('ALTER TABLE `',
      REPLACE(is_tables.TABLE_SCHEMA, '`', '``'), '`.`',
      REPLACE(is_tables.TABLE_NAME, '`', '``'), '` FORCE;')
    FROM information_schema.TABLES is_tables
      INNER JOIN information_schema.COLUMNS col ON col.TABLE_SCHEMA =
 is_tables.TABLE_SCHEMA
        AND col.TABLE_NAME = is_tables.TABLE_NAME
      LEFT OUTER JOIN information_schema.INNODB_SYS_TABLES systables ON
        SUBSTRING_INDEX(systables.NAME, '#', 1) =
 CONCAT(is_tables.TABLE_SCHEMA,'/',is_tables.TABLE_NAME)
      LEFT OUTER JOIN information_schema.INNODB_SYS_COLUMNS syscolumns ON
        syscolumns.TABLE_ID = systables.TABLE_ID AND syscolumns.NAME = col.COLUMN_NAME
    WHERE col.COLUMN_TYPE IN ('time','timestamp','datetime')
      AND is_tables.TABLE_TYPE = 'BASE TABLE'
      AND is_tables.TABLE_SCHEMA NOT IN ('mysql','information_schema','performance_schema')
      AND (is_tables.ENGINE = 'InnoDB' AND syscolumns.MTYPE = 6);
```

Vérifications préalables aux mises à jour de MySQL 5.7 vers 8.0

MySQL 8.0 inclut plusieurs incompatibilités avec MySQL 5.7. Ces incompatibilités peuvent provoquer des problèmes lors d'une mise à niveau de MySQL 5.7 vers MySQL 8.0. Une certaine préparation est donc nécessaire sur votre base de données pour garantir la réussite de la mise à niveau. La liste suivante est une liste généralisée de ces incompatibilités :

- Les tables ne doivent pas utiliser de fonctions ou de types de données obsolètes.
- Il ne doit y avoir aucun fichier *.frm orphelin.
- Les déclencheurs ne doivent pas avoir de definer manquant ou vide, ni de contexte de création invalide.
- Aucune table partitionnée ne doit utiliser de moteur de stockage dépourvu de prise en charge native du partitionnement.
- Il ne doit y avoir aucune violation de mot clé ou de mot réservé. Certains mots clés doivent être réservés dans MySQL 8.0 alors qu'ils ne l'étaient pas par le passé.

  Pour en savoir plus, consultez Mots clés et mots réservés dans la documentation MySQL.
- Aucune table de la base de données du système `mysql`dans MySQL 5.7 ne doit avoir le même nom que la table utilisée dans le dictionnaire de données MySQL 8.0.
- Aucun mode SQL obsolète ne doit être défini dans la configuration variable de votre système `sql_mode`.
- Aucune table ni procédure stockée avec des éléments de colonne `ENUM` ou `SET` individuels ne doit dépasser 255 caractères ou 1 020 octets de longueur.
- Avant de mettre à niveau vers la version MySQL 8.0.13 ou une version ultérieure, aucune partition de table ne doit se trouver dans les espaces de stockage InnoDB partagés.
- Aucune requête ni définition de programme de la version MySQL 8.0.12 ou d'une version antérieure ne doit utiliser de qualificateur `ASC` ou `DESC` pour les clauses `GROUP BY`.
- Votre installation MySQL ne doit pas utiliser de fonctionnalités incompatibles avec MySQL 8.0.

  Pour en savoir plus, consultez Fonctionnalités supprimées dans MySQL 8.0 dans la documentation MySQL.
- Aucun nom de contrainte de clé étrangère ne doit dépasser 64 caractères.
- Pour une meilleure prise en charge d'Unicode, envisagez de convertir les objets qui utilisent le jeu de caractères `utf8mb3` pour utiliser le jeu de caractères `utf8mb4`. Le jeu de caractères `utf8mb3` est obsolète. Envisagez également d'utiliser `utf8mb4` pour référencer les jeux de caractères au lieu de `utf8`. Actuellement, `utf8` est un alias du jeu de caractères `utf8mb3`.

Pour en savoir plus, consultez Le jeu de caractères utf8mb3 (encodage Unicode 3 octets en UTF-8) dans la documentation MySQL.

Lorsque vous démarrez une mise à niveau de MySQL 5.7 vers 8.0, Amazon RDS exécute automatiquement des vérifications préalables pour détecter ces incompatibilités. Pour plus d'informations sur la mise à niveau vers MySQL 8.0, consultez Mise à niveau de MySQL dans la documentation MySQL.

Ces vérifications préalables sont obligatoires. Vous ne pouvez pas choisir de les ignorer. Elles offrent les avantages suivants :

- Elles vous permettent d'éviter les temps d'arrêts non planifiés pendant la mise à niveau.
- Si vous avez des incompatibilités, Amazon RDS empêche la mise à niveau et vous fournit un journal pour que vous en sachiez plus à leur sujet. Vous pouvez ensuite utiliser le journal pour préparer votre base de données pour la mise à niveau vers la version 8.0 de MySQL en éliminant ces incompatibilités. Pour plus d'informations sur la suppression des incompatibilités, voir Préparation de votre installation pour la mise à niveau dans la documentation MySQL et Mise à niveau vers MySQL 8.0 ? voici ce que vous devez savoir... sur le blog MySQL Server.

Certaines vérifications préalables sont incluses avec MySQL et d'autres ont été spécifiquement créées par l'équipe Amazon RDS. Pour de plus amples informations sur les vérifications préalables fournies par MySQL, veuillez consulter Upgrade Checker Utility.

Les vérifications préalables s'exécutent avant que l'instance de base de données soit arrêtée pour la mise à niveau, ce qui signifie que leur exécution n'entraîne aucun temps d'arrêt. Si les vérifications préalables trouvent une incompatibilité, Amazon RDS annule automatiquement la mise à niveau avant que l'instance de base de données soit arrêtée. Amazon RDS génère également un événement pour l'incompatibilité. Pour de plus amples informations sur les événements Amazon RDS, veuillez consulter Utilisation de la notification d'événement Amazon RDS (p. 467)

Amazon RDS enregistre des informations détaillées sur chaque incompatibilité dans le fichier journal `PrePatchCompatibility.log`. Dans la plupart des cas, l'entrée de journal inclut un lien vers la documentation MySQL permettant de corriger l'incompatibilité. Pour de plus amples informations sur l'affichage des fichiers journaux, veuillez consulter Liste et affichage des fichiers journaux de base de données (p. 491).

En raison de la nature des vérifications préalables, elle analysent les objets dans votre base de données. L'analyse entraîne la consommation de ressources et augmente le temps nécessaire pour la mise à niveau.

> **Note**
>
> Amazon RDS n'exécute les vérifications préalables que pour une mise à niveau de MySQL 5.7 vers MySQL 8.0. Elles ne sont pas exécutées pour les mises à niveau vers une version antérieure à MySQL 8.0. Par exemple, les vérifications préalables ne sont pas exécutées pour une mise à niveau de MySQL 5.6 vers MySQL 5.7.

Test d'une mise à niveau

Avant d'effectuer une mise à niveau de version majeure sur votre instance de base de données, testez soigneusement la compatibilité de votre base de données avec la nouvelle version. En outre, vous devez tester soigneusement la compatibilité de toutes les applications qui accèdent à la base de données avec la nouvelle version. Nous vous recommandons d'utiliser la procédure suivante.

Pour tester une mise à niveau de version majeure

1. Passez en revue la documentation de la mise à niveau pour la nouvelle version du moteur de base de données afin de voir si des problèmes de compatibilité peuvent affecter votre base de données ou vos applications :

- Changements dans MySQL 5.6
- Changements dans MySQL 5.7
- Changements dans MySQL 8.0

2. Si votre instance de base de données est membre d'un groupe de paramètres de base de données personnalisé, créez un nouveau groupe de paramètres de base de données avec vos paramètres existants, qui soit compatible avec la nouvelle version majeure. Spécifiez le nouveau groupe de paramètres de base de données lorsque vous mettez à niveau votre instance de test afin que les tests de mise à niveau puissent vérifier son bon fonctionnement. Pour de plus amples informations sur la création d'un groupe de paramètres de base de données, veuillez consulter Utilisation de groupes de paramètres de base de données (p. 225).
3. Créez un instantané de base de données de l'instance de base de données à mettre à niveau. Pour de plus amples informations, veuillez consulter Création d'un instantané de base de données (p. 327).
4. Restaurez l'instantané de base de données pour créer une nouvelle instance de base de données de test. Pour de plus amples informations, veuillez consulter Restauration à partir d'un instantané de base de données (p. 329).
5. Modifiez cette nouvelle instance de base de données de test pour la mettre à niveau vers la nouvelle version, en utilisant l'une des méthodes détaillées plus loin. Si vous avez créé un groupe de paramètres à l'étape 2, spécifiez ce groupe de paramètres.
6. Évaluez le stockage utilisé par l'instance mise à niveau pour déterminer si la mise à niveau requiert un stockage supplémentaire.
7. Exécutez sur l'instance de base de données mise à niveau autant de tests d'assurance qualité que nécessaire pour garantir que votre base de données et votre application fonctionnent correctement avec la nouvelle version. Implémentez tous les nouveaux tests requis pour évaluer l'impact des éventuels problèmes de compatibilité que vous avez identifiés à l'étape 1. Testez toutes les fonctions et procédures stockées. Dirigez les versions de test de vos applications vers l'instance de base de données mise à niveau.
8. En cas de succès de tous les tests, effectuez la mise à niveau sur votre instance de base de données de production. Nous vous recommandons de ne pas autoriser les opérations d'écriture sur l'instance de base de données tant que vous n'avez pas confirmé que tout fonctionne correctement.

Mise à niveau d'une instance de base de données MySQL

Pour de plus amples informations sur la mise à niveau manuelle ou automatique d'une instance de base de données MySQL, veuillez consulter Mise à niveau d'une version du moteur d'une instance de base de données (p. 267).

Mises à niveau automatiques des versions mineures pour MySQL

Si vous activez l'option Mise à niveau automatique des versions mineures au moment de créer ou modifier une instance de base de données, votre instance de base de données peut être mise à niveau automatiquement.

Pour certaines versions majeures de RDS pour MySQL dans certaines régions AWS, RDS désigne une version mineure comme version de mise à niveau automatique. Une fois qu'une version mineure a été testée et approuvée par Amazon RDS, la mise à niveau de la version mineure se produit automatiquement pendant votre fenêtre de maintenance. RDS ne définit pas automatiquement les dernières versions mineures publiées comme version de mise à niveau automatique. Avant de désigner une publication de version récente comme version de mise à niveau automatique, RDS prend en compte plusieurs critères, à savoir :

- Problèmes de sécurité connus
- Bogues dans la version de la communauté MySQL
- Stabilité globale du parc depuis la publication de la version mineure

Vous pouvez utiliser la commande AWS CLI et le script suivants pour déterminer la version cible de mise à niveau mineure automatique actuelle pour une version mineure MySQL spécifiée dans une région AWS spécifique.

```
aws rds describe-db-engine-versions --output=table --engine mysql --engine-version minor-version --region region
```

Par exemple, la commande AWS CLI suivante détermine la cible de mise à niveau mineure automatique pour MySQL minor version 5.7.19 dans la région USA Est (Ohio) AWS (us-east-2).

```
aws rds describe-db-engine-versions --output=table --engine mysql --engine-version 5.7.19
 --region us-east-2
```

Votre sortie est similaire à ce qui suit.

```
-----------------------------------------------------------------------------------------
|                                DescribeDBEngineVersions                                 |
+---------------------------------------------------------------------------------------+
||                                  DBEngineVersions                                     ||
|+-----------------------------------------------+-----------------------------------+|
||  DBEngineDescription                          |  MySQL Community Edition          ||
||  DBEngineVersionDescription                   |  mysql 5.7.19                     ||
||  DBParameterGroupFamily                       |  mysql5.7                         ||
||  Engine                                       |  mysql                            ||
||  EngineVersion                                |  5.7.19                           ||
||  Status                                       |  available                        ||
||  SupportsGlobalDatabases                      |  False                            ||
||  SupportsLogExportsToCloudwatchLogs           |  True                             ||
||  SupportsParallelQuery                        |  False                            ||
||  SupportsReadReplica                          |  True                             ||
|+-----------------------------------------------+-----------------------------------+|
|||                                ExportableLogTypes                                 |||
||+-------------------------------------------------------------------------------------+||
|||  audit                                                                            |||
|||  error                                                                            |||
|||  general                                                                          |||
|||  slowquery                                                                        |||
||+-------------------------------------------------------------------------------------+||
|||                                ValidUpgradeTarget                                 |||
||+-------------+---------------+---------+----------------+-------------------------+||
||| AutoUpgrade |  Description  | Engine  | EngineVersion  |  IsMajorVersionUpgrade  |||
||+-------------+---------------+---------+----------------+-------------------------+||
|||  False      |  MySQL 5.7.21 |  mysql  |  5.7.21        |  False                  |||
|||  False      |  MySQL 5.7.22 |  mysql  |  5.7.22        |  False                  |||
|||  False      |               |  mysql  |  5.7.23        |  False                  |||
|||  False      |  MySQL 5.7.24 |  mysql  |  5.7.24        |  False                  |||
|||  False      |  MySQL 5.7.25 |  mysql  |  5.7.25        |  False                  |||
|||  True       |  MySQL 5.7.26 |  mysql  |  5.7.26        |  False                  |||
|||  False      |  MySQL 5.7.28 |  mysql  |  5.7.28        |  False                  |||
|||  False      |  MySQL 5.7.30 |  mysql  |  5.7.30        |  False                  |||
|||  False      |  MySQL 5.7.31 |  mysql  |  5.7.31        |  False                  |||
|||  False      |  MySQL 8.0.11 |  mysql  |  8.0.11        |  True                   |||
|||  False      |  MySQL 8.0.13 |  mysql  |  8.0.13        |  True                   |||
|||  False      |  MySQL 8.0.15 |  mysql  |  8.0.15        |  True                   |||
|||  False      |  MySQL 8.0.16 |  mysql  |  8.0.16        |  True                   |||
|||  False      |  MySQL 8.0.17 |  mysql  |  8.0.17        |  True                   |||
|||  False      |  MySQL 8.0.19 |  mysql  |  8.0.19        |  True                   |||
```

```
|||  False      |  MySQL 8.0.20 |  mysql  |  8.0.20        |  True                    |||
|||  False      |  MySQL 8.0.21 |  mysql  |  8.0.21        |  True                    |||
||+-------------+---------------+---------+----------------+--------------------------+||
```

Dans cet exemple, la valeur de `AutoUpgrade` est `True` pour MySQL version 5.7.26. Ainsi, la cible de mise à niveau mineure automatique est MySQL version 5.7.26, comme mis en évidence dans la sortie.

Une instance de base de données MySQL est automatiquement mise à niveau pendant votre fenêtre de maintenance si les critères suivants sont réunis :

- L'option Mise à niveau automatique des versions mineures est activée pour l'instance de base de données.
- L'instance de base de données exécute une version mineure du moteur de base de données qui est inférieure à la version mineure de la mise à niveau automatique actuelle.

Pour plus d'informations, consultez Mise à niveau automatique de la version mineure du moteur (p. 269).

Mise à niveau d'une base de données MySQL avec des temps d'arrêt réduits

Si votre instance de base de données MySQL est en cours d'utilisation avec une application de production, vous pouvez utiliser la procédure suivante pour mettre à niveau la version de la base de données pour votre instance de base de données. Cette procédure peut réduire les temps d'arrêt de votre application.

La procédure suivante illustre un exemple de mise à niveau de MySQL version 5.5 vers MySQL version 5.6. Vous pouvez utiliser les mêmes étapes générales pour des mises à niveau vers d'autres versions majeures.

Pour mettre à niveau une base de données MySQL alors qu'une instance de base de données est en cours d'utilisation

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Créez un réplica en lecture de votre instance de base de données MySQL 5.5. Ce processus crée une copie pouvant être mise à niveau de votre base de données.
   a. Sur la console, choisissez Bases de données, puis sélectionnez l'instance de bases de données que vous souhaitez mettre à niveau.
   b. Pour Actions, choisissez Créer des réplicas en lecture.
   c. Spécifiez une valeur pour Identifiant de l'instance DB pour votre réplica en lecture et assurez-vous que la Classe d'instance DB et les autres paramètres correspondent à votre instance de base de données MySQL 5.5.
   d. Choisissez Créer un réplica en lecture.
3. Une fois que le réplica en lecture a été créé et que Statut indique Disponible, mettez à niveau le réplica en lecture vers MySQL 5.6 :
   a. Sur la console, choisissez Bases de données, puis sélectionnez le réplica en lecture que vous venez de créer.
   b. Sélectionnez Modifier.
   c. Pour Version du moteur de base de données, choisissez la version MySQL 5.6 vers laquelle effectuer la mise à niveau, puis sélectionnez Continuer.
   d. Pour Scheduling of Modifications (Planification des modifications), choisissez Appliquer immédiatement.
   e. Choisissez Modifier l'instance de base de données pour démarrer la mise à niveau.

4. Lorsque la mise à niveau est terminée et que Statut indique Disponible, vérifiez que le réplica en lecture mis à niveau est à jour avec l'instance de base de données MySQL 5.5 source. Pour cela, connectez-vous au réplica en lecture et exécutez la commande `SHOW SLAVE STATUS`. Si le champ `Seconds_Behind_Master` a pour valeur `0`, la réplication est à jour.
5. Faites de votre réplica en lecture MySQL 5.6 une instance de base de données autonome.

   Important

   Lorsque vous effectuez la promotion de votre réplica en lecture MySQL 5.6 en une instance de base de données mono-AZ autonome, il cesse d'être un réplica de votre instance de base de données MySQL 5.5. Nous vous conseillons d'effectuer la promotion de votre réplica en lecture MySQL 5.6 au cours d'un créneau de maintenance, lorsque votre instance de base de données MySQL 5.5 source est en mode lecture seule et que toutes les opérations d'écriture sont suspendues. Une fois la promotion terminée, vous pouvez diriger vos opérations d'écriture vers l'instance de base de données MySQL 5.6 mise à niveau pour garantir qu'aucune opération d'écriture ne se perde.
   En outre, avant la promotion de votre réplica en lecture MySQL 5.6, nous vous conseillons d'effectuer toutes les opérations en langage de définition de données (DDL) nécessaires sur votre réplica en lecture MySQL 5.6. Par exemple, la création d'index. Cette approche permet d'éviter tout effet négatif sur les performances du réplica en lecture MySQL 5.6 après sa promotion. Pour promouvoir un réplica en lecture.

   a. Sur la console, choisissez Bases de données, puis sélectionnez le réplica en lecture que vous venez de mettre à niveau.
   b. Pour Actions, choisissez Promote (Promouvoir).
   c. Choisissez Oui pour activer les sauvegardes automatiques pour l'instance du réplica en lecture. Pour de plus amples informations, veuillez consulter Utilisation des sauvegardes (p. 317).
   d. Choisissez Continuer.
   e. Choisissez Promouvoir le réplica en lecture.
6. Vous disposez à présent d'une version mise à niveau de votre base de données MySQL. À ce stade, vous pouvez diriger vos applications vers la nouvelle instance de base de données MySQL 5.6, ajouter des réplicas en lecture, configurer la prise en charge Multi-AZ, etc.

Mise à niveau d'un instantané de base de données MySQL

Amazon RDS vous permet de créer un instantané de base de données de volume de stockage de votre instance de base de données MySQL. Lorsque vous créez un instantané de base de données, l'instantané est basé sur la version du moteur utilisée par votre instance Amazon RDS. Outre la mise à niveau de la version du moteur DB de votre instance de base de données, vous pouvez également mettre à niveau la version du moteur de vos instantanés DB. A titre d'exemple, vous pouvez mettre à niveau des instantanés DB créés à partir du moteur MySQL 5.1 dans des instantanés DB pour le moteur MySQL 5.5. Après avoir restauré un instantané de base de données mis à niveau vers une nouvelle version de moteur, vous devez vérifier que la mise à jour est réussie. Pour savoir comment vérifier une mise à niveau majeure, consultez Test d'une mise à niveau (p. 809). Pour savoir comment restaurer un instantané de base de données, consultez Restauration à partir d'un instantané de base de données (p. 329).

Amazon RDS prend en charge la mise à niveau d'un instantané de base de données MySQL de MySQL version 5.1 vers MySQL 5.5.

Vous pouvez mettre à niveau des instantanés de base de données manuels, qui peuvent être chiffrés ou non chiffrés, de MySQL 5.1 vers MySQL 5.5 au sein de la même région AWS. Vous ne pouvez pas mettre à niveau des instantanés DB automatisés qui sont créés lors du processus de sauvegarde automatique.

Console

Pour mettre à niveau un instantané de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Snapshots.
3. Pour Actions, choisissez Upgrade Snapshot (Mettre à niveau l'instantané). La page Upgrade Snapshot (Mettre à niveau l'instantané) s'affiche.
4. Choisissez la New engine version (Version du nouveau moteur) vers laquelle mettre à niveau.
5. Choisissez Save changes (Enregistrer les changements) pour mettre à niveau l'instantané.

   Pendant le processus de mise à niveau, toutes les actions d'instantané sont désactivées pour l'instantané de base de données. De même, le statut de l'instantané de base de données passe de disponible à upgrading (mise à niveau), puis passe à active, une fois la mise à niveau terminée. Si l'instantané de base de données ne peut pas être mis à jour en raison d'un problème d'instantané endommagé, le statut devient indisponible. Vous ne pouvez pas récupérer l'instantané lorsqu'il a ce statut.

   > **Note**
   >
   > Si la mise à niveau de l'instantané de base de données échoue, l'instantané revient à l'état d'origine avec la version originale.

AWS CLI

Pour mettre à niveau un instantané de base de données vers une nouvelle version du moteur de base de données, utilisez la commande modify-db-snapshot de l'AWS CLI.

Paramètres

- `--db-snapshot-identifier` – L'identifiant de l'instantané de base de données à mettre à niveau. L'identifiant doit être unique pour un Amazon Resource Name (ARN). Pour plus d'informations, consultez Utilisation des Amazon Resource Names (ARN) dans Amazon RDS (p. 298).
- `--engine-version` – La version du moteur vers laquelle la mise à niveau de l'instantané de base de données doit être effectuée.

Example

Pour Linux, macOS ou Unix :

```
aws rds modify-db-snapshot \
    --db-snapshot-identifier <mydbsnapshot> \
    --engine-version <new_version>
```

Pour Windows :

```
aws rds modify-db-snapshot ^
    --db-snapshot-identifier <mydbsnapshot> ^
    --engine-version <new_version>
```

API RDS

Pour mettre à niveau un instantané de base de données vers une nouvelle version du moteur de base de données, appelez l'opération ModifyDBSnapshot de l'API Amazon RDS.

- `DBSnapshotIdentifier` – L'identifiant de l'instantané de base de données à mettre à niveau. L'identifiant doit être unique pour un Amazon Resource Name (ARN). Pour plus d'informations, consultez Utilisation des Amazon Resource Names (ARN) dans Amazon RDS (p. 298).
- `EngineVersion` – La version du moteur vers laquelle la mise à niveau de l'instantané de base de données doit être effectuée.

Example

```
https://rds.us-west-2.amazonaws.com/
   ?Action=ModifyDBSnapshot
   &DBSnapshotIdentifier=mydbsnapshot
   &EngineVersion=newversion
   &SignatureVersion=4
   &Version=2014-10-31
   &X-Amz-Algorithm=AWS4-HMAC-SHA256
   &X-Amz-Credential=AKIADQKE4SARGYLE/20161222/us-west-1/rds/aws4_request
   &X-Amz-Date=20161222T233051Z
   &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
   &X-Amz-Signature=8052a76dfb18469393c5f0182cdab0ebc224a9c7c5c949155376c1c250fc7ec3
```

Importation de données dans une instance de base de données MySQL

Vous pouvez utiliser plusieurs techniques différentes pour importer des données dans une instance de base de données Amazon RDS for MySQL. La meilleure méthode dépend de la source des données, de la quantité de données et de savoir si l'importation est effectuée une seule fois ou en continu. Si vous migrez une application avec les données, tenez également compte du temps d'immobilisation que vous êtes prêt à accepter.

Présentation

Le tableau suivant contient les techniques d'importation des données dans une instance de base de données Amazon RDS pour MySQL.

Source	Quantité de données	Une seule fois ou en continu	Interruption de l'application	Technique	En savoir plus
Base de données MySQL existante sur site ou sur Amazon EC2	Toute	Une seule fois	Momentanée	Créez une sauvegarde de votre base de données sur site, stockez-la sur Amazon S3, puis restituez le fichier de sauvegarde sur une nouvelle instance de base de données Amazon RDS exécutant MySQL.	Restauration d'une sauvegarde dans une instance de base de données MySQL Amazon RDS (p. 821)
Toute base de	Toute	Une seule fois	Minimale	Utilisez AWS Database Migration Service pour migrer la base de données avec une	Qu'est-ce que

Source	Quantité de données	Une seule fois ou en continu	Interruption de l'application	Technique	En savoir plus
données existante		ou en continu		interruption minimale et, en cas de nombreux moteurs de base de données, poursuivre la réplication en continu.	AWS Database Migratio dans le Guide de l'utilisateur AWS Database Migratio
Instance de base de données Amazon RDS MySQL existante	N'importe quel compte	Une seule fois ou en continu	Minimale	Créez un réplica en lecture pour la réplication continue. Promouvez le réplica en lecture pour la création unique d'une nouvelle instance de base de données.	Utilisation des réplicas en lecture (p. 275)
Base de données MySQL ou MariaDB existante	Petite	Une seule fois	Momentanée	Copiez les données directement dans votre instance de base de données Amazon RDS MySQL à l'aide d'un utilitaire de ligne de commande.	Importation de données à partir d'une base de données MySQL ou MariaDB vers une instance de base de données MySQL ou MariaDB Amazon RDS (p. 830)
Données non stockées dans une base de données existante	Medium	Une seule fois	Momentanée	Créez des fichiers plats et importez-les à l'aide de l'utilitaire `mysqlimport`.	Importation de données à partir d'une source vers une instance de base de données MySQL ou MariaDB (p. 846)

Source	Quantité de données	Une seule fois ou en continu	Interruption de l'application	Technique	En savoir plus
Base de données MySQL ou MariaDB existante sur site ou sur Amazon EC2	Toute	En continu	Minimale	Configurez la réplication avec une base de données MySQL existante comme source de réplication.	Réplication avec une instance MySQL ou MariaDB s'exécutant à l'extérieur d'Amazon RDS (p. 863) ou Importation de données vers une instance de base de données MySQL ou MariaDB Amazon RDS avec un temps réduit (p. 832)

Note

La base de données système `'mysql'` contient les informations d'authentification et d'autorisation requises pour se connecter à l'instance de base de données et accéder aux données. La suppression, la modification, le renommage ou la troncation de tables, de données ou d'autres contenus de la base de données `'mysql'` de votre instance de base de données peut produire une erreur et rendre inaccessibles l'instance de base de données et vos données. Si cela se produit, vous pouvez restituer l'instance de base de données depuis un instantané à l'aide de la commande AWS CLI `restore-db-instance-from-db-snapshot`. Vous pouvez récupérer l'instance de base de données à l'aide de la commande AWS CLI `restore-db-instance-to-point-in-time`.

Considérations sur l'importation de données

Voici des informations techniques supplémentaires sur le chargement de données dans MySQL. Elles sont destinées aux utilisateurs avancés qui connaissent bien l'architecture de serveur MySQL. Tous les commentaires relatifs à LOAD DATA LOCAL INFILE s'appliquent également à `mysqlimport`.

Journal binaire

Si la journalisation binaire est activée, les chargements de données s'exposent à des pertes de performance et nécessitent un espace disque supplémentaire (jusqu'à 4 fois plus grand), par comparaison

avec le chargement des mêmes données lorsque la journalisation binaire est désactivée. La gravité des pertes de performance et la quantité d'espace disque disponible requis sont directement proportionnelles à la taille des transactions utilisées pour charger les données.

Taille de la transaction

La taille de la transaction joue un rôle important dans les chargements de données MySQL. Elle exerce une influence majeure sur la consommation des ressources, l'utilisation de l'espace disque, le processus de reprise, la durée de la récupération et le format d'entrée (fichiers plats ou SQL). Cette section décrit comment la taille de la transaction influe sur la journalisation binaire. En outre, elle plaide en faveur de la désactivation de cette même journalisation lors de chargements de données volumineux. Comme évoqué précédemment, la journalisation binaire est activée et désactivée selon la valeur attribuée à la période de rétention des sauvegardes automatiques Amazon RDS. Les valeurs différentes de zéro activent la journalisation binaire, tandis que la valeur zéro la désactive. Nous décrivons aussi l'impact des transactions volumineuses sur InnoDB et expliquons pourquoi il importe que les transactions conservent une petite taille.

Petites transactions

Pour les petites transactions, la journalisation binaire multiplie par deux le nombre d'écritures sur disque requises pour charger les données. Elle peut ainsi affecter gravement les performances des autres sessions de base de données et accroître le temps requis pour charger les données. La dégradation qu'elle provoque dépend en partie du taux de chargement, des autres activités de base données se déroulant en parallèle et de la capacité de l'instance de base de données Amazon RDS.

Les journaux binaires consomment aussi un espace disque approximativement égal à la quantité de données chargées jusqu'à leur sauvegarde et leur suppression. Heureusement, Amazon RDS réduit cette consommation en sauvegardant et en supprimant régulièrement les journaux binaires.

Transactions volumineuses

Les transactions volumineuses s'exposent à des pertes de performance 3 fois supérieures pour les IOPS et l'utilisation du disque quand la journalisation binaire est activée. En effet, le cache du journal binaire est alors écrit sur disque, ce qui entraîne une utilisation de l'espace disque et une opération d'E/S supplémentaire pour chaque écriture. Comme le cache ne peut pas être écrit sur le journal binaire tant que la transaction n'est pas validée ou annulée, il utilise de l'espace disque proportionnellement à la quantité de données chargée. Lorsque la transaction est validée, le cache doit être copié sur le journal binaire, ce qui crée une troisième copie des données sur disque.

Pour cette raison, il doit y avoir au moins trois fois plus d'espace disque disponible pour charger les données que lorsque la journalisation binaire est désactivée. Par exemple, 10 Gio de données chargées dans une même transaction utilisent au moins 30 Gio d'espace disque pendant le chargement. Cette transaction utilise 10 Gio pour la table + 10 Gio pour le cache du journal binaire + 10 Gio pour le journal binaire lui-même. Le fichier cache demeure sur le disque jusqu'à ce que la session qui l'a créé se termine ou que la session remplisse à nouveau le cache du journal binaire lors d'une autre transaction. Étant donné que le journal binaire demeure sur le disque jusqu'à la sauvegarde, la libération des 20 Gio supplémentaires peut prendre un certain temps.

Si les données ont été chargées à l'aide de LOAD DATA LOCAL INFILE, une autre copie des données est toutefois créée lorsque la base de données doit être récupérée à partir d'une sauvegarde exécutée avant le chargement. Pendant le récupération, MySQL extrait les données du journal binaire dans un fichier plat. MySQL exécute ensuite LOAD DATA LOCAL INFILE, exactement comme dans la transaction initiale. Cependant, le fichier d'entrée se trouve alors sur le serveur de base de données. Dans le cas de l'exemple précédent, la récupération échoue, sauf si 40 Gio d'espace disque ou plus sont disponibles.

Désactiver la journalisation binaire

Chaque fois que possible, désactivez la journalisation binaire lors des chargements de données volumineux afin d'éviter une surcharge des ressources et des contraintes d'espace disque supplémentaire.

Dans Amazon RDS, la désactivation de la journalisation binaire consiste simplement à définir la période de rétention des sauvegardes avec la valeur zéro (0). Si vous procédez ainsi, nous vous recommandons de prendre un instantané de l'instance de base de données immédiatement avant le chargement. Au besoin, vous pourrez ainsi annuler rapidement et facilement les modifications effectuées pendant le chargement.

Après le chargement, définissez la période de rétention des sauvegardes avec une valeur appropriée, différente de zéro.

Vous ne pouvez pas définir la période de rétention des sauvegardes sur la valeur zéro si l'instance de base de données est une instance de base de données source pour les réplicas en lecture.

InnoDB

Les informations de cette section fournissent un puissant argument pour que les transactions conservent une petite taille lors de l'utilisation d'InnoDB.

Annuler

InnoDB génère l'annulation pour prendre en charge des fonctions telles que la restauration de transaction et MVCC. L'annulation est stockée dans l'espace de table système InnoDB (généralement ibdata1) et conservée jusqu'à ce qu'elle soit supprimée par le thread de purge. Comme le thread de purge ne peut pas aller au-delà de l'annulation de la transaction active la plus ancienne, il est effectivement bloqué jusqu'à ce que la transaction soit validée ou restaurée. Si la base de données traite d'autres transactions pendant le chargement, leur annulation s'accumule également dans l'espace de table système et ne peut pas être supprimée, même si les transactions sont validées et qu'aucune transaction ne nécessite l'annulation pour MVCC. Dans ce cas, toutes les transactions (y compris les transactions en lecture seule) qui accèdent aux lignes modifiées par une transaction quelle qu'elle soit (pas simplement la transaction de chargement) ralentissent, car elles analysent les annulations susceptibles d'avoir été purgées si ce n'est pour la transaction de chargement de longue durée. Ce ralentissement provient du fait que les transactions analysent les annulations susceptibles d'avoir été purgées si ce n'est pour la transaction de chargement de longue durée.

Les annulations sont stockées dans l'espace de table du système, et celui-ci ne peut jamais être réduit. Les transactions de chargements de données volumineux peuvent donc entraîner un agrandissement conséquent de l'espace de table système et utiliser ainsi une espace disque que vous ne pouvez pas revendiquer sans recréer intégralement la base de données.

Restauration

InnoDB est optimisé pour les validations. La restauration d'une transaction à une version antérieure peut être extrêmement longue. Dans certains cas, il peut être plus rapide d'effectuer une restauration à un instant dans le passé ou de restaurer un instantané de bases de données.

Format des données en entrée

MySQL peut accepter les données entrantes sous deux formes différentes : fichiers plats et SQL. Cette section soulignes certains des principaux avantages et désavantages de chaque format.

Fichiers plats

Le chargement de fichiers plats avec LOAD DATA LOCAL INFILE peut être la solution la plus rapide et la moins coûteuse pour charger les données, aussi longtemps que la taille des transactions demeure relativement petite. Comparés au chargement des mêmes données avec SQL, les fichiers plats nécessitent généralement moins de trafic réseau, des coûts de transmission inférieurs et un chargement plus rapide en raison d'une surcharge réduite de la base de données.

Une seule transaction de grande taille

LOAD DATA LOCAL INFILE charge la totalité du fichier plat comme une seule transaction. Ce n'est pas nécessairement un inconvénient. Si la taille des fichiers individuels peut demeurer petite, cette situation présente un certain nombre d'avantages :

- Capacité de reprise – il est facile de suivre les fichiers qui ont été chargés. Si un problème survient pendant le chargement, vous pouvez reprendre la transaction là où elle s'est arrêtée sans trop de peine. Certaines données devront peut-être être retransmises vers Amazon RDS, mais dans le cas de petits fichiers, la quantité retransmise est minimale.
- Chargement de données en parallèle – si vous devez économiser les opérations d'E/S par seconde et la bande passante réseau avec un seul chargement de fichier, le chargement en parallèle peut économiser du temps.
- Limitation du taux de chargement – le chargement des données impacte-t-il négativement d'autres processus ? Limitez le chargement en augmentant l'intervalle entre les fichiers.

Soyez vigilant

Les avantages de LOAD DATA LOCAL INFILE diminuent rapidement lorsque la taille des transactions augmente. Si la décomposition d'un ensemble de données volumineux en ensembles de plus petite taille n'est pas une option, SQL peut être le meilleur choix.

SQL

SQL possède un avantage principal sur les fichiers plats : il permet facilement de conserver aux transactions une petite taille. Cependant, le chargement de SQL peut prendre significativement plus de temps que les fichiers plats et il peut être difficile de définir à quel endroit reprendre le chargement après une défaillance. Par exemple, il n'est pas possible de redémarrer les fichiers mysqldump. Si une défaillance se produit lors du chargement d'un fichier mysqldump, celui-ci nécessite une modification ou un remplacement avant que le chargement puisse reprendre. La solution consiste à procéder à une restauration à un instant dans le passé avant le chargement et à relire le fichier après que l'origine de la défaillance a été éliminée.

Effectuer des points de contrôle à l'aide des instantanés Amazon RDS

Si vous avez un chargement qui va nécessiter plusieurs heures, voire plusieurs jours, le chargement sans journalisation binaire n'est pas une perspective très attrayante, à moins que vous ne puissiez effectuer des points de contrôle réguliers. C'est là que la fonction de snapshot DB Amazon RDS se révèle très pratique. Un snapshot DB crée une copie cohérente à un instant donné de votre instance de base de données, copie qui peut être utilisée pour restaurer la base de données à ce point dans le passé en cas d'incident ou autre contretemps.

Pour créer un point de contrôle, prenez simplement un snapshot DB. Tous les snapshots DB précédents pris pour les points de contrôle peuvent être supprimés sans affecter la durabilité ou le temps de restauration.

Comme les instantanés sont également rapides, les points de contrôle fréquents n'allongent pas de façon significative le temps de chargement.

Diminution du temps de chargement

Voici quelques conseils supplémentaires pour réduire les temps de chargement :

- Créez tous les index secondaires avant le chargement. Cette solution est contre-intuitive pour ceux qui connaissent d'autres bases de données. L'ajout ou la modification d'un index secondaire entraîne la

création par MySQL d'une nouvelle table avec les modifications d'index, la copie des données de la table existante vers la nouvelle table et la suppression de la table d'origine.

- Chargez les données dans l'ordre PK. Ce conseil est particulièrement utile pour les tables InnoDB, pour lesquelles les temps de chargement peuvent être réduits de 75 à 80 % et la taille des fichiers de données divisée par deux.
- Désactivez les contraintes de clé étrangère foreign_key_checks=0. Ceci est nécessaire pour les fichiers plats chargés avec LOAD DATA LOCAL INFILE dans de nombreux cas. Pour tout chargement, la désactivation des contrôles FK offre des gains de performance significatifs. Veillez simplement à bien activer les contraintes et à vérifier les données après le chargement.
- Effectuez un chargement en parallèle à moins que vos ressources ne soient proches d'une limite. Utilisez des tables partitionnées le cas échéant.
- Utilisez des insertions à valeurs multiples lors du chargement avec SQL pour minimiser les frais généraux lors de l'exécution d'instructions. Si vous utilisez mysqldump, cela est fait automatiquement.
- Réduisez les E/S du journal InnoDB innodb_flush_log_at_trx_commit=0
- Si vous chargez des données dans une instance de base de données ne disposant pas de réplicas en lecture, définissez le paramètre sync_binlog sur 0 lors du chargement des données. Une fois le chargement des données terminé, définissez le paramètre sync_binlog de nouveau sur 1.
- Chargez les données avant de convertir l'instance de base de données en déploiement multi-AZ. Toutefois, si l'instance de base de données utilise déjà un déploiement multi-AZ, passer à un déploiement mono-AZ pour le chargement des données n'est pas recommandé, car cela fournit uniquement des améliorations marginales.

> **Note**
>
> L'utilisation d'innodb_flush_log_at_trx_commit=0 oblige InnoDB à vider ses journaux toutes les secondes, et non à chaque validation. Il en résulte un avantage conséquent en termes de vitesse, mais cela peut aussi conduire à une perte des données lors d'un incident. A utiliser avec précaution.

Rubriques

- Restauration d'une sauvegarde dans une instance de base de données MySQL Amazon RDS (p. 821)
- Importation de données à partir d'une base de données MySQL ou MariaDB vers une instance de base de données MySQL ou MariaDB Amazon RDS (p. 830)
- Importation de données vers une instance de base de données MySQL ou MariaDB Amazon RDS avec un temps réduit (p. 832)
- Importation de données à partir d'une source vers une instance de base de données MySQL ou MariaDB (p. 846)

Restauration d'une sauvegarde dans une instance de base de données MySQL Amazon RDS

Amazon RDS prend en charge l'importation de bases de données MySQL à l'aide de fichiers de sauvegarde. Vous pouvez créer une sauvegarde de votre base de données, la stocker sur Amazon S3, puis restaurer le fichier de sauvegarde sur une nouvelle instance de base de données Amazon RDS qui exécute MySQL.

Le scénario décrit dans cette section restaure une sauvegarde d'une base de données sur site. Vous pouvez utiliser cette technique pour les bases de données situées dans d'autres emplacements, tels que Amazon EC2 ou des services cloud non AWS, tant que la base de données est accessible.

Le scénario pris en charge est présenté dans le schéma suivant.

L'importation de fichiers de sauvegarde depuis Amazon S3 est prise en charge pour MySQL version 5.6, 5.7 et 8.0. L'importation de fichiers de sauvegarde depuis Amazon S3 est disponible dans toutes les régions AWS.

Nous vous recommandons d'importer votre base de données vers Amazon RDS à l'aide de fichiers de sauvegarde si votre base de données sur site peut être hors connexion pendant que le fichier de sauvegarde est créé, copié et restauré. Si votre base de données ne peut pas être hors connexion, vous pouvez utiliser la réplication des journaux binaires (binlog) pour mettre à jour la base de données après avoir migré vers Amazon RDS via Amazon S3 comme expliqué dans cette rubrique. Pour plus d'informations, consultez Réplication avec une instance MySQL ou MariaDB s'exécutant à l'extérieur d'Amazon RDS (p. 863). Vous pouvez également utiliser AWS Database Migration Service pour migrer votre base de données vers Amazon RDS. Pour de plus amples informations, veuillez consulter Qu'est-ce qu'AWS Database Migration Service ?

Limitations et recommandations pour l'importation de fichiers de sauvegarde de Amazon S3 vers Amazon RDS

Voici des limitations et recommandations pour l'importation de fichiers de sauvegarde depuis Amazon S3 :

- Vous pouvez uniquement importer vos données vers une nouvelle instance de base de données, pas une instance de base de données existante.
- Vous devez utiliser Percona XtraBackup pour créer la sauvegarde de votre base de données locale.
- Vous ne pouvez pas migrer à partir d'une base de données source dotée de tables définies à l'extérieur du répertoire de données MySQL par défaut.
- Vous devez importer vos données dans la version mineure par défaut de votre version majeure MySQL dans votre région AWS. Par exemple, si votre version principale est MySQL 5.6 et que la version mineure par défaut pour votre région AWS est 5.6.44, vous devez importer vos données dans une instance DB MySQL version 5.6.44. Vous pouvez mettre à niveau votre instance DB après l'importation. Pour plus d'informations sur la détermination de la version secondaire par défaut, reportez-vous à la section Versions de MySQL sur Amazon RDS (p. 782).
- La rétromigration n'est pas prise en charge à la fois pour les versions principales et pour les versions mineures. Par exemple, il n'est pas possible de migrer de la version 5.7 à la version 5.6. De même, il n'est pas possible de migrer de la version 5.6.39 à la version 5.6.37.
- Vous ne pouvez pas importer une base de données MySQL 5.5.

- Vous ne pouvez pas importer une base de données MySQL sur site d'une version majeure vers une autre. Par exemple, vous ne pouvez pas importer une base de données MySQL 5.6 dans une base de données Amazon RDS MySQL 5.7 ou 8.0. De même, vous ne pouvez pas importer une base de données MySQL 5.7 dans une base de données Amazon RDS MySQL 8.0. Vous pouvez mettre à niveau votre instance de base de données après l'importation.
- Vous ne pouvez pas restaurer à partir d'une base de données source chiffrée, mais vous pouvez restaurer vers une instance de base de données Amazon RDS chiffrée.
- Vous ne pouvez pas restaurer à partir d'une sauvegarde chiffrée dans le compartiment Amazon S3.
- Vous ne pouvez pas restaurer à partir d'un compartiment Amazon S3 d'une région AWS différente de celle de votre instance de base de données Amazon RDS.
- L'importation à partir d'Amazon S3 n'est pas prise en charge sur la classe d'instance de base de données db.t2.micro. Toutefois, vous pouvez procéder à une restauration vers une autre classe d'instance de base de données, puis modifier la classe d'instance de base de données ultérieurement. Pour plus d'informations sur les classes d'instance , consultez Spécifications matérielles pour les classes d'instance de base de données (p. 25).
- Amazon S3 limite la taille d'un fichier chargé vers un compartiment Amazon S3 à 5 To. Si un fichier de sauvegarde dépasse 5 To, vous devez diviser celui-ci en plusieurs fichiers plus petits.
- Lorsque vous restaurez la base de données, la sauvegarde est copiée, puis extraite sur votre instance de base de données. Par conséquent, allouez pour votre instance de base de données une quantité d'espace de stockage égale ou supérieure à la somme de la taille de sauvegarde, plus la taille de la base de données d'origine sur le disque.
- Amazon RDS limite le nombre de fichiers chargés vers un compartiment Amazon S3 à 1 million. Si les données de sauvegarde de votre base de données, y compris toutes les sauvegardes complètes et incrémentielles, dépassent 1 million de fichiers, utilisez un fichier Gzip (.gz), tar (.tar.gz) ou Percona xbstream (.xbstream) pour stocker les fichiers des sauvegardes complètes et incrémentielles dans le compartiment Amazon S3. Percona XtraBackup 8.0 prend uniquement en charge Percona xbstream pour la compression.
- Les comptes utilisateur ne sont pas importés automatiquement. Enregistrez vos comptes utilisateur depuis votre base de données source et ajoutez-les à votre nouvelle instance de base de données ultérieurement.
- Les fonctions ne sont pas importées automatiquement. Enregistrez vos fonctions depuis votre base de données source et ajoutez-les à votre nouvelle instance de base de données ultérieurement.
- Les procédures stockées ne sont pas importées automatiquement. Enregistrez vos procédures stockées depuis votre base de données source et ajoutez-les à votre nouvelle instance de base de données ultérieurement.
- Les informations de format de fuseau horaire ne sont pas importées automatiquement. Enregistrez les informations de fuseau horaire depuis votre base de données source et ajoutez-les à votre nouvelle instance de base de données ultérieurement. Pour plus d'informations, consultez Fuseau horaire local pour les instances de bases de données MySQL (p. 791).
- Le paramètre `innodb_data_file_path` doit être configuré avec un seul fichier de données qui utilise le nom de fichier de données par défaut `"ibdata1"`. Les bases de données comportant deux fichiers de données, ou avec un fichier de données portant un nom différent, ne peuvent pas faire l'objet d'une migration à l'aide de cette méthode.

  Voici des exemples de noms de fichier non autorisés : `"innodb_data_file_path=ibdata1:50M;ibdata2:50M:autoextend"` et `"innodb_data_file_path=ibdata01:50M:autoextend"`.
- La taille maximale de la base de données restaurée est la taille maximale de base de données prise en charge moins la taille de la sauvegarde. Ainsi, si la taille maximale de base de données prise en charge est de 64 TiO et que la taille de la sauvegarde est de 30 TiO, la taille maximale de la base de données restaurée est de 34 TiO, comme dans l'exemple suivant :

  ```
  64 TiB - 30 TiB = 34 TiB
  ```

Pour de plus amples informations sur la taille maximale de base de données prise en charge par Amazon RDS for MySQL, veuillez consulter Stockage SSD à usage général (p. 31) et Stockage SSD d'I/O par seconde provisionnées (p. 33).

Présentation de la configuration de l'importation des fichiers de sauvegarde de Amazon S3 vers Amazon RDS

Voici les composants que vous devrez configurer pour importer les fichiers de sauvegarde de Amazon S3 vers Amazon RDS :

- Un compartiment Amazon S3 pour stocker vos fichiers de sauvegarde.
- Une sauvegarde de votre base de données locale créée par Percona XtraBackup.
- Un rôle AWS Identity and Access Management (IAM) permettant d'autoriser Amazon RDS à accéder au compartiment.

Si vous avez déjà un compartiment Amazon S3, vous pouvez l'utiliser. Si vous n'avez pas de compartiment Amazon S3, vous pouvez en créer un nouveau. Si vous souhaitez créer un compartiment, veuillez consulter Créer un compartiment.

Utilisez l'outil Percona XtraBackup pour créer votre sauvegarde. Pour plus d'informations, consultez Création de la sauvegarde de votre base de données (p. 824).

Si vous avez déjà un rôle IAM, vous pouvez l'utiliser. Si vous n'avez pas de rôle IAM, vous pouvez en créer manuellement un nouveau. Sinon, vous pouvez choisir d'avoir un rôle IAM créé pour vous dans votre compte par l'assistant lorsque vous restaurez la base de données à l'aide de la AWS Management Console. Si vous souhaitez manuellement créer un nouveau rôle IAM ou attacher des stratégies d'approbation et d'autorisation à un rôle IAM existant, consultez Création manuelle d'un rôle IAM (p. 826). Si vous souhaitez qu'un nouveau rôle IAM soit créé pour vous, suivez la procédure décrite dans Console (p. 828).

Création de la sauvegarde de votre base de données

Utilisez le logiciel Percona XtraBackup pour créer votre sauvegarde. Vous pouvez installer Percona XtraBackup à partir de la page Download Percona XtraBackup.

> **Note**
>
> Pour la migration MySQL 8.0, vous devez utiliser Percona XtraBackup 8.0. Percona XtraBackup 8.0.12 et versions ultérieures prennent en charge la migration de toutes les versions de MySQL. Si vous migrez vers Amazon RDS MySQL 8.0.20 ou versions ultérieures, vous devez utiliser Percona XTrabackUp 8.0.12 ou versions ultérieures.
> Pour les migrations MySQL 5.7, vous pouvez également utiliser Percona XtraBackup 2.4. Pour les migrations de versions antérieures de MySQL, vous pouvez également utiliser Percona XtraBackup 2.3 ou 2.4.

Vous pouvez créer une sauvegarde complète de vos fichiers de base de données MySQL à l'aide de Percona XtraBackup. Sinon, si vous utilisez déjà Percona XtraBackup pour sauvegarder vos fichiers de base de données MySQL, vous pouvez charger les fichiers et répertoires existants de vos sauvegardes complètes et incrémentielles.

Pour de plus amples informations sur la sauvegarde de votre base de données avec Percona XtraBackup, veuillez consulter la Documentation Percona XtraBackup et le binaire xtrabackup sur le site web de Percona.

Création d'une sauvegarde complète à l'aide de Percona XtraBackup

Pour créer une sauvegarde complète de vos fichiers de base de données MySQL qui peut être restaurée à partir de Amazon S3, utilisez l'utilitaire Percona XtraBackup (`xtrabackup`) pour sauvegarder votre base de données.

Par exemple, la commande suivante crée une sauvegarde d'une base de données MySQL et stocke les fichiers dans le dossier `/on-premises/s3-restore/backup`.

```
xtrabackup --backup --user=<myuser> --password=<password> --target-dir=</on-premises/s3-
restore/backup>
```

Si vous souhaitez compresser votre sauvegarde en un seul fichier (qui peut être divisé ultérieurement, si nécessaire), vous pouvez enregistrer votre sauvegarde dans l'un des formats suivants :

- Gzip (.gz)
- tar (.tar)
- Percona xbstream (.xbstream)

> **Note**
>
> Percona XtraBackup 8.0 prend uniquement en charge Percona xbstream pour la compression.

La commande suivante crée une sauvegarde de votre base de données MySQL, divisée en plusieurs fichiers Gzip.

```
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
```

La commande suivante crée une sauvegarde de votre base de données MySQL, divisée en plusieurs fichiers tar.

```
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
```

La commande suivante crée une sauvegarde de votre base de données MySQL, divisée en plusieurs fichiers xbstream.

```
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
```

Utilisation des sauvegardes incrémentielles avec Percona XtraBackup

Si vous utilisez déjà Percona XtraBackup pour effectuer des sauvegardes complètes et incrémentielles de vos fichiers de base de données MySQL, vous n'avez pas besoin de créer de sauvegarde complète et de charger les fichiers de sauvegarde vers Amazon S3. Au lieu de cela, vous pouvez économiser beaucoup de temps en copiant vos fichiers et répertoires de sauvegarde existants dans votre compartiment Amazon S3. Pour de plus amples informations sur la création de sauvegardes incrémentielles à l'aide de Percona XtraBackup, veuillez consulter Incremental Backup (Sauvegarde incrémentielle).

Lorsque vous copiez les fichiers existants des sauvegardes complètes et incrémentielles dans un compartiment Amazon S3, vous devez copier de façon récursive le contenu du répertoire de base.

Ce contenu inclut la sauvegarde complète, ainsi que tous les fichiers et répertoires des sauvegardes incrémentielles. Cette copie doit conserver la structure d'annuaire dans le compartiment Amazon S3. Amazon RDS itère dans tous les fichiers et annuaires. Amazon RDS utilise le fichier `xtrabackup-checkpoints` inclus avec chaque sauvegarde incrémentielles pour identifier le répertoire de base et pour ordonner les sauvegardes incrémentielles par leur plage de numéros de séquence de journal.

Considérations relatives à la sauvegarde pour Percona XtraBackup

Amazon RDS utilise vos fichiers de sauvegarde sur la base des noms de fichier. Nommez vos fichiers de sauvegarde avec l'extension de fichier appropriée basée sur le format de fichier—par exemple, `.xbstream` pour les fichiers stockés en utilisant le format de xbstream Percona.

Amazon RDS utilise vos fichiers de sauvegarde dans l'ordre alphabétique, ainsi que l'ordre numérique naturel. Utilisez l'option `split` lorsque vous émettez la commande `xtrabackup` pour vous assurer que vos fichiers de sauvegarde sont écrits et nommés dans l'ordre approprié.

Amazon RDS ne prend pas en charge les sauvegardes partielles créées à l'aide de Percona XtraBackup. Vous ne pouvez pas utiliser les options suivantes pour créer une sauvegarde partielle lorsque vous sauvegardez les fichiers source pour votre base de données : `--tables`, `--tables-exclude`, `--tables-file`, `--databases`, `--databases-exclude` ou `--databases-file`.

Amazon RDS prend en charge les sauvegardes incrémentielles créées à l'aide de Percona XtraBackup. Pour de plus amples informations sur la création de sauvegardes incrémentielles à l'aide de Percona XtraBackup, veuillez consulter Incremental Backup (Sauvegarde incrémentielle).

Création manuelle d'un rôle IAM

Si vous n'avez pas de rôle IAM, vous pouvez en créer manuellement un nouveau. Sinon, vous pouvez choisir d'avoir un rôle IAM créé pour vous par l'assistant lorsque vous restaurez la base de données à l'aide de la AWS Management Console. Si vous souhaitez qu'un nouveau rôle IAM soit créé pour vous, suivez la procédure décrite dans Console (p. 828).

Pour créer manuellement un rôle IAM afin d'importer votre base de données à partir de Amazon S3, créez un rôle pour déléguer des autorisations depuis le service Amazon RDS vers votre compartiment Amazon S3. Lorsque vous créez un rôle IAM, vous attachez des stratégies d'approbation et d'autorisation. Pour importer vos fichiers de sauvegarde depuis Amazon S3, utilisez des stratégies d'approbation et d'autorisation similaires aux exemples suivants. Pour de plus amples informations sur la création d'un rôle, veuillez consulter Création d'un rôle pour déléguer des autorisations à un service AWS.

Sinon, vous pouvez choisir d'avoir un rôle IAM créé pour vous par l'assistant lorsque vous restaurez la base de données à l'aide de la AWS Management Console. Si vous souhaitez qu'un nouveau rôle IAM soit créé pour vous, suivez la procédure décrite dans Console (p. 828)

Les stratégies d'approbation et d'autorisation nécessitent que vous fournissiez un Amazon Resource Name (ARN). Pour de plus amples informations sur le formatage des ARN, veuillez consulter ARN (Amazon Resource Name) et espaces de noms de service AWS.

Example Stratégie d'approbation pour l'importation à partir d'Amazon S3

```
{
    "Version": "2012-10-17",
    "Statement":
    [{
        "Effect": "Allow",
        "Principal": {"Service":  "rds.amazonaws.com"},
        "Action": "sts:AssumeRole"
    }]
}
```

Example Stratégie d'autorisation pour l'importation à partir de Amazon S3 — Autorisations des utilisateurs IAM

```
{
    "Version":"2012-10-17",
    "Statement":
    [
        {
            "Sid":"AllowS3AccessRole",
            "Effect":"Allow",
            "Action":"iam:PassRole",
            "Resource":"arn:aws:iam::IAM User ID:role/S3Access"
        }
    ]
}
```

Example Stratégie d'autorisation pour l'importation à partir de Amazon S3 — Autorisations des rôles

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
        "Effect": "Allow",
        "Action":
            [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
        "Resource": "arn:aws:s3:::bucket_name"
        },
        {
        "Effect": "Allow",
        "Action":
            [
                "s3:GetObject"
            ],
        "Resource": "arn:aws:s3:::bucket_name/prefix*"
        }
    ]
}
```

Note

Si vous incluez un préfixe de nom de fichier, vous devez inclure un astérisque (*) après le préfixe. Si vous ne voulez pas spécifier un préfixe, indiquez uniquement un astérisque.

Pour importer des données à partir d'Amazon S3 vers une nouvelle instance de base de données MySQL

Vous pouvez importer des données de Amazon S3 vers une nouvelle instance de base de données MySQL DB à l'aide de AWS Management Console, AWS CLI ou de l'API RDS.

Console

Pour importer des données à partir d'Amazon S3 vers une nouvelle instance de base de données MySQL

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le coin supérieur droit de la console Amazon RDS, choisissez la région AWS dans laquelle créer votre instance de base de données. Choisissez la même région AWS que celle du compartiment Amazon S3 contenant la sauvegarde de votre base de données.
3. Dans la panneau de navigation, choisissez Databases (Bases de données).
4. Choisissez Restaurer à partir de S3 pour lancer l'assistant.

   L'assistant s'ouvre à la page Select engine (Sélectionner un moteur).
5. Sur la page Sélectionner le moteur, choisissez MySQL, puis Suivant.

   La page Specify source backup details (Spécifier les détails de sauvegarde source) s'affiche.

6. Sur la page Specify source backup details (Spécifier les détails de sauvegarde source), spécifiez des informations sur votre sauvegarde.

a. Pour Moteur source, choisissez mysql.
b. Pour Version de moteur source, choisissez la version MySQL de votre base de données source.
c. Pour Compartiment S3, choisissez votre compartiment Amazon S3.
d. (Facultatif) Pour Préfixe du chemin de dossier S3, saisissez un préfixe de chemin de fichier pour les fichiers stockés dans votre compartiment Amazon S3. Si vous ne spécifiez pas de préfixe, RDS crée votre cluster/instance de base de données à l'aide de tous les fichiers et dossiers du dossier racine du compartiment S3. Si vous indiquez un préfixe, RDS crée votre instance de base de données à l'aide des fichiers et dossiers du compartiment S3 pour lesquels le chemin du fichier commence par le préfixe spécifié. Par exemple, supposons que vous stockez vos fichiers de sauvegarde sur S3 dans un sous-dossier appelé « sauvegardes » et que vous avez plusieurs ensembles de fichiers de sauvegarde, chacun dans son propre répertoire (gzip_backup1, gzip_backup2, etc.). Dans ce cas, vous devez spécifier un préfixe sauvegardes/gzip_backup1 pour restaurer les fichiers dans le dossier gzip_backup1.
e. Pour Créer un rôle, choisissez Oui afin de créer un rôle IAM dans votre compte ou Non afin de sélectionner un rôle IAM existant.
f. Pour Rôle IAM, sélectionnez un rôle IAM existant ou pour Nom d'un nouveau rôle IAM, spécifiez le nom d'un nouveau rôle IAM. Vous pouvez choisir d'avoir un nouveau rôle IAM créé pour vous en sélectionnant Oui pour Créer un rôle.

7. Choisissez Next pour continuer. La page Specify DB details (Spécifier les détails de la base de données) s'affiche.

   Sur la page Specify DB details (Spécifier les détails de la base de données), spécifiez les informations de votre instance de base de données. Pour plus d'informations sur chaque paramètre, consultez Paramètres des instances de base de données (p. 151).

   > **Note**
   >
   > Assurez d'allouer suffisamment de mémoire pour votre nouvelle instance de base de données afin que la restauration puisse réussir. À ce stade, vous pouvez aussi allouer de la mémoire supplémentaire pour une croissance future.

8. Choisissez Next pour continuer. La page Configure advanced settings (Configurer les paramètres avancés) s'affiche.

   Fournissez des informations supplémentaires dont Amazon RDS a besoin pour lancer l'instance de base de données. Pour plus d'informations sur chaque paramètre, consultez Paramètres des instances de base de données (p. 151).

9. Choisissez Create database (Créer une base de données).

AWS CLI

Pour importer les données à partir de Amazon S3 vers une nouvelle instance de base de données MySQL à l'aide de l'AWS CLI, appelez la commande restore-db-instance-from-s3 avec les paramètres suivants. Pour plus d'informations sur chaque paramètre, consultez Paramètres des instances de base de données (p. 151).

> **Note**
>
> Assurez d'allouer suffisamment de mémoire pour votre nouvelle instance de base de données afin que la restauration puisse réussir. À ce stade, vous pouvez aussi allouer de la mémoire supplémentaire pour une croissance future.

- `--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

Pour Linux, macOS ou Unix :

```
aws rds restore-db-instance-from-s3 \
--allocated-storage 250 \
--db-instance-identifier myidentifier \
--db-instance-class db.m4.large \
--engine mysql \
--master-username masterawsuser \
--master-user-password masteruserpassword \
--s3-bucket-name mybucket \
--s3-ingestion-role-arn arn:aws:iam::account-number:role/rolename \
--s3-prefix bucketprefix \
--source-engine mysql \
--source-engine-version 5.6.40
```

Pour Windows :

```
aws rds restore-db-instance-from-s3 ^
--allocated-storage 250 ^
--db-instance-identifier myidentifier ^
--db-instance-class db.m4.large ^
--engine mysql ^
--master-username masterawsuser ^
--master-user-password masteruserpassword ^
--s3-bucket-name mybucket ^
--s3-ingestion-role-arn arn:aws:iam::account-number:role/rolename ^
--s3-prefix bucketprefix ^
--source-engine mysql ^
--source-engine-version 5.6.40
```

API RDS

Pour importer les données à partir de Amazon S3 vers une nouvelle instance de base de données MySQL à l'aide de l'API Amazon RDS, appelez l'opération RestoreDBInstanceFromS3.

Importation de données à partir d'une base de données MySQL ou MariaDB vers une instance de base de données MySQL ou MariaDB Amazon RDS

Si votre scénario le prend en charge, il est plus facile de transférer des données vers et depuis Amazon RDS à l'aide des fichiers de sauvegarde et de Amazon S3. Pour plus d'informations, consultez Restauration d'une sauvegarde dans une instance de base de données MySQL Amazon RDS (p. 821).

Vous pouvez également importer des données à partir d'une base de données MySQL ou MariaDB existant vers une instance de base de données MySQL ou MariaDB Amazon RDS. Pour cela, vous devez copier la base de données avec mysqldump et la transférer directement dans l'instance de base de données Amazon RDS MySQL ou MariaDB. L'utilitaire de ligne de commande `mysqldump` est généralement utilisé pour effectuer des sauvegardes et des transferts de données d'un serveur MySQL ou MariaDB vers un autre. Il est fourni avec les logiciels clients MySQL et MariaDB.

Une commande `mysqldump` classique pour déplacer les données d'une base de données externe vers une instance de bases de données Amazon RDS ressemble à :

```
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**
>
> Veillez à ne pas laisser d'espace entre l'option `-p` et le mot de passe saisi.

> **Note**
>
> - Excluez les schémas suivants du fichier de vidage : `sys`, `performance_schema` et `information_schema`. L'utilitaire `mysqldump` exclut ces schémas par défaut.
> - Si vous devez migrer les utilisateurs et les privilèges, envisagez d'utiliser un outil qui génère le langage de contrôle des données (DCL) pour les recréer, tel que l'utilitaire pt-show-grants.

Les paramètres utilisés sont les suivants :

- `-u local_user` – Utilisez ce paramètre pour spécifier un nom d'utilisateur. Lors de la première utilisation de ce paramètre, vous spécifiez le nom d'un compte utilisateur sur la base de données MySQL ou MariaDB identifiée par le paramètre `--databases`.
- `--databases database_name` – Utilisez ce paramètre pour spécifier le nom de la base de données sur l'instance MySQL ou MariaDB locale que vous souhaitez importer dans Amazon RDS.
- `--single-transaction` – Utilisez ce paramètre pour vérifier que toutes les données chargées depuis la base de données locale sont en cohérence avec un point dans le temps unique. S'il existe d'autres processus qui modifient les données lorsque `mysqldump` les lit, cette option permet de maintenir l'intégrité des données.
- `--compress` – Utilisez ce paramètre pour réduire la consommation de bande passante réseau par compression des données à partir de la base de données locale avant de les envoyer vers Amazon RDS.
- `--order-by-primary` – Utilisez ce paramètre pour réduire le temps de chargement en triant les données de chaque tableau sur par clé primaire.
- `-plocal_password` – Utilisez ce paramètre pour spécifier un mot de passe. Lors de la première utilisation de ce paramètre, vous spécifiez le mot de passe du compte utilisateur identifié par le premier paramètre `-u`.
- `-u RDS_user` – Utilisez ce paramètre pour spécifier un nom d'utilisateur. Lors de la seconde utilisation de ce paramètre, vous spécifiez le nom d'un compte utilisateur sur la base de données par défaut pour l'instance de bases de données Amazon RDS MySQL ou MariaDB identifiée par le paramètre `--host`.
- `--port port_number` – Utilisez ce paramètre pour spécifier le port pour votre instance de base de données Amazon RDS MySQL ou MariaDB. Par défaut, il s'agit du port 3306, sauf si vous avez modifié la valeur lorsque vous avez créé l'instance.

- `--host host_name` – Utilisez ce paramètre pour spécifier le nom DNS du point de terminaison de l'instance de base de données Amazon RDS, par exemple `myinstance.123456789012.us-east-1.rds.amazonaws.com`. Vous pouvez trouver la valeur du point de terminaison dans les détails de l'instance dans Amazon RDS Management Console.
- `-pRDS_password` – Utilisez ce paramètre pour spécifier un mot de passe. Lors de la seconde utilisation de ce paramètre, vous spécifiez le mot de passe du compte utilisateur identifié par le second paramètre `-u`.

Vous devez créer manuellement les procédures stockées, déclencheurs, fonctions ou événements dans votre base de données Amazon RDS. Si vous avez l'un de ces objets dans la base de données que vous copiez, excluez-les lorsque vous exécutez `mysqldump` en associant les paramètres suivants à votre commande `mysqldump` : `--routines=0 --triggers=0 --events=0`.

L'exemple suivant copie l'exemple de base de données `world` de l'hôte local sur une instance de bases de données MySQL Amazon RDS.

Pour Linux, macOS ou Unix :

```
sudo mysqldump -u localuser \
    --databases world \
    --single-transaction \
    --compress \
    --order-by-primary  \
    -plocalpassword | mysql -u rdsuser \
        --port=3306 \
        --host=myinstance.123456789012.us-east-1.rds.amazonaws.com \
        -prdspassword
```

Pour Windows, la commande suivante doit être exécutée dans une invite de commandes ouverte en cliquant avec le bouton droit sur Invite de commandes dans le menu Programmes de Windows, puis en choisissant Exécuter en tant qu'administrateur :

```
mysqldump -u localuser ^
    --databases world ^
    --single-transaction ^
    --compress ^
    --order-by-primary  ^
    -plocalpassword | mysql -u rdsuser ^
        --port=3306 ^
        --host=myinstance.123456789012.us-east-1.rds.amazonaws.com ^
        -prdspassword
```

Importation de données vers une instance de base de données MySQL ou MariaDB Amazon RDS avec un temps réduit

Si votre scénario le prend en charge, il est plus facile de transférer des données vers et depuis Amazon RDS à l'aide des fichiers de sauvegarde et de Amazon S3. Pour plus d'informations, consultez Restauration d'une sauvegarde dans une instance de base de données MySQL Amazon RDS (p. 821).

Dans certains cas, vous devez importer les données à partir d'une base de données externe MySQL ou MariaDB prenant en charge une application active vers une instance de base de données MySQL ou MariaDB Amazon RDS. Vous pouvez alors utiliser la procédure suivante pour réduire l'impact sur la disponibilité de l'application. Cette procédure peut s'avérer également utile si vous travaillez avec une

base de données très volumineuse. Dans ce cas, elle vous permet de réduire le coût de l'importation en diminuant la quantité de données transmises à AWS via le réseau.

Dans cette procédure, vous pouvez transférer une copie des données de la base de données vers une instance Amazon EC2 et importer les données dans une nouvelle instance de base de données Amazon RDS. Vous pouvez alors utiliser la réplication pour mettre à jour l'instance de base de données Amazon RDS avec votre instance externe active, avant de rediriger votre application vers l'instance de base de données Amazon RDS. Vous configurez la réplication MariaDB en fonction des identificateurs de transaction globaux (GTID) si l'instance externe est MariaDB 10.0.2 ou version ultérieure, et que l'instance cible est Amazon RDS MariaDB ; sinon, vous configurez la réplication en fonction des coordonnées des journaux binaires. Nous recommandons la réplication basée sur les identificateurs de transaction globaux si votre base de données externe la prend en charge en raison de ses fonctions améliorées de sécurité en cas d'incident. Pour plus d'informations, consultez Identificateurs de transaction mondiaux dans la documentation MariaDB.

Note

Il est déconseillé d'utiliser cette procédure avec les bases de données MySQL source à partir des versions MySQL antérieures à la version 5.1, en raison de problèmes potentiels de réplication. Pour de plus amples informations, veuillez consulter Compatibilité de réplication entre versions MySQL dans la documentation MySQL.

Créer une copie de votre base de données existante

La première étape de la migration d'un volume important de données vers une instance de base de données MySQL ou MariaDB Amazon RDS avec un arrêt minimal consiste à créer une copie des données source.

Vous pouvez recourir à l'utilitaire `mysqldump` pour créer une sauvegarde de base de données au format SQL ou texte délimité. Vous devez procéder à une série de tests avec chaque format dans un environnement autre que de production pour voir quelle méthode diminue le temps d'exécution de `mysqldump`.

Vous pouvez aussi évaluer les performances de `mysqldump` par rapport à l'avantage offert par l'utilisation du format texte délimité pour le chargement. Une sauvegarde à l'aide du format texte délimité crée un fichier texte séparé par des tabulations pour chaque table vidée. Vous pouvez charger ces fichiers en parallèle à l'aide de la commande `LOAD DATA LOCAL INFILE` pour réduire le temps requis pour importer votre base de données. Pour de plus amples informations sur le choix d'un format `mysqldump` et le chargement des données, veuillez consulter Utilisation de mysqldump pour les sauvegardes dans la documentation MySQL.

Avant de démarrer l'opération de sauvegarde, vous devez définir les options de réplication sur la base de données MySQL ou MariaDB que vous copiez sur Amazon RDS. Les options de réplication incluent l'activation de la journalisation binaire et la configuration d'un ID serveur unique. La définition de ces options oblige votre serveur à démarrer la journalisation des transactions de base de données et le prépare à être une instance de réplication source ultérieurement dans le processus.

Note

- Utilisez l'option `--single-transaction` avec `mysqldump`, car elle vide un état cohérent de la base de données. Pour vous assurer de la validité d'un fichier de vidage, n'exécutez pas les instructions DDL (Data Definition Language) pendant l'exécution de `mysqldump`. Vous pouvez planifier une fenêtre de maintenance pour ces opérations.
- Excluez les schémas suivants du fichier de vidage : `sys`, `performance_schema` et `information_schema`. L'utilitaire `mysqldump` exclut ces schémas par défaut.
- Si vous devez migrer les utilisateurs et les privilèges, envisagez d'utiliser un outil qui génère le langage de contrôle des données (DCL) pour les recréer, tel que l'utilitaire pt-show-grants.

Pour définir les options de réplication

1. Modifiez le fichier my.cnf (qui se trouve généralement sous `/etc`).

```
sudo vi /etc/my.cnf
```

Ajoutez les options `log_bin` et `server_id` à la section `[mysqld]`. L'option `log_bin` fournit un identifiant de nom de fichier pour les fichiers journaux binaires. L'option `server_id` fournit un identifiant unique pour le serveur dans les relations source/réplica.

L'exemple suivant illustre la section `[mysqld]` mise à jour d'un fichier my.cnf :

```
[mysqld]
log-bin=mysql-bin
server-id=1
```

Pour de plus amples informations, veuillez consulter la documentation MySQL.

2. Redémarrez le service `mysql`.

```
sudo service mysqld restart
```

Pour créer une copie de sauvegarde de votre base de données existante

1. Créez une sauvegarde de vos données à l'aide de l'utilitaire `mysqldump`, en spécifiant un format SQL ou un format texte délimité.

   Vous devez spécifier `--master-data=2` pour pouvoir créer un fichier de sauvegarde qui puisse être utilisé pour démarrer la réplication entre les serveurs. Pour de plus amples informations, veuillez consulter la documentation mysqldump.

   Pour améliorer les performances et assurer l'intégrité des données, utilisez les options `--order-by-primary` et `--single-transaction` de `mysqldump`.

   Pour éviter d'inclure la base de données système MySQL dans la sauvegarde, n'utilisez pas l'option `--all-databases` avec `mysqldump`. Pour de plus amples informations, veuillez consulter Création d'un instantané de vidage avec mysqldump dans la documentation MySQL.

   Utilisez `chmod` si nécessaire pour vous assurer que le répertoire où le fichier de sauvegarde est en cours de création est accessible en écriture.

   > **Important**
   >
   > Sur Windows, exécutez la fenêtre de commande en tant qu'administrateur.

   - Pour produire une sortie SQL, utilisez la commande suivante.

     Pour Linux, macOS ou Unix :

     ```
     sudo mysqldump \
         --databases database_name \
         --master-data=2  \
         --single-transaction \
         --order-by-primary \
         -r backup.sql \
         -u local_user \
         -p password
     ```

     Pour Windows :

     ```
     mysqldump ^
         --databases database_name ^
         --master-data=2  ^
         --single-transaction ^
     ```

```
    --order-by-primary ^
    -r backup.sql ^
    -u local_user ^
    -p password
```

- Pour produire une sortie à texte délimité, utilisez la commande suivante.

  Pour Linux, macOS ou 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
```

  Pour 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

  Vous devez créer manuellement les procédures stockées, déclencheurs, fonctions ou événements dans votre base de données Amazon RDS. Si vous avez l'un quelconque de ces objets dans la base de données que vous copiez, excluez-les lorsque vous exécutez `mysqldump` en associant les arguments suivants à votre commande `mysqldump` : `--routines=0 --triggers=0 --events=0`.

  Lors de l'utilisation du format texte délimité, un commentaire `CHANGE MASTER TO` est retourné quand vous exécutez `mysqldump`. Ce commentaire contient le nom du fichier journal maître et son emplacement. Si l'instance externe est autre que MariaDB version 10.0.2 ou supérieure, notez les valeurs pour `MASTER_LOG_FILE` et `MASTER_LOG_POS`. Vous avez besoin de ces valeurs lors de la configuration de la réplication.

```
-- Position to start replication or point-in-time recovery from
--
-- CHANGE MASTER TO MASTER_LOG_FILE='mysql-bin-changelog.000031', MASTER_LOG_POS=107;
```

  Si vous utilisez le format SQL, vous pouvez obtenir le nom du fichier journal maître et son emplacement dans l'étape 4 de la procédure : Répliquer entre votre base de données externe et la nouvelle instance de base de données Amazon RDS (p. 842). Si l'instance externe est MariaDB version 10.0.2 ou ultérieure, vous pouvez obtenir l'identifiant de transaction global à l'étape suivante.

2. Si l'instance externe que vous utilisez est MariaDB version 10.0.2 ou ultérieure, vous utilisez la réplication basée sur l'identifiant de transaction global. Exécutez `SHOW MASTER STATUS` sur l'instance MariaDB externe pour obtenir le nom du fichier journal binaire et son emplacement, puis convertissez-les en un identifiant de transaction global en exécutant `BINLOG_GTID_POS` sur l'instance MariaDB externe.

```
SELECT BINLOG_GTID_POS('binary log file name', binary log file position);
```

Notez l'identifiant de transaction global retourné, vous en aurez besoin pour configurer la réplication.

3. Compressez les données copiées afin de réduire la quantité de ressources réseau nécessaires pour copier vos données sur l'instance de base de données Amazon RDS. Notez la taille du fichier de sauvegarde ; vous avez besoin de cette information lorsque vous déterminez la taille elle-même de l'instance Amazon EC2 à créer. Lorsque vous avez terminé, compressez le fichier de sauvegarde à l'aide de GZIP ou de votre utilitaire de compression favori.
   - Pour compresser une sortie SQL, utilisez la commande suivante.

     ```
     gzip backup.sql
     ```

   - Pour compresser une sortie à texte délimité, utilisez la commande suivante.

     ```
     tar -zcvf backup.tar.gz target_directory
     ```

Créer une instance Amazon EC2 et copier la base de données compressée

La copie du fichier de sauvegarde compressé de votre base de données sur une instance Amazon EC2 nécessite moins de ressources réseau que l'exécution d'une copie directe de données non compressées entre instances de bases de données. Une fois que vos données sont dans Amazon EC2, vous pouvez les copier directement de cet emplacement vers votre instance de base de données Amazon RDS MySQL ou MariaDB. Pour pouvoir économiser sur le coût des ressources réseau, votre instance Amazon EC2 doit se trouver dans la même région AWS que votre instance de base de données Amazon RDS. Le fait d'avoir l'instance Amazon EC2 dans la même région AWS que votre instance de bases de données Amazon RDS réduit également la latence réseau pendant l'importation.

Pour créer une instance Amazon EC2 et copier vos données

1. Dans la région AWS où vous envisagez de créer l'instance de base de données RDS pour exécuter votre moteur de base de données MySQL, créez un VPC, un groupe de sécurité VPC et un sous-réseau VPC. Assurez-vous que les règles entrantes de votre groupe de sécurité VPC autorisent les adresses IP requises pour que votre application se connecte à AWS. Il peut s'agir d'une plage d'adresses IP (par

exemple, `203.0.113.0/24`) ou d'un autre groupe de sécurité VPC. Vous pouvez utiliser la Console de gestion Amazon VPC pour créer et gérer des VPC, des sous-réseaux et des groupes de sécurité. Pour plus d'informations, consultez Démarrez avec Amazon VPC dans le Guide de démarrage Amazon Virtual Private Cloud.

> **Note**
>
> Les comptes AWS plus anciens peuvent aussi lancer des instances en mode Amazon EC2-Classic. Dans ce cas, assurez-vous que les règles entrantes du groupe de sécurité de base de données de votre instance Amazon RDS autorisent l'accès à votre instance EC2-Classic à l'aide de l'adresse IP privée Amazon EC2. Pour plus d'informations, consultez Utilisation des groupes de sécurité DB (plateforme EC2-Classic) (p. 1596).

2. Ouvrez la Console de gestion Amazon EC2 et sélectionnez la région AWS qui contiendra votre instance Amazon EC2 et votre instance de bases de données Amazon RDS. Lancez une instance Amazon EC2 à l'aide du VPC, du sous-réseau et du groupe de sécurité que vous avez créés à l'étape 1. Vérifiez que vous sélectionnez un type d'instance avec un stockage suffisant pour le fichier de sauvegarde de votre base de données une fois qu'il est décompressé. Pour plus d'informations sur les instances Amazon EC2, consultez Démarrez avec les instances Amazon EC2 Linux dans le Guide de l'utilisateur Amazon Elastic Compute Cloud pour Linux.
3. Pour vous connecter à votre instance de base de données Amazon RDS à partir de votre instance Amazon EC2, vous devez modifier votre groupe de sécurité VPC et ajouter une règle de trafic entrant en spécifiant l'adresse IP privée de votre instance EC2. L'adresse IP privée se trouve sous l'onglet Détails du volet Instance de la fenêtre de la console EC2. Pour modifier le groupe de sécurité VPC et ajouter une règle de trafic entrant, sélectionnez Groupes de sécurité dans le volet de navigation de la console EC2, choisissez votre groupe de sécurité et ajoutez une règle de trafic entrant pour MySQL/Aurora en spécifiant l'adresse IP privée de votre instance EC2. Pour apprendre à ajouter une règle de trafic entrant à un groupe de sécurité VPC, consultez la page Ajout et suppression de règles.
4. Copiez le fichier de sauvegarde compressé de votre base de données depuis votre système local vers votre instance Amazon EC2. Utilisez `chmod` si nécessaire pour vous assurer d'avoir l'autorisation d'écriture pour le répertoire cible de l'instance Amazon EC2. Vous pouvez utiliser `scp` ou un client SSH pour copier le fichier. Voici un exemple :

```
$ scp -r -i key pair.pem backup.sql.gz ec2-user@EC2 DNS:/target_directory/backup.sql.gz
```

> **Important**
>
> Assurez-vous de copier les données sensibles à l'aide d'un protocole de transfert réseau sécurisé.

5. Connectez-vous à votre instance Amazon EC2, puis installez les dernières mises à jour et les outils clients MySQL à l'aide des commandes suivantes :

```
sudo yum update -y
sudo yum install mysql -y
```

   Pour plus d'informations, consultez Comment vous connecter à votre instance dans le Guide de l'utilisateur Amazon Elastic Compute Cloud pour Linux.
6. Une fois connecté à votre instance Amazon EC2, décompressez le fichier de sauvegarde de votre base de données. Exemples :
   - Pour décompresser une sortie SQL, utilisez la commande suivante :

```
gzip backup.sql.gz -d
```

   - Pour décompresser une sortie texte délimité, utilisez la commande suivante :

```
tar xzvf backup.tar.gz
```

Créer une instance de base de données MySQL ou MariaDB Amazon RDS et importer les données de l'instance Amazon EC2

En créant une instance de base de données Amazon RDS MySQL ou MariaDB dans la même région AWS que votre instance Amazon EC2, vous pouvez importer le fichier de sauvegarde à partir d'EC2 plus rapidement que via Internet.

Pour créer une instance de base de données MySQL ou MariaDB Amazon RDS et importer vos données

1. Déterminez quelle classe d'instance de base de données et quelle quantité d'espace de stockage sont nécessaires pour prendre en charge la charge de travail attendue pour cette instance de base de données Amazon RDS. Dans le cadre de ce processus, décidez de l'espace suffisant et de la capacité de traitement qui conviennent à vos procédures de chargement des données, ainsi que ce qui est requis pour gérer la charge de travail de production. Vous pouvez estimer ces éléments en fonction de la taille et des ressources de la base de données source MySQL ou MariaDB. Pour plus d'informations, consultez Classes d'instances de base de données (p. 6).
2. Déterminez si les IOPS provisionnées Amazon RDS sont nécessaires pour prendre en charge les charges de travail. Le stockage des IOPS provisionnées fournit un débit rapide pour les charges de travail de traitement transactionnel en ligne (OLTP), très gourmandes en opérations d'E/S. Pour plus d'informations, consultez Stockage SSD d'I/O par seconde provisionnées (p. 33).
3. Ouvrez la console Amazon RDS . Dans le coin supérieur droit, choisissez la région AWS qui contient votre instance Amazon EC2.
4. Dans la panneau de navigation, choisissez Databases (Bases de données).
5. Choisissez Create database (Créer une base de données), puis parcourez les différentes étapes pour choisir les options de votre instance de base de données :

   a. Veillez à choisir Standard Create (Création standard).
   b. Dans la sectionEngine options (Options de moteur), choisissez MySQL ou MariaDB, selon le cas.
   c. Pour la Version, choisissez la version compatible avec votre instance MySQL source, comme suit :

- Si votre instance source est MySQL 5.1.x, l'instance de base de données Amazon RDS doit être MySQL 5.5.x.
- Si votre instance source est MySQL 5.5.x, l'instance de base de données Amazon RDS doit être MySQL 5.5.x ou version ultérieure.
- Si votre instance source est MySQL 5.6.x, l'instance de base de données Amazon RDS doit être MySQL 5.6.x ou MariaDB.
- Si votre instance source est MySQL 5.7.x, l'instance de base de données Amazon RDS doit être MySQL 5.7.x, 5.6.x ou MariaDB.
- Si votre instance source est MySQL 8.0.x, l'instance de base de données Amazon RDS doit être MySQL 8.0.x.
- Si votre instance source est MariaDB 5.1, 5.2 ou 5.3, l'instance de base de données Amazon RDS doit être MySQL 5.1.x.
- Si votre instance source est MariaDB 5.5 ou version ultérieure, l'instance de base de données Amazon RDS doit être MariaDB.

d. Dans la section Templates (Modèles), choisissez Dev/Test pour ignorer la configuration du déploiement Multi-AZ et le stockage sur volumes IOPS provisionnés.

e. Dans la section Paramètres, spécifiez l’identifiant d’instance de base de données demandé et les informations sur l'utilisateur.

f. Dans les sections DB instance class (Classe d’instance de base de données) et Storage (Stockage), spécifiez la classe d’instance de base de données et la taille de stockage alloué que vous souhaitez.

g. Dans la section Availability & durability (Disponibilité et durabilité), choisissez Do not create a standby instance (Ne pas créer d’instance de standby) pour Multi-AZ deployment (Déploiement Multi-AZ).

h. Dans la section Connectivity (Connectivité), choisissez les mêmes Virtual Private Cloud (VPC) et groupe de sécurité VPC que pour votre instance Amazon EC2. Cette approche garantit que votre instance Amazon EC2 et votre instance Amazon RDS sont visibles l'une de l'autre sur le réseau. Définissez Publicly Accessible (Accessible publiquement) sur Yes (Oui). Pour configurer la réplication avec votre base de données source comme décrit ci-après, votre instance de base de données doit être publiquement accessible.

   Utilisez les valeurs par défaut pour tous les autres paramètres de cette section.

   Dans la section Sauvegarde, définissez la période de rétention des sauvegardes avec la valeur 0 days (0 jours).

   Utilisez les valeurs par défaut pour tous les autres paramètres de cette section.

i. Ouvrez la section Additional configuration (Configuration supplémentaire) et spécifiez un Initial database name (Nom de la base de données initiale).

   Définissez la Backup retention period (Période de rétention des sauvegardes) sur 0 days (jours)

   Utilisez les valeurs par défaut pour tous les autres paramètres de cette section.

j. Choisissez Create database (Créer une base de données).

   Votre nouvelle instance de base de données apparaît dans la liste Databases (Bases de données) avec l’état Creating (Création en cours). Attendez que le Status (État) de votre instance de base de données affiche Available (Disponible).

Ne configurez pas plusieurs zones de disponibilité, la rétention des sauvegardes ou les réplicas en lecture tant que vous n'avez pas importé la sauvegarde de la base de données. Lorsque l'importation est terminée, vous pouvez définir l'option Multi-AZ et la rétention des sauvegardes comme vous le souhaitez pour l'instance de production. Pour accéder à une démonstration de la création d'une

instance de base de données, veuillez consulter Création d'une instance de base de données Amazon RDS (p. 146).

6. Vérifiez les options de configuration par défaut de l'instance de base de données Amazon RDS. Dans le volet de navigation de la console RDS, choisissez Parameter groups (Groupes de paramètres), puis sélectionnez l'icône loupe à côté du groupe de paramètres default.mysqlx.x ou default.mariadbx.x. Si ce groupe de paramètres ne dispose pas des options de configuration que vous voulez, trouvez un autre groupe qui les possède ou créez un groupe de paramètres. Pour plus d'informations sur la création d'un groupe de paramètres, consultez Utilisation de groupes de paramètres de base de données (p. 225).

   Si vous choisissez d'utiliser un autre groupe de paramètres que le groupe par défaut, associez-le à votre instance de base de données Amazon RDS. Pour de plus amples informations, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).
7. Connectez-vous à l'instance de base de données Amazon RDS comme utilisateur maître et créez les utilisateurs requis pour prendre en charge les administrateurs, les applications et les services qui doivent accéder à l'instance. Le nom d'hôte de l'instance de bases de données Amazon RDS est la valeur Point de terminaison de cette instance sans le numéro de port. Par exemple, `mysampledb.claxc2oy9ak1.us-west-2.rds.amazonaws.com`. Vous pouvez trouver la valeur du point de terminaison dans les détails de l'instance dans Amazon RDS Management Console.
8. Connectez-vous à votre instance Amazon EC2. Pour plus d'informations, consultez Comment vous connecter à votre instance dans le Guide de l'utilisateur Amazon Elastic Compute Cloud pour Linux.
9. Connectez-vous à votre instance de bases de données Amazon RDS comme hôte à distance depuis votre instance Amazon EC2 à l'aide de la commande `mysql`. Voici un exemple de.

   ```
   mysql -h host_name -P 3306 -u db_master_user -p
   ```

   Le nom d'hôte est le nom DNS du point de terminaison de l'instance de base de données Amazon RDS.
10. Dans l'invite de commande `mysql`, exécutez la commande `source` et transmettez-lui le nom du fichier de vidage de votre base de données pour charger les données dans l'instance de bases de données Amazon RDS :

    - Pour le format SQL, utilisez la commande suivante.

      ```
      mysql> source backup.sql;
      ```

    - Pour le format texte délimité, créez d'abord la base de données (s'il ne s'agit pas de la base de données par défaut que vous avez créée lors de la configuration de l'instance de base de données Amazon RDS).

      ```
      mysql> create database database_name;
      $ mysql> use database_name;
      ```

      Créez ensuite les tables.

      ```
      mysql> source table1.sql
      $ mysql> source table2.sql
      etc...
      ```

      Enfin, importez les données.

      ```
      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...
```

Pour améliorer les performances, vous pouvez exécuter ces opérations en parallèle à partir de plusieurs connexions de telle sorte que l'ensemble de vos tables soient créées et chargées simultanément.

> **Note**
>
> Si vous avez utilisé des options de mise en forme des données avec `mysqldump` lorsque vous avez initialement vidé la table, vous devez utiliser les mêmes options avec `mysqlimport` ou LOAD DATA LOCAL INFILE pour garantir une interprétation correcte du contenu du fichier de données.

11. Exécutez une simple requête SELECT sur l'une ou les deux tables de la base de données importée afin de vérifier que l'importation s'est déroulée avec succès.

> **Note**
>
> Si vous n'avez plus besoin de l'instance Amazon EC2 utilisée dans cette procédure, mettez fin à l'instance EC2 pour réduire votre utilisation des ressources Amazon AWS. Pour mettre fin à une instance EC2, consultez Arrêter une instance.

Répliquer entre votre base de données externe et la nouvelle instance de base de données Amazon RDS

Votre base de données source a probablement été mise à jour pendant la copie et le transfert des données vers l'instance de base de données MySQL ou MariaDB Amazon RDS. Ceci étant, vous pouvez utiliser la réplication pour maintenir la base de données copiée à jour par rapport à la base de données source.

> **Note**
>
> Les autorisations requises pour démarrer la réplication sur une instance de base de données Amazon RDS sont restreintes et ne sont pas disponibles pour votre utilisateur principal Amazon RDS. Pour cette raison, vous devez utiliser la commande Amazon RDS mysql.rds_set_external_master (p. 901) ou la commande

mysql.rds_set_external_master_gtid (p. 589) pour configurer la réplication, ainsi que la commande mysql.rds_start_replication (p. 913) pour démarrer la réplication entre votre base de données active et votre base de données Amazon RDS.

Pour démarrer la réplication

Précédemment, vous avez activé la journalisation binaire et défini un ID serveur unique pour votre base de données source. Maintenant, vous pouvez configurer votre instance de base de données Amazon RDS comme réplica avec votre base de données active comme instance de réplication source.

1. Dans la Console de gestion Amazon RDS, ajoutez l'adresse IP du serveur qui héberge la base de données source au groupe de sécurité du VPC de l'instance de base de données Amazon RDS. Pour plus d'informations sur la modification d'un groupe de sécurité de VPC, consultez Security Groups for Your VPC (Groupes de sécurité pour votre VPC) dans le Guide de l'utilisateur Amazon Virtual Private Cloud.

   Il se peut aussi que vous ayez besoin de configurer votre réseau local pour autoriser les connexions à partir de l'adresse IP de votre instance de base de données Amazon RDS, de telle sorte qu'elle puisse communiquer avec votre instance source. Pour obtenir l'adresse IP de l'instance de base de données Amazon RDS, utilisez la commande `host`.

   ```
   host db_instance_endpoint
   ```

   Le nom d'hôte est le nom DNS du point de terminaison de l'instance de base de données Amazon RDS. Par exemple : `myinstance.123456789012.us-east-1.rds.amazonaws.com`. Vous pouvez trouver la valeur du point de terminaison dans les détails de l'instance dans Amazon RDS Management Console.

2. A l'aide du client de votre choix, connectez-vous à l'instance source et créez un utilisateur à utiliser pour la réplication. Ce compte est utilisé exclusivement pour la réplication et doit être limité à votre domaine pour améliorer la sécurité. Voici un exemple.

   ```
   CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'password';
   ```

3. Pour l'instance source, attribuez les privilèges `REPLICATION CLIENT` et `REPLICATION SLAVE` à votre utilisateur de réplication. Par exemple, pour accorder les privilèges `REPLICATION CLIENT` et `REPLICATION SLAVE` sur toutes les bases de données à l'utilisateur « `repl_user` » de votre domaine, émettez la commande suivante.

   ```
   GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'
    IDENTIFIED BY 'password';
   ```

4. Si vous avez utilisé le format SQL pour créer votre fichier de sauvegarde et que l'instance externe n'est pas MariaDB 10.0.2 ou version ultérieure, examinez le contenu de ce fichier.

   ```
   cat backup.sql
   ```

   Le fichier inclut un commentaire `CHANGE MASTER TO` qui contient le nom du fichier journal maître et son emplacement. Ce commentaire est inclus dans le fichier de sauvegarde quand vous utilisez l'option `--master-data` avec `mysqldump`. Notez les valeurs pour `MASTER_LOG_FILE` et `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;
   ```

Si vous avez utilisé le format texte délimité pour créer votre fichier de sauvegarde et que l'instance externe n'est pas MariaDB 10.0.2 ou version ultérieure, vous devez avoir déjà les coordonnées du journal binaire de l'étape 1 de la procédure Pour créer une copie de sauvegarde de votre base de données existante (p. 835).

Si l'instance externe est MariaDB 10.0.2 ou version ultérieure, vous devez déjà avoir l'identifiant de transaction global à partir duquel démarrer la réplication de l'étape 2 de la procédure Pour créer une copie de sauvegarde de votre base de données existante (p. 835).

5. Transformez l'instance de base de données Amazon RDS en réplica. Si l'instance externe n'est pas de version MariaDB 10.0.2 ou ultérieure, connectez-vous à l'instance de bases de données Amazon RDS en tant qu'utilisateur principal et identifiez la base de données source comme instance de réplication source à l'aide de la commande mysql.rds_set_external_master (p. 901). Si vous avez un fichier de sauvegarde au format SQL, utilisez le nom et la position du fichier journal maître que vous avez déterminés dans l'étape précédente. Vous pouvez également utiliser le nom et la position que vous avez déterminés lors de la création des fichiers de sauvegarde si vous avez utilisé le format texte délimité. Voici un exemple.

```
CALL mysql.rds_set_external_master ('myserver.mydomain.com', 3306,
    'repl_user', 'password', 'mysql-bin-changelog.000031', 107, 0);
```

Si l'instance externe est de version MariaDB 10.0.2 ou ultérieure, connectez-vous à l'instance de bases de données Amazon RDS en tant qu'utilisateur maître et identifiez la base de données source comme instance de réplication source à l'aide de la commande mysql.rds_set_external_master_gtid (p. 589). Utilisez l'identifiant de transaction global de l'étape 2 de la procédure Pour créer une copie de sauvegarde de votre base de données existante (p. 835). Voici un exemple.

```
CALL mysql.rds_set_external_master_gtid ('source_server_ip_address', 3306,
 'ReplicationUser', 'password', 'GTID', 0);
```

`source_server_ip_address` est l'adresse IP de l'instance de réplication source. Une adresse DNS privée EC2 n'est pas prise en charge actuellement.

6. Sur l'instance de base de données Amazon RDS, émettez la commande mysql.rds_start_replication (p. 913) pour démarrer la réplication.

```
CALL mysql.rds_start_replication;
```

7. Sur l'instance de bases de données Amazon RDS, exécutez la commande SHOW SLAVE STATUS pour déterminer quand le réplica est à jour avec l'instance de réplication source. Les résultats de la commande `SHOW SLAVE STATUS` incluent le champ `Seconds_Behind_Master`. Lorsque le champ `Seconds_Behind_Master` renvoie 0, le réplica est à jour avec l'instance de réplication source.
8. Une fois que l'instance de base de données Amazon RDS est à jour, activez les sauvegardes automatiques de façon à pouvoir restaurer la base de données si nécessaire. Vous pouvez activer ou modifier les sauvegardes automatiques de votre instance de bases de données Amazon RDS avec la Console de gestion Amazon RDS. Pour plus d'informations, consultez Utilisation des sauvegardes (p. 317).

Rediriger votre application active vers votre instance Amazon RDS

Une fois que l'instance de base de données Amazon RDS MySQL ou MariaDB est à jour avec l'instance de réplication source, vous pouvez mettre à jour votre application active et utiliser l'instance Amazon RDS.

Pour rediriger votre application active vers votre instance de base de données MySQL ou MariaDB Amazon RDS et arrêter la réplication

1. Pour ajouter le groupe de sécurité VPC pour l'instance de base de données Amazon RDS, ajoutez l'adresse IP du serveur qui héberge l'application. Pour plus d'informations sur la modification d'un groupe de sécurité de VPC, consultez Security Groups for Your VPC (Groupes de sécurité pour votre VPC) dans le Guide de l'utilisateur Amazon Virtual Private Cloud.
2. Vérifiez que le champ `Seconds_Behind_Master` de la commande SHOW SLAVE STATUS a pour résultat 0, valeur indiquant que le réplica est à jour avec l'instance de réplication source.

```
SHOW SLAVE STATUS;
```

3. Fermez toutes les connexions à la source une fois leurs transactions terminées.
4. Mettez à jour votre application pour utiliser l'instance de base de données Amazon RDS. Cette mise à jour implique généralement de modifier les paramètres de connexion pour identifier le nom d'hôte et le port de l'instance de base de données Amazon RDS, le compte utilisateur et le mot de passe avec lesquels se connecter, et la base de données à utiliser.
5. Arrêtez la réplication pour l'instance Amazon RDS à l'aide de la commande mysql.rds_stop_replication (p. 916).

```
CALL mysql.rds_stop_replication;
```

6. Exécutez la commande mysql.rds_reset_external_master (p. 909) sur votre instance de base de données Amazon RDS pour réinitialiser la configuration de réplication de telle sorte que cette instance ne soit plus identifiée comme un réplica.

```
CALL mysql.rds_reset_external_master;
```

7. Activez des fonctions Amazon RDS supplémentaires, telles que la prise en charge de plusieurs zones de disponibilités et les réplicas en lecture. Pour plus d'informations, consultez Haute disponibilité (multi-AZ) pour Amazon RDS (p. 43) et Utilisation des réplicas en lecture (p. 275).

Note

Si vous n'avez plus besoin de l'instance Amazon RDS utilisée dans cette procédure, supprimez l'instance RDS pour réduire votre utilisation des ressources Amazon AWS. Pour supprimer une instance RDS, consultez Suppression d'une instance de base de données (p. 313).

Importation de données à partir d'une source vers une instance de base de données MySQL ou MariaDB

Si vous disposez de plus d'1 Gio de données à charger ou que vos données sont issues d'une autre source qu'une base de données MySQL ou MariaDB, nous vous recommandons de créer des fichiers plats et de les charger avec mysqlimport. mysqlimport est un autre utilitaire de ligne de commande groupé avec le logiciel client MySQL et MariaDB, dont l'objet est de charger des fichiers plats dans MySQL ou MariaDB. Pour de plus amples informations sur mysqlimport, veuillez consulter mysqlimport - Programme d'importation de données dans la documentation MySQL.

Il est également recommandé de créer des snapshots DB de l'instance de base de données Amazon RDS cible avant et après le chargement de données. Les snapshots DB Amazon RDS sont des sauvegardes complètes de votre instance de base de données qui peuvent être utilisées pour restaurer l'instance de base de données à un état connu. Lorsque vous lancez un snapshot DB, les opérations d'E/S sur votre instance de base de données sont momentanément suspendues pendant la sauvegarde de la base de données.

La création d'un instantané de base de données juste avant le chargement vous permet, si besoin est, de restaurer la base de données à son état avant le chargement. Un instantané de base de données pris immédiatement après le chargement vous évite de devoir charger les données à nouveau en cas d'incident et peut être utilisé pour faire naître de nouvelles instances de bases de données.

La liste suivante montre les étapes à suivre. Chaque étape est présentée plus en détail ci-après.

1. Créer les fichiers plats contenant les données à charger.
2. Arrêter les applications accédant à l'instance de base de données cible.
3. Créer un snapshot DB.
4. Envisager la désactivation des sauvegardes Amazon RDS automatiques.
5. Charger les données à l'aide de mysqlimport.
6. Activer à nouveau les sauvegardes automatiques.

Étape 1 : Créer les fichiers plats contenant les données à charger

Utilisez un format courant, tel que CSV (valeurs séparées par des virgules), pour stocker les données à charger. Chaque table doit avoir son propre fichier ; les données de plusieurs tables ne peuvent pas être combinées dans le même fichier. Attribuez à chaque fichier le même nom que celui de la table à laquelle il correspond. L'extension du fichier est laissée à votre libre choix. Par exemple, si le nom de la table est « ventes », le nom du fichier peut être « ventes.csv » ou « ventes.txt », mais pas « sales_01.csv ».

Chaque fois que possible, triez les données sur la clé primaire de la table en cours de chargement. Cela améliore de façon spectaculaire les temps de chargement et réduit le stockage disque requis.

Cette procédure est d'autant plus rapide et efficace que les fichiers ont une petite taille. Si la taille non compressée d'un fichier est supérieure à 1 Gio, scindez-le en plusieurs fichiers et chargez chacun d'eux séparément.

Sur les systèmes Unix (Linux inclus), utilisez la commande « split ». Par exemple, la commande suivante fractionne le fichier sales.csv en plusieurs fichiers de moins d'1 Gio, le fractionnement n'intervenant qu'aux sauts de ligne (-C 1024m). Les nouveaux fichiers sont nommés sales.part_00, sales.part_01, etc.

```
split -C 1024m -d sales.csv sales.part_
```

Des utilitaires semblables sont disponibles sur les autres systèmes d'exploitation.

Étape 2 : Arrêter les applications accédant à l'instance de base de données cible

Avant de démarrer un chargement volumineux, arrêtez toute activité d'application accédant à l'instance de base de données cible sur laquelle s'effectuera le chargement. Nous vous le conseillons vivement si d'autres sessions vont modifier les tables en cours de chargement ou celles auxquelles elles font référence. Cela réduit le risque de violation des contraintes intervenant pendant le chargement et améliore les performances de chargement. Dans le même temps, cela permet également de restaurer l'instance de base de données au point juste antérieur au chargement sans perdre les modifications effectuées par les processus non impliqués dans le chargement.

Il est vrai que cela peut ne pas être possible ou pratique. Si vous ne pouvez pas empêcher les applications d'accéder à l'instance de base de données avant le chargement, prenez les mesures nécessaires pour garantir la disponibilité et l'intégrité de vos données. Les étapes spécifiques requises varient grandement en fonction de cas d'utilisation spécifiques et des exigences du site.

Étape 3 : Créer un instantané de base de données

Si vous envisagez de charger des données dans une nouvelle instance de base de données qui ne contient aucune donnée, vous pouvez ignorer cette étape. Sinon, la création d'un instantané de bases de données de votre instance de base de données vous permet, si nécessaire, de restaurer l'instance de base de données à son état avant le chargement. Comme précédemment évoqué, lorsque vous lancez un snapshot DB, les opérations d'E/S sur votre instance de base de données sont suspendues quelques minutes pendant la sauvegarde de la base de données.

Dans l'exemple ci-dessous, nous utilisons la commande `create-db-snapshot` de l'AWS CLI pour créer un instantané de base de données de notre instance AcmeRDS et lui attribuer l'identifiant « preload ».

Pour Linux, macOS ou Unix :

```
aws rds create-db-snapshot \
    --db-instance-identifier AcmeRDS \
    --db-snapshot-identifier preload
```

Pour Windows :

```
aws rds create-db-snapshot ^
    --db-instance-identifier AcmeRDS ^
    --db-snapshot-identifier preload
```

Vous pouvez aussi utiliser la restauration de la fonctionnalité de snapshot DB pour créer des instances de bases de données de test pour des essais ou pour annuler les modifications effectuées pendant le chargement.

Gardez à l'esprit que la restauration d'une base de données à partir d'un instantané de bases de données crée une nouvelle instance de base de données qui, comme toutes les instances de base de données, possède un point de terminaison et un identifiant unique. Si vous devez restaurer l'instance de base de données sans modifier le point de terminaison, vous devez d'abord supprimer l'instance de base de données de telle sorte que le point de terminaison puisse être réutilisé.

Par exemple, pour créer une instance de base de données pour les essais ou autres tests, vous attribuez à l'instance de base de données son propre identifiant. Dans l'exemple, « AcmeRDS-2 » est l'identifiant

et nous nous connectons à l'instance de base de données à l'aide du point de terminaison associé à AcmeRDS-2.

Pour Linux, macOS ou Unix :

```
aws rds restore-db-instance-from-db-snapshot \
    --db-instance-identifier AcmeRDS-2 \
    --db-snapshot-identifier preload
```

Pour Windows :

```
aws rds restore-db-instance-from-db-snapshot ^
    --db-instance-identifier AcmeRDS-2 ^
    --db-snapshot-identifier preload
```

Pour réutiliser le point de terminaison existant, nous devons d'abord supprimer l'instance de base de données, puis attribuer le même identifiant à la base de données restaurée.

Pour Linux, macOS ou 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
```

Pour 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
```

L'exemple prend un instantané de bases de données final de l'instance de base de données avant de la supprimer. Cette action est facultative, mais recommandée.

Étape 4 : Envisager la désactivation des sauvegardes Amazon RDS automatiques

> **Warning**
>
> Ne désactivez pas les sauvegardes automatiques si vous devez conserver la possibilité d'effectuer une restauration à un instant dans le passé.

Étant donné que la désactivation des sauvegardes automatiques efface toutes les sauvegardes existantes, la restauration à un instant dans le passé n'est pas possible une fois que les sauvegardes automatiques ont été désactivées. La désactivation des sauvegardes automatiques est une optimisation des performances et n'est pas requise pour les chargements de données. Les instantanés manuels de bases de données ne sont pas affectés par la désactivation des sauvegardes automatiques. Tous les instantanés manuels de base de données existants demeurent disponibles pour la restauration.

La désactivation des sauvegardes automatiques réduit le temps de chargement de près de 25 %, ainsi que la quantité d'espace de stockage requise pendant le chargement. Si vous envisagez de charger des

données dans une nouvelle instance de base de données qui ne contient aucune donnée, la désactivation des sauvegardes constitue un moyen simple d'accélérer le chargement et d'éviter d'utiliser le stockage supplémentaire nécessaire pour les sauvegardes. Cependant, si vous envisagez d'effectuer le chargement dans une instance de base de données qui contient déjà des données, vous devez évaluer les avantages de la désactivation des sauvegardes par rapport aux conséquences qu'entraînera la perte de la possibilité d'exécuter une restauration à un instant dans le passé.

Les instances de bases de données ont les sauvegardes automatiques activées par défaut (avec une période de rétention égale à une journée). Pour désactiver les sauvegardes automatiques, vous devez définir la période de rétention des sauvegardes avec la valeur zéro. Après le chargement, vous pouvez réactiver les sauvegardes en définissant la période de rétention des sauvegardes avec une valeur différente de zéro. Pour activer ou désactiver les sauvegardes, Amazon RDS doit arrêter l'instance de base de données et la redémarrer pour activer ou désactiver la journalisation MySQL ou MariaDB.

Utilisez la commande AWS CLI `modify-db-instance` de l'interface de ligne de commande AWS pour définir la période de rétention à la valeur de zéro et pour immédiatement appliquer la modification. Comme la définition de la période de rétention à la valeur zéro nécessite un redémarrage de l'instance de base de données, attendez que le redémarrage soit terminé avant de poursuivre.

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier AcmeRDS \
    --apply-immediately \
    --backup-retention-period 0
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier AcmeRDS ^
    --apply-immediately ^
    --backup-retention-period 0
```

Vous pouvez vérifier le statut de votre instance de base de données avec la commande AWS CLI `describe-db-instances`. L'exemple montre comment afficher l'état de l'instance de base de données de l'instance de base de données AcmeRDS.

```
aws rds describe-db-instances --db-instance-identifier AcmeRDS --query "*[].
{DBInstanceStatus:DBInstanceStatus}"
```

Lorsque l'état de l'instance de base de données est `available`, vous êtes prêt à continuer.

Étape 5 : Charger les données

Choisissez l'utilitaire mysqlimport pour charger les fichiers plats dans Amazon RDS. Dans l'exemple, nous demandons à mysqlimport de charger tous les fichiers « sales » dont l'extension commence par « part_ ». Il s'agit d'un moyen pratique de charger tous les fichiers créés dans l'exemple « split ». Utilisez l'option --compress pour réduire le trafic réseau. L'option --fields-terminated-by=',' est utilisée pour les fichiers CSV et l'option --local spécifie que les données entrantes se trouvent sur le client. Comme sans l'option --local, l'instance de base de données Amazon RDS recherche les données sur l'hôte de base de données, spécifiez toujours l'option --local.

Pour Linux, macOS ou Unix :

```
mysqlimport --local \
    --compress \
    --user=username \
    --password \
```

```
    --host=hostname \
    --fields-terminated-by=',' Acme sales.part_*
```

Pour Windows :

```
mysqlimport --local ^
    --compress ^
    --user=username ^
    --password ^
    --host=hostname ^
    --fields-terminated-by=',' Acme sales.part_*
```

Pour les chargements de données très volumineux, prenez régulièrement des snapshots DB supplémentaires entre les chargements de fichiers et notez les fichiers chargés. Si un problème se produit, vous pouvez sans peine reprendre à partir du point du dernier snapshot DB et éviter ainsi les rechargements très longs.

Étape 6 : Activer les sauvegardes automatiques Amazon RDS

Une fois le chargement terminé, réactivez les sauvegardes automatiques Amazon RDS en redéfinissant la période de rétention des sauvegardes à la valeur qui était la sienne avant le chargement. Comme noté précédemment, Amazon RDS redémarre l'instance de base de données. Par conséquent, préparez-vous à une brève interruption de service.

Dans l'exemple, nous utilisons la commande modify-db-instance de l'AWS CLI pour activer les sauvegardes automatiques pour l'instance de base de données AcmeRDS et définir la période de rétention sur 1 journée.

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier AcmeRDS \
    --backup-retention-period 1 \
    --apply-immediately
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier AcmeRDS ^
    --backup-retention-period 1 ^
    --apply-immediately
```

Utilisation de la réplication MySQL dans Amazon RDS

Vous utilisez généralement des réplicas en lecture pour configurer la réplication entre instances de base de données Amazon RDS. Pour obtenir des informations générales sur les réplicas en lecture, veuillez consulter Utilisation des réplicas en lecture (p. 275). Pour obtenir des informations spécifiques sur l'utilisation des réplicas en lecture dans Amazon RDS MySQL, veuillez consulter Utilisation de réplicas en lecture MySQL (p. 851).

Vous pouvez utiliser des identifiants de transaction globaux (GTID) pour la réplication avec Amazon RDS MySQL. Pour plus d'informations, consultez Utilisation de la réplication basée sur des identifiants de transaction globaux (GTID) pour Amazon RDS MySQL (p. 857).

Vous pouvez également configurer la réplication entre une instance de base de données Amazon RDS MySQL et une instance MySQL ou une instance MariaDB externe à Amazon RDS. Pour plus d'informations sur la réplication de configuration avec une source externe, consultez Réplication avec une instance MySQL ou MariaDB s'exécutant à l'extérieur d'Amazon RDS (p. 863).

Pour chacune de ces options de réplication, vous pouvez utiliser la réplication basée sur les lignes, basée sur les instructions ou mixte. La réplication basée sur les lignes réplique uniquement les lignes modifiées à la suite d'une instruction SQL. La réplication basée sur les instructions réplique l'ensemble de l'instruction SQL. La réplication mixte utilise la réplication basée sur les instructions chaque fois que possible, mais bascule vers la réplication basée sur les lignes lorsque des instructions SQL présentant un risque pour la réplication basée sur les instructions sont exécutées. La réplication mixte est recommandée dans la plupart des cas. Le format de journalisation binaire de l'instance de base de données détermine si la réplication est basée sur les lignes, basée sur les instructions ou mixte. Pour plus d'informations sur la définition du format de journalisation binaire, consultez la section Format de journalisation binaire (p. 513).

> Note
>
> Vous pouvez configurer la réplication de sorte à importer des bases de données d'une instance MySQL ou MariaDB extérieure à Amazon RDS, ou à exporter des bases de données vers de telles instances. Pour plus d'informations, consultez Importation de données vers une instance de base de données MySQL ou MariaDB Amazon RDS avec un temps réduit (p. 832) et Exportation de données à partir d'une instance DB MySQL grâce à la réplication (p. 869).

Rubriques

- Utilisation de réplicas en lecture MySQL (p. 851)
- Utilisation de la réplication basée sur des identifiants de transaction globaux (GTID) pour Amazon RDS MySQL (p. 857)
- Réplication avec une instance MySQL ou MariaDB s'exécutant à l'extérieur d'Amazon RDS (p. 863)

Utilisation de réplicas en lecture MySQL

Cette section contient des informations spécifiques sur l'utilisation des réplicas en lecture dans Amazon RDS MySQL. Pour obtenir des informations générales sur les réplicas en lecture et des instructions pour les utiliser, veuillez consulter Utilisation des réplicas en lecture (p. 275).

Rubriques

- Configuration de réplicas en lecture avec MySQL (p. 851)
- Configuration de la réplication retardée avec MySQL (p. 852)
- Mises à jour de réplicas en lecture avec MySQL (p. 855)
- Déploiements multi-AZ de réplicas en lecture avec MySQL (p. 855)
- Surveillance des réplicas en lecture MySQL (p. 855)
- Démarrage et arrêt de la réplication avec des réplicas en lecture MySQL (p. 856)
- Résolution d'un problème de réplica en lecture MySQL (p. 856)

Configuration de réplicas en lecture avec MySQL

Avant qu'une instance de base de données MySQL puisse être utilisée comme source de réplication, vous devez activer les sauvegardes automatiques sur l'instance de base de données source. Pour cela, vous devez définir la période de rétention des sauvegardes sur une valeur autre que 0. Cette exigence s'applique également à un réplica en lecture qui serait l'instance de base de données source d'un autre réplica en lecture. Les sauvegardes automatiques sont prises en charge uniquement pour les réplicas en lecture exécutant une version de MySQL 5.6 ou une version ultérieure. Vous pouvez configurer la réplication en fonction des coordonnées des journaux binaires pour une instance de base de données MySQL.

Dans Amazon RDS MySQL 5.7.23 et les versions MySQL 5.7 ultérieures, vous pouvez configurer la réplication avec des identifiants de transaction globaux (GTID). Pour plus d'informations, consultez Utilisation de la réplication basée sur des identifiants de transaction globaux (GTID) pour Amazon RDS MySQL (p. 857).

Vous pouvez créer jusqu'à cinq réplicas en lecture à partir d'une seule instance de base de données. Pour que la réplication fonctionne de façon efficace, chaque réplica en lecture doit avoir la même quantité de ressources de calcul et de stockage que l'instance de base de données source. Si vous mettez à l'échelle l'instance de base de données source, faites-le également pour les réplicas en lecture.

Si un réplica en lecture exécute une version de MySQL 5.6 ou ultérieure, vous pouvez la spécifier comme instance de base de données source pour un autre réplica en lecture. Par exemple, vous pouvez créer ReadReplica1 from MyDBInstance, puis ReadReplica2 à partir de ReadReplica1. Les mises à jour effectuées sur InstanceDB sont répliquées sur ReplicaEnLecture1 puis répliquées de ReplicaEnLecture1 vers ReplicaEnLecture2. Vous ne pouvez pas avoir plus de quatre instances impliquées dans une chaîne de réplication. Par exemple, vous pouvez créer ReadReplica1 à partir de MySourceDBInstance, ReadReplica2 à partir de ReadReplica1, puis ReadReplica3 à partir de ReadReplica2, mais vous ne pouvez pas créer ReadReplica4 à partir de ReadReplica3.

Si vous procédez à la promotion d'un réplica en lecture MySQL qui réplique à son tour vers d'autres réplicas en lecture, ces réplicas en lecture restent actifs. Considérez un exemple dans lequel InstanceDB1 réplique vers InstanceDB2, et InstanceDB2 réplique vers InstanceDB3. Si vous promouvez InstanceDB2, la réplication d'InstanceDB1 vers InstanceDB2 n'intervient plus, mais InstanceDB2 continue à répliquer vers InstanceDB3.

Pour activer les sauvegardes automatiques sur un réplica en lecture pour Amazon RDS MySQL version 5.6 ou ultérieure, commencez par créer le réplica en lecture. Modifiez ensuite le réplica en lecture pour activer les sauvegardes automatiques.

Vous pouvez exécuter plusieurs actions de création ou de suppression simultanées pour les réplicas en lecture qui référencent la même instance de base de données source. Pour cela, restez dans la limite de cinq réplicas en lecture pour chaque instance source.

Un réplica en lecture d'une instance de base de données MySQL ne peut pas utiliser une version de moteur de base de données inférieure à son instance de base de données source.

Préparation des instances de base de données MySQL qui utilisent MyISAM

Si votre instance de base de données MySQL utilise un moteur non transactionnel tel que MyISAM, vous devez effectuer les étapes suivantes pour configurer correctement votre réplica en lecture. Ces étapes sont nécessaires pour vous assurer que le réplica en lecture dispose d'une copie cohérente de vos données. Ces étapes ne sont pas nécessaires si toutes vos tables utilisent un moteur transactionnel comme InnoDB.

1. Arrêtez toutes les opérations DML (Data Manipulation Language) et DDL (Data Definition Language) sur les tables non transactionnelles dans l'instance de bases de données source et attendez qu'elles se terminent. Les instructions SELECT peuvent continuer à fonctionner.
2. Videz et verrouillez les tables dans l'instance de bases de données source.
3. Créez le réplica en lecture en suivant l'une des méthodes présentées dans les sections suivantes.
4. Vérifiez l'avancement de la création du réplica en lecture en utilisant, par exemple, l'opération d'API `DescribeDBInstances`. Une fois que le réplica en lecture est disponible, déverrouillez les tables de l'instance de base de données source et reprenez les opérations de base de données normales.

Configuration de la réplication retardée avec MySQL

Vous pouvez utiliser la réplication retardée comme stratégie pour la reprise après sinistre. Grâce à elle, vous spécifiez le temps minimal, en secondes, à utiliser pour retarder la réplication à partir de la base de données principale vers le réplica en lecture. En cas de sinistre, par exemple la suppression accidentelle d'une table, vous appliquez la procédure suivante pour reprendre rapidement après le sinistre :

- Arrêtez la réplication vers le réplica en lecture avant que lui soit envoyée la modification qui a provoqué le sinistre.

  Utilisez la procédure stockée mysql.rds_stop_replication (p. 916) pour arrêter la réplication.
- Arrêtez la réplication et précisez qu'elle doit s'arrêter automatiquement à une position donnée dans un fichier journal.

  Vous indiquez une position juste avant le sinistre grâce à la procédure stockée mysql.rds_start_replication_until (p. 914).
- Effectuez la promotion du réplica en lecture pour qu'il devienne la nouvelle instance de base de données source, en suivant les instructions figurant dans Promotion d'un réplica en lecture en instance de bases de données autonome (p. 282).

  Note

  - Dans Amazon RDS MySQL 5.7, la réplication retardée est prise en charge pour MySQL 5.7.22 et versions ultérieures. Dans Amazon RDS MySQL 5.6, la réplication retardée est prise en charge pour MySQL 5.6.40 et versions ultérieures. La réplication retardée n'est pas prise en charge dans Amazon RDS MySQL 8.0.
  - Utilisez des procédures stockées pour configurer la réplication retardée. Vous ne pouvez pas configurer la réplication retardée avec la AWS Management Console, l'AWS CLI ou l'API Amazon RDS.
  - Dans Amazon RDS MySQL 5.7.23 et les versions MySQL 5.7 ultérieures, vous pouvez utiliser une réplication basée sur des identifiants de transaction globaux (GTID) dans une configuration de réplication retardée. Si vous utilisez une réplication basée sur des identifiants de transaction globaux (GTID), utilisez la procédure stockée mysql.rds_start_replication_until_gtid (p. 915) au lieu de la procédure stockée mysql.rds_start_replication_until (p. 914). Pour en savoir plus sur les réplications basées sur des identifiants de transaction globaux (GTID), consultez Utilisation de la réplication basée sur des identifiants de transaction globaux (GTID) pour Amazon RDS MySQL (p. 857).

Rubriques

- Configuration de la réplication retardée pendant la création du réplica en lecture (p. 853)
- Modification de la réplication retardée pour un réplica en lecture existant (p. 854)
- Définition d'une position où arrêter la réplication vers un réplica en lecture (p. 854)

Configuration de la réplication retardée pendant la création du réplica en lecture

Pour configurer la réplication retardée pour tout réplica en lecture à venir créé à partir d'une instance de base de données, exécutez la procédure stockée mysql.rds_set_configuration (p. 921) avec le paramètre `target delay`.

Pour configurer la réplication retardée pendant la création du réplica en lecture

1. À l'aide d'un client MySQL, connectez-vous à l'instance de base de données MySQL qui constituera la source des réplicas en lecture en tant qu'utilisateur principal.
2. Exécutez la procédure stockée mysql.rds_set_configuration (p. 921) avec le paramètre `target delay`.

   Par exemple, exécutez la procédure stockée suivante pour indiquer que la réplication est retardée d'au moins une heure (3 600 secondes) pour tout réplica en lecture créé à partir de l'instance de base de données actuelle.

```
call mysql.rds_set_configuration('target delay', 3600);
```

> **Note**
>
> Une fois cette procédure stockée exécutée, tout réplica en lecture que vous créez en utilisant l'AWS CLI ou l'API Amazon RDS est configuré avec la réplication retardée du nombre de secondes spécifié.

Modification de la réplication retardée pour un réplica en lecture existant

Pour modifier la réplication retardée pour un réplica en lecture existant, exécutez la procédure stockée mysql.rds_set_source_delay (p. 912).

Pour modifier la réplication retardée pour un réplica en lecture existant

1. En utilisant un client MySQL, connectez-vous au réplica en lecture en tant qu'utilisateur principal.
2. Utilisez la procédure stockée mysql.rds_stop_replication (p. 916) pour arrêter la réplication.
3. Exécutez la procédure stockée mysql.rds_set_source_delay (p. 912).

   Par exemple, exécutez la procédure stockée suivante pour indiquer que la réplication vers le réplica en lecture est retardée d'au moins une heure (3 600 secondes).

   ```
   call mysql.rds_set_source_delay(3600);
   ```

4. Utilisez la procédure stockée mysql.rds_start_replication (p. 913) pour lancer la réplication.

Définition d'une position où arrêter la réplication vers un réplica en lecture

Après avoir arrêté la réplication vers le réplica en lecture, vous pouvez démarrer la réplication, puis l'arrêter à la position spécifiée dans le fichier journal binaire en utilisant la procédure stockée mysql.rds_start_replication_until (p. 914).

Pour démarrer la réplication vers un réplica en lecture et l'arrêter à une position donnée

1. En utilisant un client MySQL, connectez-vous à l'instance de base de données MySQL source en tant qu'utilisateur principal.
2. Exécutez la procédure stockée mysql.rds_start_replication_until (p. 914).

   L'exemple suivant lance la réplication et réplique les modifications jusqu'à ce qu'il atteigne la position `120` dans le fichier journal binaire `mysql-bin-changelog.000777`. Dans un scénario de reprise après sinistre, nous supposons que cette position `120` est juste avant le sinistre.

   ```
   call mysql.rds_start_replication_until(
     'mysql-bin-changelog.000777',
     120);
   ```

La réplication s'arrête automatiquement lorsque le point d'arrêt est atteint. L'événement RDS suivant est généré : `Replication has been stopped since the replica reached the stop point specified by the rds_start_replication_until stored procedure`

Une fois la réplication arrêtée, dans un scénario de reprise après sinistre, vous pouvez Promotion d'un réplica en lecture en instance de bases de données autonome (p. 282) promouvoir le réplica en lecture pour qu'il devienne la nouvelle instance de base de données source. Pour de plus amples informations sur

la promotion du réplica en lecture, veuillez consulter Promotion d'un réplica en lecture en instance de bases de données autonome (p. 282).

Mises à jour de réplicas en lecture avec MySQL

Les réplicas en lecture sont conçus pour prendre en charge les requêtes de lecture, mais vous pouvez avoir besoin de mises à jour ponctuelles. À titre d'exemple, vous pouvez avoir besoin d'ajouter un index, pour optimiser les types spécifiques de requêtes qui accèdent au réplica. Vous pouvez autoriser les mises à jour en affectant au paramètre `read_only` la valeur `0` dans le groupe de paramètres de base de données pour le réplica en lecture. Soyez prudent lors de la désactivation de la lecture seule sur un réplica en lecture car cela peut poser des problèmes si le réplica en lecture devient incompatible avec l'instance de base de données source. Remplacez la valeur du paramètre `read_only` par `1` dès que possible.

Déploiements multi-AZ de réplicas en lecture avec MySQL

Vous pouvez créer un réplica en lecture à partir de déploiements d'instance de base de données mono-AZ ou multi-AZ. Vous utilisez des déploiements multi-AZ pour améliorer la durabilité et la disponibilité des données critiques, mais vous ne pouvez pas utiliser une instance secondaire multi-AZ pour servir les requêtes en lecture seule. À la place, vous pouvez créer des réplicas en lecture à partir d'instances de base de données multi-AZ à trafic élevé pour décharger les requêtes en lecture seule. Si l'instance source d'un déploiement multi-AZ bascule vers l'instance secondaire, tous les réplicas en lecture associés se mettent automatiquement à utiliser l'instance secondaire (désormais principale) comme source de réplication. Pour plus d'informations, consultez Haute disponibilité (multi-AZ) pour Amazon RDS (p. 43).

Vous pouvez désormais créer un réplica en lecture en tant qu'instance de base de données multi-AZ. Amazon RDS crée une instance de secours de votre réplica dans une autre zone de disponibilité pour la prise en charge du basculement pour le réplica. La création de votre réplica en lecture en tant qu'instance de base de données multi-AZ est indépendante du fait que la base de données source soit ou non une instance de base de données multi-AZ.

> Note
>
> Pour créer un réplica en lecture en tant qu'instance de base de données multi-AZ, l'instance de base de données doit être MySQL 5.6 ou une version ultérieure.

Surveillance des réplicas en lecture MySQL

Pour les réplicas en lecture MySQL, vous pouvez surveiller le retard de réplication dans Amazon CloudWatch en consultant la métrique Amazon RDS `ReplicaLag`. La métrique `ReplicaLag` contient la valeur du champ `Seconds_Behind_Master` de la commande `SHOW SLAVE STATUS`.

Les causes courantes du retard de réplication pour MySQL sont les suivantes :

- Une indisponibilité du réseau.
- L'écriture dans des tables avec des index différents sur un réplica en lecture. Si le paramètre `read_only` est défini sur `0` sur le réplica en lecture, la réplication peut être rompue si le réplica en lecture devient incompatible avec l'instance de base de données source. Une fois que vous avez effectué les tâches de maintenance sur le réplica en lecture, nous vous recommandons de définir à nouveau le paramètre `read_only` sur `1`.
- Utilisation d'un moteur de stockage non transactionnel tel que MyISAM. La réplication est uniquement prise en charge pour le moteur de stockage InnoDB sur MySQL.

Lorsque la métrique `ReplicaLag` atteint 0, le réplica a rattrapé l'instance de bases de données source. Si la métrique `ReplicaLag` retourne -1, la réplication n'est actuellement pas active. `ReplicaLag`= -1 est équivalent à `Seconds_Behind_Master` = `NULL`.

Démarrage et arrêt de la réplication avec des réplicas en lecture MySQL

Vous pouvez arrêter et redémarrer le processus de réplication sur une instance de base de données Amazon RDS en appelant les procédures stockées système mysql.rds_stop_replication (p. 916) et mysql.rds_start_replication (p. 913). Vous pouvez procéder ainsi lors d'une réplication entre deux instances Amazon RDS pour des opérations de longue durée, telles que la création d'un grand index. Vous devez également arrêter et démarrer la réplication lors de l'importation ou de l'exportation de bases de données. Pour de plus amples informations, veuillez consulter Importation de données vers une instance de base de données MySQL ou MariaDB Amazon RDS avec un temps réduit (p. 832) et Exportation de données à partir d'une instance DB MySQL grâce à la réplication (p. 869).

Si la réplication est arrêtée pendant plus de 30 jours consécutifs, manuellement ou en raison d'une erreur de réplication, Amazon RDS met fin à la réplication entre l'instance de base de données source et tous les réplicas en lecture. Cela permet d'éviter l'augmentation des besoins en stockage sur l'instance de bases de données source et d'importants délais de basculement. L'instance de base de données du réplica en lecture est toujours disponible. En revanche, la réplication ne peut pas être reprise, car les journaux binaires requis par le réplica en lecture sont supprimés de l'instance de base de données source une fois la réplication terminée. Vous pouvez créer un nouveau réplica en lecture pour l'instance de base de données source afin de rétablir la réplication.

Résolution d'un problème de réplica en lecture MySQL

Dans certains cas, pour les instances de base de données, les réplicas en lecture présentent des erreurs ou des incohérences de données entre le réplica en lecture et son instance de base de données source. Ce problème survient quand des événements de journaux binaires ou des journaux redo InnoDB ne sont pas vidés lors d'une panne du réplica en lecture ou de l'instance de base de données source. Dans ces situations, supprimez et recréez manuellement les réplicas en lecture. Vous pouvez réduire la probabilité que cela se produise dans MySQL 5.5 en définissant les variables dynamiques suivantes : `sync_binlog=1`, `innodb_flush_log_at_trx_commit=1` et `innodb_support_xa=1`. Ces paramètres peuvent réduire les performances. Testez donc leur impact avant d'implémenter les modifications dans un environnement de production. Pour MySQL 5.5, `sync_binlog` utilise la valeur `0` par défaut, mais dans MySQL 5.6 et les versions ultérieures, ces problèmes se produisent moins souvent dans la mesure où ces paramètres sont tous définis sur les valeurs recommandées par défaut.

Les technologies de réplication pour MySQL sont asynchrones. Par conséquent, des augmentations `BinLogDiskUsage` sur l'instance de base de données source et `ReplicaLag` sur le réplica en lecture sont prévisibles. Par exemple, un volume élevé d'opérations d'écriture sur l'instance de bases de données source peut se produire en parallèle. Tandis que les opérations d'écritures sur le réplica en lecture sont sérialisées à l'aide d'un seul thread d'E/S, ce qui peut conduire à un retard entre l'instance source et le réplica. Pour de plus amples informations sur les réplicas en lecture seule dans la documentation MySQL, veuillez consulter Détails d'implémentation de la réplication.

Vous pouvez effectuer plusieurs opérations pour réduire le retard entre les mises à jour d'une instance de base de données source et les mises à jour suivantes appliquées au réplica en lecture, telles que les opérations suivantes :

- Dimensionnement d'un réplica en lecture pour qu'il ait une taille de stockage et une classe d'instance de base de données comparables à celles de l'instance de base de données source.
- Garantie que les réglages des paramètres dans les groupes de paramètres de base de données utilisés par l'instance de base de données source et le réplica en lecture sont compatibles. Pour obtenir plus d'informations et un exemple, reportez-vous à la présentation du paramètre `max_allowed_packet`, plus loin dans cette section.

Amazon RDS surveille l'état de réplication de vos réplicas en lecture et met à jour le champ `Replication State` de l'instance du réplica en lecture avec la valeur `Error` si la réplication s'arrête pour une raison

quelconque. Par exemple, dans le cas de requêtes DML exécutées sur votre réplica en lecture qui sont en conflit avec les mises à jour effectuées sur l'instance de base de données source.

Vous pouvez passer en revue les détails de l'erreur associée et déclenchée par le moteur MySQL, en consultant le champ `Replication Error`. Des événements indiquant l'état du réplica en lecture sont également générés, y compris RDS-EVENT-0045 (p. 474), RDS-EVENT-0046 (p. 474) et RDS-EVENT-0047 (p. 472). Pour plus d'informations sur les événements et l'abonnement aux événements, consultez Utilisation de la notification d'événement Amazon RDS (p. 467). Si un message d'erreur MySQL est renvoyé, passez en revue le numéro de l'erreur dans la documentation sur les messages d'erreur MySQL.

Un problème courant susceptible de causer des erreurs de réplication se pose lorsque la valeur du paramètre `max_allowed_packet` d'un réplica en lecture est inférieure à celle du paramètre `max_allowed_packet` de l'instance de base de données source. Le paramètre `max_allowed_packet` est un paramètre personnalisé que vous pouvez définir dans un groupe de paramètres de base de données. Vous utilisez `max_allowed_packet` pour spécifier la taille maximale du code DML qui peut être exécuté sur la base de données. Dans certains cas, la valeur `max_allowed_packet` du groupe de paramètres de base de données associé à un réplica en lecture est inférieure à la valeur `max_allowed_packet` du groupe de paramètres de base de données associé à l'instance de base de données source. Dans ces cas, le processus de réplication peut lancer l'erreur `Packet bigger than 'max_allowed_packet' bytes` et arrêter la réplication. Pour corriger cette erreur, faites en sorte que l'instance de base de données source et le réplica en lecture utilisent des groupes de paramètres de base de données avec les mêmes valeurs pour le paramètre `max_allowed_packet`.

Voici d'autres situations courantes susceptibles de causer des erreurs de réplication :

- Écriture sur les tables d'un réplica en lecture. Dans certains cas, vous pouvez créer des index sur un réplica en lecture différents des index sur l'instance de base de données source. Vous devez alors définir le paramètre `read_only` sur `0` pour créer les index. Si vous écrivez dans des tables sur le réplica en lecture, cela peut interrompre la réplication si le réplica en lecture devient incompatible avec l'instance de base de données source. Une fois que vous avez effectué les tâches de maintenance sur le réplica en lecture, nous vous recommandons de définir à nouveau le paramètre `read_only` sur `1`.
- Utilisation d'un moteur de stockage non transactionnel tel que MyISAM. Les réplicas en lecture nécessitent un moteur de stockage transactionnel. La réplication est uniquement prise en charge pour le moteur de stockage InnoDB sur MySQL.
- Utilisation de requêtes non déterministes non sécurisées telles que `SYSDATE()`. Pour de plus amples informations, veuillez consulter Détermination d'instructions sécurisées et non sécurisées dans la journalisation binaire.

Si vous décidez que vous pouvez ignorer une erreur en toute sécurité, vous pouvez suivre la procédure décrite dans la section Ignorer une erreur de réplication (p. 881). Sinon, vous pouvez d'abord supprimer le réplica en lecture. Vous créez ensuite une instance à l'aide du même identifiant d'instance de base de données, de telle sorte que le point de terminaison demeure le même que celui de votre ancien réplica en lecture. Si une erreur de réplication est corrigée, le champ `Replication State` prend la valeur replicating (réplication en cours).

Utilisation de la réplication basée sur des identifiants de transaction globaux (GTID) pour Amazon RDS MySQL

La présente section vous apprend à utiliser les identifiants de transaction globaux (GTID) avec la réplication des journaux binaires entre les instances de base de données Amazon RDS MySQL.

Si vous utilisez la réplication des journaux binaires, mais que vous ne maîtrisez pas la réplication GTID avec MySQL, veuillez consulter la page Replication with Global Transaction Identifiers dans la documentation MySQL.

> **Note**
>
> La réplication GTID est prise en charge pour RDS MySQL version 5.7.23 et pour les versions ultérieures de MySQL 5.7. Toutes les instances de base de données RDS MySQL dans une configuration de réplication doivent respecter cette exigence. La réplication GTID n'est pas prise en charge pour RDS MySQL 5.5, 5.6 ou 8.0.

Rubriques

- Présentation des identifiants de transaction globaux (GTID) (p. 858)
- Paramètres pour la réplication basée sur des identifiants de transaction globaux (GTID) (p. 859)
- Configuration de la réplication basée sur des identifiants de transaction globaux (GTID) pour les nouveaux réplicas en lecture (p. 860)
- Configuration de la réplication basée sur des identifiants de transaction globaux (GTID) pour des réplicas en lecture existants. (p. 860)
- Désactivation de la réplication basée sur des identifiants de transaction globaux (GTID) pour une instance de base de données RDS MySQL avec des réplicas en lecture (p. 862)

> **Note**
>
> Pour de plus amples informations sur la configuration de la réplication GTID avec une base de données externe, veuillez consulter Réplication avec une instance MySQL ou MariaDB s'exécutant à l'extérieur d'Amazon RDS (p. 863).

Présentation des identifiants de transaction globaux (GTID)

Les identifiants de transaction globaux (GTID) sont des identifiants uniques générés pour des transactions MySQL validées. Vous pouvez utiliser ces identifiants pour simplifier et faciliter la résolution des problèmes liés à la réplication des journaux binaires.

MySQL utilise deux types différents de transactions pour la réplication des journaux binaires :

- Transactions GTID – Transactions identifiées par un identifiant de transaction global (GTID).
- Transactions anonymes – Transactions auxquelles aucun identifiant de transaction global (GTID) n'est associé.

Dans une configuration de réplication, les GTID sont uniques parmi toutes les instances de base de données. Les GTID simplifient la configuration de réplication dans la mesure où, lorsque vous les utilisez, vous n'avez pas à vous référer aux positions des fichiers journaux. Les GTID facilitent également le suivi des transactions répliquées et déterminent si l'instance source et les réplicas sont cohérents.

Vous pouvez utiliser la réplication GTID pour répliquer des données avec les réplicas en lecture MySQL d'Amazon RDS ou avec une base de données MySQL externe. Pour les réplicas en lecture RDS MySQL, vous pouvez configurer une réplication GTID lorsque vous créez de nouveaux réplicas en lecture, ou convertir des réplicas en lecture existants pour utiliser la réplication GTID.

Vous pouvez également utiliser la réplication GTID dans une configuration de réplication retardée avec RDS MySQL. Pour plus d'informations, consultez Configuration de la réplication retardée avec MySQL (p. 852).

Paramètres pour la réplication basée sur des identifiants de transaction globaux (GTID)

Utilisez les paramètres suivants pour configurer une réplication GTID.

Paramètre	Valeurs valides	Description
`gtid_mode`	`OFF`, `OFF_PERMISSIVE`, `ON_PERMISSIVE`, `ON`	`OFF` spécifie que les nouvelles transactions sont des transactions anonymes (et n'ont donc pas de GTID), et qu'une transaction doit être anonyme pour être répliquée. `OFF_PERMISSIVE` spécifie que les nouvelles transactions sont des transactions anonymes, mais que toutes les transactions peuvent être répliquées. `ON_PERMISSIVE` spécifie que les nouvelles transactions sont des transactions GTID, mais que toutes les transactions peuvent être répliquées. `ON` spécifie que les nouvelles transactions sont des transactions GTID, et qu'une transaction doit être une transaction GTID pour être répliquée.
`enforce_gtid_consistency`	`OFF`, `ON`, `WARN`	`OFF` autorise les transactions à enfreindre la cohérence GTID. `ON` interdit aux transactions d'enfreindre la cohérence GTID. `WARN` autorise les transactions à enfreindre la cohérence GTID mais génère un avertissement lorsqu'une infraction se produit.

> **Note**
>
> Dans AWS Management Console, le paramètre `gtid_mode` apparaît sous la forme `gtid-mode`.

Pour la réplication GTID, utilisez ces paramètres pour le groupe de paramètres de votre instance de base de données ou de votre réplica en lecture :

- `ON` et `ON_PERMISSIVE` s'appliquent uniquement à la réplication sortante à partir d'une instance de base de données RDS ou d'un cluster Aurora MySQL. Ces deux valeurs forcent votre instance de base de données RDS ou votre cluster de base de données Aurora à utiliser des identifiants de transaction globaux (GTID) pour les transactions répliquées sur une base de données externe. `ON` exige que la base de données externe utilise également la réplication GTID. `ON_PERMISSIVE` rend la réplication GTID facultative sur la base de données externe.
- S'il est défini, `OFF_PERMISSIVE` indique que vos instances de base de données RDS ou votre cluster de base de données Aurora peuvent accepter la réplication entrante à partir d'une base de données externe, que cette dernière utilise la réplication GTID ou non.
- S'il est défini, `OFF` indique que vos instances de base de données RDS ou votre cluster de base de données Aurora acceptent uniquement la réplication entrante à partir de bases de données externes qui n'utilisent pas la réplication GTID.

Pour de plus amples informations sur les groupes de paramètres, veuillez consulter Utilisation de groupes de paramètres de base de données (p. 225).

Configuration de la réplication basée sur des identifiants de transaction globaux (GTID) pour les nouveaux réplicas en lecture

Lorsque la réplication GTID est activée pour une instance de base de données RDS MySQL, elle est configurée automatiquement pour les réplicas en lecture de l'instance de base de données.

Pour activer la réplication GTID pour des nouveaux réplicas en lecture

1. Assurez-vous que le groupe de paramètres associé à l'instance de base de données contient la configuration de paramètres suivante :

   - `gtid_mode` – `ON` ou `ON_PERMISSIVE`
   - `enforce_gtid_consistency` – `ON`

   Pour plus d'informations sur la définition des paramètres de configuration à l'aide de groupes de paramètres, veuillez consulter Utilisation de groupes de paramètres de base de données (p. 225).
2. Si vous modifiez le groupe de paramètres de l'instance de base de données, redémarrez celle-ci. Pour en savoir plus à ce sujet, veuillez consulter Redémarrage d'une instance de base de données (p. 272).
3. Créez un ou plusieurs réplicas en lecture de l'instance de base de données. Pour en savoir plus à ce sujet, veuillez consulter Création d'un réplica en lecture (p. 280).

Amazon RDS tente d'établir une réplication GTID entre l'instance de base de données MySQL et les réplicas en lecture à l'aide du paramètre `MASTER_AUTO_POSITION`. En cas d'échec, Amazon RDS utilise les positions de fichiers journaux pour la réplication avec les réplicas en lecture. Pour de plus amples informations sur le paramètre `MASTER_AUTO_POSITION`, veuillez consulter la page GTID Auto-Positioning dans la documentation MySQL.

Configuration de la réplication basée sur des identifiants de transaction globaux (GTID) pour des réplicas en lecture existants.

Pour une instance de base de données RDS MySQL existante avec des réplicas en lecture qui n'utilise pas la réplication GTID, vous pouvez configurer la réplication GTID entre l'instance de base de données et les réplicas en lecture.

Pour activer la réplication GTID pour des réplicas en lecture existants

1. Si l'instance de base de données ou un réplica en lecture utilise RDS MySQL version 5.7.22 ou versions antérieures, mettez à niveau l'instance de base de données ou le réplica en lecture. Effectuez une mise à niveau vers RDS MySQL version 5.7.23 ou une version ultérieure de MySQL 5.7.

   Pour plus d'informations, consultez Mise à niveau du moteur de base de données MySQL (p. 804).
2. (Facultatif) Réinitialisez les paramètres GTID et testez le comportement de l'instance de base de données et des réplicas en lecture :

   a. Assurez-vous que le groupe de paramètres associé à l'instance de base de données et à chaque réplica en lecture contient le paramètre `enforce_gtid_consistency` défini sur `WARN`.

      Pour plus d'informations sur la définition des paramètres de configuration à l'aide de groupes de paramètres, veuillez consulter Utilisation de groupes de paramètres de base de données (p. 225).
   b. Si vous modifiez le groupe de paramètres de l'instance de base de données, redémarrez celle-ci. Si vous modifiez le groupe de paramètres pour un réplica en lecture, redémarrez celui-ci.

Pour plus d'informations, consultez Redémarrage d'une instance de base de données (p. 272).

c. Exécutez votre instance de base de données et vos réplicas en lecture avec votre charge de travail normale et surveillez les fichiers journaux.

   Si vous recevez des avertissements relatifs à des transactions incompatibles avec les identifiants de transaction globaux, modifiez votre application de sorte qu'elle utilise uniquement des fonctions compatibles avec les identifiants de transaction globaux. Assurez-vous que l'instance de base de données ne génère aucun avertissement relatif à des transactions incompatibles avec les identifiants de transaction globaux avant de passer à l'étape suivante.

3. Réinitialisez les paramètres GTID de la réplication basée sur des identifiants de transaction globaux qui autorise les transactions anonymes jusqu'à ce que les réplicas en lecture les aient toutes traitées.

   a. Assurez-vous que le groupe de paramètres associé à l'instance de base de données et à chaque réplica en lecture contient la configuration de paramètres suivante :

      - `gtid_mode` – `ON_PERMISSIVE`
      - `enforce_gtid_consistency` – `ON`

   b. Si vous modifiez le groupe de paramètres de l'instance de base de données, redémarrez celle-ci. Si vous modifiez le groupe de paramètres pour un réplica en lecture, redémarrez celui-ci.

4. Attendez que toutes vos transactions anonymes soient répliquées. Pour vérifier qu'elles ont été répliquées, procédez comme suit :

   a. Exécutez l'instruction suivante sur votre instance de base de données.

```
SHOW MASTER STATUS;
```

      Notez les valeurs dans les colonnes `File` et `Position`.

   b. Sur chaque réplica en lecture, utilisez les informations de fichier et de position de instance source lors de l'étape précédente pour exécuter la requête suivante.

```
SELECT MASTER_POS_WAIT('file', position);
```

      Par exemple, si votre fichier se nomme `mysql-bin-changelog.000031` et que sa position est `107`, exécutez l'instruction suivante.

```
SELECT MASTER_POS_WAIT('mysql-bin-changelog.000031', 107);
```

      Si le réplica en lecture a dépassé la position spécifiée, la requête renvoie immédiatement un résultat. Sinon, la fonction attend. Passez à l'étape suivante lorsque la requête a renvoyé un résultat pour tous les réplicas en lecture.

5. Réinitialisez les paramètres GTID uniquement pour la réplication GTID.

   a. Assurez-vous que le groupe de paramètres associé à l'instance de base de données et à chaque réplica en lecture contient la configuration de paramètres suivante :

      - `gtid_mode` – `ON`
      - `enforce_gtid_consistency` – `ON`

   b. Redémarrez l'instance de base de données et chaque réplica en lecture.

6. Sur chaque réplica en lecture, exécutez la procédure suivante.

```
CALL mysql.rds_set_master_auto_position(1);
```

Désactivation de la réplication basée sur des identifiants de transaction globaux (GTID) pour une instance de base de données RDS MySQL avec des réplicas en lecture

Vous pouvez désactiver la réplication GTID pour une instance de base de données RDS MySQL avec des réplicas en lecture.

Pour désactiver la réplication GTID pour une instance de base de données RDS MySQL avec des réplicas en lecture

1. Sur chaque réplica en lecture, exécutez la procédure suivante.

```
CALL mysql.rds_set_master_auto_position(0);
```

2. Réinitialisez `gtid_mode` sur `ON_PERMISSIVE`.

   a. Assurez-vous que le groupe de paramètres associé à l'instance de base de données RDS MySQL et à chaque réplica en lecture contient le paramètre `gtid_mode` défini sur `ON_PERMISSIVE`.

      Pour plus d'informations sur la définition des paramètres de configuration à l'aide de groupes de paramètres, veuillez consulter Utilisation de groupes de paramètres de base de données (p. 225).

   b. Redémarrez l'instance de base de données RDS MySQL et chaque réplica en lecture. Pour de plus amples informations sur le redémarrage, veuillez consulter Redémarrage d'une instance de base de données (p. 272).

3. Réinitialisez `gtid_mode` sur `OFF_PERMISSIVE` :

   a. Assurez-vous que le groupe de paramètres associé à l'instance de base de données RDS MySQL et à chaque réplica en lecture contient le paramètre `gtid_mode` défini sur `OFF_PERMISSIVE`.

   b. Redémarrez l'instance de base de données RDS MySQL et chaque réplica en lecture.

4. Attendez que toutes les transactions GTID soient appliquées sur tous les réplicas en lecture. Pour vérifier qu'elles ont été appliquées, procédez comme suit :

   Attendez que toutes les transactions GTID soient appliquées sur l'instance principale d'Aurora. Pour vérifier qu'elles ont été appliquées, procédez comme suit :

   a. Sur l'instance de base de données RDS MySQL, exécutez la commande `SHOW MASTER STATUS`.

      Votre sortie doit ressembler à ce qui suit.

```
File                        Position
------------------------------------
mysql-bin-changelog.000031      107
------------------------------------
```

      Notez le fichier et la position dans votre sortie.

   b. Sur chaque réplica en lecture, utilisez les informations de fichier et de position de instance source lors de l'étape précédente pour exécuter la requête suivante.

```
SELECT MASTER_POS_WAIT('file', position);
```

      Par exemple, si votre fichier se nomme `mysql-bin-changelog.000031` et que sa position est `107`, exécutez l'instruction suivante.

```
SELECT MASTER_POS_WAIT('mysql-bin-changelog.000031', 107);
```

Si le réplica en lecture a dépassé la position spécifiée, la requête renvoie immédiatement un résultat. Sinon, la fonction attend. Lorsque la requête a renvoyé un résultat pour tous les réplicas en lecture, passez à l'étape suivante.

5. Réinitialisez les paramètres GTID pour désactiver la réplication GTID :

   a. Assurez-vous que le groupe de paramètres associé à l'instance de base de données RDS MySQL et à chaque réplica en lecture contient les valeurs suivantes :

      - `gtid_mode` – `OFF`
      - `enforce_gtid_consistency` – `OFF`

   b. Redémarrez l'instance de base de données RDS MySQL et chaque réplica en lecture.

Réplication avec une instance MySQL ou MariaDB s'exécutant à l'extérieur d'Amazon RDS

Vous pouvez configurer la réplication entre une instance de base de données MySQL ou MariaDB Amazon RDS et une instance MariaDB externe à Amazon RDS.

Rubriques

- Avant de commencer (p. 863)
- Configuration d'une réplication de position de fichier journal binaire avec une instance source externe (p. 864)
- Configuration d'une réplication basée sur GTID avec une instance source externe (p. 866)

Avant de commencer

Vous pouvez configurer la réplication en utilisant la position du fichier journal binaire des transactions répliquées. Sur Amazon RDS MySQL 5.7.23 et les versions MySQL 5.7 ultérieures, vous pouvez aussi configurer la réplication avec des identifiants de transaction globaux (GTID).

Les autorisations requises pour démarrer la réplication sur une instance de base de données Amazon RDS sont restreintes et ne sont pas disponibles pour votre utilisateur principal Amazon RDS. Pour cette raison, assurez-vous d'utiliser les commandes Amazon RDS mysql.rds_set_external_master (p. 901) et mysql.rds_start_replication (p. 913) pour configurer la réplication entre votre base de données active et votre base de données Amazon RDS.

Pour définir le format de journalisation binaire pour une base de données MySQL ou MariaDB, mettez à jour le paramètre `binlog_format`. Si votre instance de base de données utilise le groupe de paramètres d'instance de base de données par défaut, créez un nouveau groupe de paramètres de base de données pour modifier les paramètres `binlog_format`. Nous vous recommandons d'utiliser le paramètre par défaut pour `binlog_format`, à savoir `MIXED`. Cependant, vous pouvez également définir `binlog_format` sur `ROW` ou `STATEMENT` si vous avez besoin d'un format binlog spécifique. Redémarrez votre instance de base de données pour que les modifications prennent effet.

Pour plus d'informations sur la configuration du paramètre `binlog_format`, consultez la section Format de journalisation binaire (p. 513). Pour de plus amples informations sur les implications des différents types de réplication MySQL, veuillez consulter la section Advantages and Disadvantages of Statement-Based and Row-Based Replication de la documentation MySQL.

Note

Utilisez la procédure de cette rubrique pour configurer la réplication dans tous les cas, à l'exception de celui où l'instance externe est MariaDB version 10.0.2 ou ultérieure et où l'instance Amazon RDS est MariaDB. Dans ce cas, utilisez la procédure Configuration d'une réplication basée sur GTID dans une instance de base de données MariaDB Amazon RDS (p. 577) pour configurer la réplication basée sur l'identifiant de transaction global.

Configuration d'une réplication de position de fichier journal binaire avec une instance source externe

Suivez ces instructions lorsque vous configurez une instance source externe et un réplica sur Amazon RDS :

- Surveillez les événements de basculement de l'instance de base de données Amazon RDS qui constitue votre réplica. En cas de basculement, l'instance de base de données qui est votre réplica peut alors être recréée sur un nouvel hôte avec une autre adresse réseau. Pour plus d'informations sur la surveillance des événements de basculement, consultez Utilisation de la notification d'événement Amazon RDS (p. 467).
- Tenez à jour les journaux binaires sur votre instance source, jusqu'à ce que vous ayez vérifié qu'ils ont été appliqués au réplica. Cette maintenance garantit que vous pouvez restaurer votre instance source en cas de défaillance.
- Activez les sauvegardes automatiques sur votre instance de base de données Amazon RDS. L'activation des sauvegardes automatiques garantit que vous pouvez restaurer votre réplica sur un instant donné si vous devez resynchroniser votre instance source et votre réplica. Pour plus d'informations sur les sauvegardes et la restauration à un instant dans le passé, consultez Sauvegarde et restauration d'une instance de base de données Amazon RDS (p. 317).

Pour configurer une réplication de position de fichier journal binaire avec une instance source externe

1. Rendez l'instance MySQL ou MariaDB source accessible en lecture seule.

```
mysql> FLUSH TABLES WITH READ LOCK;
mysql> SET GLOBAL read_only = ON;
```

2. Exécutez la commande `SHOW MASTER STATUS` sur l'instance source MySQL ou MariaDB pour déterminer l'emplacement du journal binaire.

   Vous obtenez une sortie similaire à ce qui suit.

```
File                          Position
------------------------------------
 mysql-bin-changelog.000031      107
------------------------------------
```

3. Copiez la base de données de l'instance externe vers l'instance de bases de données Amazon RDS à l'aide de `mysqldump`. Pour les bases de données très volumineuses, il se peut que vous vouliez utiliser la procédure décrite dans Importation de données vers une instance de base de données MySQL ou MariaDB Amazon RDS avec un temps réduit (p. 832).

   Pour Linux, macOS ou 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
```

Pour 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**
>
> Veillez bien à ce qu'il n'y ait pas d'espace entre l'option `-p` et le mot de passe saisi.

Pour spécifier le nom d'hôte, le nom d'utilisateur, le port et le mot de passe afin de vous connecter à votre instance de base de données Amazon RDS, utilisez les options `--host`, `--user (-u)`, `--port` et `-p` dans la commande `mysql`. Le nom d'hôte est le nom DNS du point de terminaison de l'instance de base de données Amazon RDS : par exemple, `myinstance.123456789012.us-east-1.rds.amazonaws.com`. Vous pouvez trouver la valeur du point de terminaison dans les détails de l'instance dans AWS Management Console.

4. Transformez l'instance de base de données source MySQL ou MariaDB en instance accessible de nouveau en écriture.

```
mysql> SET GLOBAL read_only = OFF;
mysql> UNLOCK TABLES;
```

Pour de plus amples informations sur les sauvegardes à utiliser avec la réplication, veuillez consulter la documentation MySQL.

5. Dans AWS Management Console, ajoutez l'adresse IP du serveur qui héberge la base de données externe source au groupe de sécurité du VPC de l'instance de base de données Amazon RDS. Pour de plus amples informations sur la modification d'un groupe de sécurité de VPC, veuillez consulter Security Groups for Your VPC (Groupes de sécurité pour votre VPC) dans le Guide de l'utilisateur Amazon Virtual Private Cloud.

   L'adresse IP peut changer lorsque les conditions suivantes sont réunies :

   - Vous utilisez une adresse IP publique pour la communication entre l'instance source externe et l'instance de base de données.
   - L'instance source externe a été arrêtée et redémarrée.

   Si ces conditions sont réunies, vérifiez l'adresse IP avant de l'ajouter.

   Vous devrez peut-être également configurer votre réseau local pour autoriser les connexions à partir de l'adresse IP de votre instance de base de données Amazon RDS. Cela permet la communication entre votre réseau local et votre instance MySQL ou MariaDB externe. Pour obtenir l'adresse IP de l'instance de base de données Amazon RDS, utilisez la commande `host`.

```
host db_instance_endpoint
```

Le nom d'hôte est le nom DNS du point de terminaison de l'instance de base de données Amazon RDS.

6. À l'aide du client de votre choix, connectez-vous à l'instance externe et créez un utilisateur à utiliser pour la réplication. Utilisez ce compte exclusivement pour la réplication et limitez-le à votre domaine pour améliorer la sécurité. Voici un exemple de.

```
CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'password';
```

7. Pour l'instance externe, attribuez les privilèges `REPLICATION CLIENT` et `REPLICATION SLAVE` à votre utilisateur de réplication. Par exemple, pour accorder les privilèges `REPLICATION CLIENT` et `REPLICATION SLAVE` sur toutes les bases de données à l'utilisateur « `repl_user` » de votre domaine, émettez la commande suivante.

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'
 IDENTIFIED BY 'password';
```

8. Transformez l'instance de base de données Amazon RDS en réplica. Pour cela, connectez-vous d'abord à l'instance de base de données Amazon RDS en tant qu'utilisateur principal. Identifiez ensuite la base de données MySQL ou MariaDB externe comme instance source à l'aide de la commande mysql.rds_set_external_master (p. 901). Utilisez le nom et la position du fichier journal maître que vous avez déterminés à l'étape 2. Voici un exemple de.

```
CALL mysql.rds_set_external_master ('mymasterserver.mydomain.com', 3306, 'repl_user',
 'password', 'mysql-bin-changelog.000031', 107, 0);
```

   Note

   Dans Amazon RDS MySQL, vous pouvez décider d'utiliser la réplication retardée en exécutant la procédure stockée mysql.rds_set_external_master_with_delay (p. 904) à la place. Notre raison d'utiliser la réplication retardée est qu'elle permet la reprise après sinistre avec la procédure stockée mysql.rds_start_replication_until (p. 914). Actuellement, la réplication retardée n'est pas prise en charge sur Amazon RDS MariaDB.

9. Sur l'instance de base de données Amazon RDS, émettez la commande mysql.rds_start_replication (p. 913) pour démarrer la réplication :

```
CALL mysql.rds_start_replication;
```

Configuration d'une réplication basée sur GTID avec une instance source externe

Lorsque vous configurez une instance source externe et un réplica sur Amazon RDS, surveillez les événements de basculement de l'instance de base de données Amazon RDS qui constitue votre réplica. En cas de basculement, l'instance de base de données qui est votre réplica peut alors être recréée sur un nouvel hôte avec une autre adresse réseau. Pour plus d'informations sur la surveillance des événements de basculement, consultez Utilisation de la notification d'événement Amazon RDS (p. 467).

Important

La réplication basée sur des identifiants de transaction globaux (GTID) est prise en charge uniquement sur Amazon RDS MySQL 5.7.23 et les versions MySQL 5.7 ultérieures. La réplication

basée sur des identifiants de transaction globaux (GTID) n'est pas prise en charge pour Amazon RDS MySQL 5.5, 5.6 ou 8.0.

Pour configurer une réplication basée sur des identifiants de transaction globaux (GTID) avec une instance source externe

1. Préparez la réplication basée sur des identifiants de transaction globaux (GTID) :

   a. Assurez-vous que la réplication basée sur des identifiants de transaction globaux (GTID) est activée sur la base de données MySQL ou MariaDB externe. Pour ce faire, assurez-vous que les paramètres suivants de la base de données externe sont définis sur les valeurs spécifiées :

      `gtid_mode` – `ON`

      `enforce_gtid_consistency` – `ON`

      Pour de plus amples informations, veuillez consulter Replication with Global Transaction Identifiers dans la documentation MySQL, ou la page Global Transaction ID dans la documentation MariaDB.

   b. Assurez-vous que le groupe de paramètres associé à l'instance de base de données contient la configuration de paramètres suivante :

      - `gtid_mode` – `ON`, `ON_PERMISSIVE` ou `OFF_PERMISSIVE`
      - `enforce_gtid_consistency` – `ON`

      Pour plus d'informations sur les groupes de paramètres, consultez Utilisation de groupes de paramètres de base de données (p. 225).

   c. Si vous modifiez le groupe de paramètres de l'instance de base de données, redémarrez celle-ci. Pour plus d'informations, consultez Redémarrage d'une instance de base de données (p. 272).

2. Rendez l'instance MySQL ou MariaDB source accessible en lecture seule.

```
mysql> FLUSH TABLES WITH READ LOCK;
mysql> SET GLOBAL read_only = ON;
```

3. Copiez la base de données de l'instance externe vers l'instance de bases de données Amazon RDS à l'aide de `mysqldump`. Pour les bases de données très volumineuses, il se peut que vous vouliez utiliser la procédure décrite dans Importation de données vers une instance de base de données MySQL ou MariaDB Amazon RDS avec un temps réduit (p. 832).

   Pour Linux, macOS ou 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
```

   Pour 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**
>
> Veillez bien à ce qu'il n'y ait pas d'espace entre l'option `-p` et le mot de passe saisi.

Pour spécifier le nom d'hôte, le nom d'utilisateur, le port et le mot de passe afin de vous connecter à votre instance de base de données Amazon RDS, utilisez les options `--host`, `--user (-u)`, `--port` et `-p` dans la commande `mysql`. Le nom d'hôte est le nom DNS du point de terminaison de l'instance de base de données Amazon RDS : par exemple, `myinstance.123456789012.us-east-1.rds.amazonaws.com`. Vous pouvez trouver la valeur du point de terminaison dans les détails de l'instance dans AWS Management Console.

4. Transformez l'instance de base de données source MySQL ou MariaDB en instance accessible de nouveau en écriture.

```
mysql> SET GLOBAL read_only = OFF;
mysql> UNLOCK TABLES;
```

Pour de plus amples informations sur les sauvegardes à utiliser avec la réplication, veuillez consulter la documentation MySQL.

5. Dans AWS Management Console, ajoutez l'adresse IP du serveur qui héberge la base de données externe source au groupe de sécurité du VPC de l'instance de base de données Amazon RDS. Pour de plus amples informations sur la modification d'un groupe de sécurité de VPC, veuillez consulter Security Groups for Your VPC (Groupes de sécurité pour votre VPC) dans le Guide de l'utilisateur Amazon Virtual Private Cloud.

   L'adresse IP peut changer lorsque les conditions suivantes sont réunies :

   - Vous utilisez une adresse IP publique pour la communication entre l'instance source externe et l'instance de base de données.
   - L'instance source externe a été arrêtée et redémarrée.

   Si ces conditions sont réunies, vérifiez l'adresse IP avant de l'ajouter.

   Vous devrez peut-être également configurer votre réseau local pour autoriser les connexions à partir de l'adresse IP de votre instance de base de données Amazon RDS. Cela permet la communication entre votre réseau local et votre instance MySQL ou MariaDB externe. Pour obtenir l'adresse IP de l'instance de base de données Amazon RDS, utilisez la commande `host`.

```
host db_instance_endpoint
```

   Le nom d'hôte est le nom DNS du point de terminaison de l'instance de base de données Amazon RDS.

6. À l'aide du client de votre choix, connectez-vous à l'instance externe et créez un utilisateur à utiliser pour la réplication. Utilisez ce compte exclusivement pour la réplication et limitez-le à votre domaine pour améliorer la sécurité. Voici un exemple de.

```
CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'password';
```

7. Pour l'instance externe, attribuez les privilèges `REPLICATION CLIENT` et `REPLICATION SLAVE` à votre utilisateur de réplication. Par exemple, pour accorder les privilèges `REPLICATION CLIENT`

et `REPLICATION SLAVE` sur toutes les bases de données à l'utilisateur « `repl_user` » de votre domaine, émettez la commande suivante.

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'
 IDENTIFIED BY 'password';
```

8. Transformez l'instance de base de données Amazon RDS en réplica. Pour cela, connectez-vous d'abord à l'instance de base de données Amazon RDS en tant qu'utilisateur principal. Identifiez ensuite la base de données MySQL ou MariaDB externe comme instance principale de réplication à l'aide de la commande mysql.rds_set_external_master_with_auto_position (p. 907). Voici un exemple de.

```
CALL mysql.rds_set_external_master_with_auto_position ('mymasterserver.mydomain.com',
 3306, 'repl_user', 'password', 0, 0);
```

   Note

   Dans Amazon RDS MySQL, vous pouvez décider d'utiliser la réplication retardée en exécutant la procédure stockée mysql.rds_set_external_master_with_delay (p. 904) à la place. Notre raison d'utiliser la réplication retardée est qu'elle permet la reprise après sinistre avec la procédure stockée mysql.rds_start_replication_until_gtid (p. 915). Actuellement, la réplication retardée n'est pas prise en charge sur Amazon RDS MariaDB.

9. Sur l'instance de base de données Amazon RDS, émettez la commande mysql.rds_start_replication (p. 913) pour démarrer la réplication.

```
CALL mysql.rds_start_replication;
```

Exportation de données à partir d'une instance DB MySQL grâce à la réplication

Pour exporter des données à partir d'une instance de base de données MySQL 5.6 ou ultérieure vers une instance MySQL exécutée en externe sur Amazon RDS, vous pouvez utiliser la réplication. Dans ce scénario, l'instance de base de données Amazon RDS MySQL est l'instance de base de données MySQL source, et l'instance MySQL exécutée en externe sur Amazon RDS est la base de données MySQL externe.

L'instance de base de données MySQL source doit exécuter la version 5.6.13 ou version ultérieure. La base de données MySQL externe peut s'exécuter soit localement dans votre centre de données, soit sur une instance Amazon EC2. La base de données MySQL externe doit exécuter la même version que l'instance de base de données MySQL source, ou une version ultérieure.

La réplication vers une base de données MySQL externe n'est prise en charge que pendant le temps nécessaire à l'exportation d'une base de données à partir de l'instance de base de données MySQL source. La réplication doit être terminée une fois que les données ont été exportées et que les applications peuvent commencer à accéder à l'instance externe.

La liste suivante montre les étapes à suivre. Chaque étape est présentée plus en détail dans les sections ultérieures.

1. Préparez une instance de base de données MySQL externe.
2. Préparez l'instance de base de données MySQL source pour la réplication.
3. Utilisez l'utilitaire mysqldump pour transférer la base de données de l'instance de base de données MySQL source vers la base de données MySQL externe.

4. Démarrez la réplication vers la base de données MySQL externe.
5. Une fois l'exportation terminée, arrêtez la réplication.

Préparer une base de données MySQL externe

Effectuez les étapes suivantes pour préparer la base de données MySQL externe.

Pour créer la base de données MySQL externe

1. Installez la base de données MySQL externe.
2. Connectez-vous à la base de données MySQL externe en tant qu'utilisateur principal. Créez ensuite les utilisateurs requis pour prendre en charge les administrateurs, les applications et les services qui accèdent à la base de données.
3. Suivez les instructions de la documentation MySQL pour préparer la base de données MySQL externe en tant que réplica. Pour de plus amples informations, veuillez consulter la documentation MySQL.
4. Configurez une règle de sortie pour que la base de données MySQL externe fonctionne comme un réplica en lecture pendant l'exportation. La règle de sortie permet à la base de données MySQL externe de se connecter à l'instance de base de données MySQL source pendant la réplication. Spécifiez une règle de sortie qui autorise les connexions TCP (Transmission Control Protocol) au port et à l'adresse IP de l'instance de base de données MySQL source.

   Spécifiez les règles de sortie appropriées pour votre environnement :

   - Si la base de données MySQL externe s'exécute dans une instance Amazon EC2 dans un Cloud privé virtuel (VPC) basé sur le service Amazon VPC, spécifiez les règles de sortie dans un groupe de sécurité VPC. Pour de plus amples informations, veuillez consulter Contrôle d'accès par groupe de sécurité (p. 1590).
   - Si la base de données MySQL externe s'exécute dans une instance Amazon EC2 qui n'est pas dans un VPC, spécifiez les règles de sortie dans un groupe de sécurité EC2-Classic.
   - Si la base de données MySQL externe est installée localement, spécifiez les règles de sortie dans un pare-feu.
5. Si la base de données MySQL externe est en cours d'exécution dans un VPC, configurez les règles pour les règles de liste de contrôle d'accès (ACL) VPC en plus de la règle de sortie du groupe de sécurité :

   - Configurez une règle d'entrée ACL autorisant le trafic TCP vers les ports 1024–65535 à partir de l'adresse IP de l'instance de base de données MySQL source.
   - Configurez une règle de sortie ACL autorisant le trafic TCP sortant vers le port et l'adresse IP de l'instance de base de données MySQL source.

   Pour de plus amples informations sur les ACL réseau Amazon VPC, veuillez consulter ACL réseau dans Amazon VPC Guide de l'utilisateur.
6. (Facultatif) Définissez le paramètre `max_allowed_packet` sur la taille maximale pour éviter les erreurs de réplication. Nous recommandons ce paramètre.

Préparer l'instance de base de données MySQL source

Effectuez les étapes suivantes pour préparer l'instance de base de données MySQL source en tant que source de réplication.

Pour préparer l'instance de base de données MySQL source

1. Assurez-vous que votre ordinateur client possède assez d'espace disque pour enregistrer les journaux binaires lors de la configuration de la réplication.
2. Connectez-vous à l'instance de base de données MySQL source et créez un compte de réplication en suivant les instructions de Création d'un utilisateur pour la réplication dans la documentation MySQL.
3. Configurez les règles d'entrée sur le système exécutant l'instance de base de données MySQL source pour permettre à la base de données MySQL externe de se connecter pendant la réplication. Spécifiez une règle d'entrée qui autorise les connexions TCP au port utilisé par l'instance de base de données MySQL source à partir de l'adresse IP de la base de données MySQL externe.
4. Spécifiez les règles de sortie :
   - Si l'instance de base de données MySQL source s'exécute dans un VPC, spécifiez les règles d'entrée dans un groupe de sécurité VPC. Pour plus d'informations, consultez Contrôle d'accès par groupe de sécurité (p. 1590).
   - Si l'instance de base de données MySQL source ne s'exécute pas dans un VPC, spécifiez les règles d'entrée dans un groupe de sécurité de base de données. Pour plus d'informations, consultez Autorisation de l'accès réseau à un groupe de sécurité DB depuis une plage IP (p. 1600).
5. Si l'instance de base de données MySQL source est en cours d'exécution dans un VPC, configurez les règles ACL VPC en plus de la règle d'entrée de groupe de sécurité :
   - Configurez une règle d'entrée ACL pour autoriser les connexions TCP au port utilisé par l'instance Amazon RDS à partir de l'adresse IP de la base de données MySQL externe.
   - Configurez une règle de sortie ACL pour autoriser les connexions TCP des ports 1024–65535 vers l'adresse IP de la base de données MySQL externe.

   Pour de plus amples informations sur les ACL réseau Amazon VPC, veuillez consulter ACL réseau dans Amazon VPC Guide de l'utilisateur.
6. Assurez-vous que la période de rétention des sauvegardes soit assez longue pour qu'aucun journal binaire ne soit purgé pendant l'exportation. Si l'un des journaux est purgé avant la fin de l'exportation, vous devez redémarrer la réplication depuis le début. Pour plus d'informations sur la configuration de la période de rétention des sauvegardes, consultez Utilisation des sauvegardes (p. 317).
7. Utilisez la procédure stockée `mysql.rds_set_configuration` pour définir une période de conservation du journal binaire suffisamment longue pour que les journaux binaires ne soient pas purgés pendant l'exportation. Pour plus d'informations, consultez Accès aux journaux binaires MySQL (p. 514).
8. Créez un réplica en lecture Amazon RDS à partir de l'instance de base de données MySQL source afin de vous assurer que les journaux binaires de l'instance de base de données MySQL source ne seront pas purgés. Pour plus d'informations, consultez Création d'un réplica en lecture (p. 280).
9. Une fois que le réplica en lecture Amazon RDS a été créé, appelez la procédure stockée `mysql.rds_stop_replication` pour arrêter le processus de réplication. L'instance de base de données MySQL source ne purge plus ses fichiers journaux binaires, ils sont donc disponibles pour le processus de réplication.
10. (Facultatif) Définissez le paramètre `max_allowed_packet` et le paramètre `slave_max_allowed_packet` sur la taille maximale pour éviter les erreurs de réplication. La taille maximale pour les deux paramètres est de 1 Go. Nous recommandons ces valeurs pour les deux paramètres. Pour plus d'informations sur la définition des paramètres, consultez Modification de paramètres dans un groupe de paramètres de bases de données (p. 229).

Copier la base de données

Effectuez les étapes suivantes pour copier la base de données.

Pour copier la base de données

1. Connectez-vous au réplica en lecture RDS de l'instance de base de données MySQL source et exécutez l'instruction `SHOW SLAVE STATUS\G` MySQL. Notez les valeurs pour les éléments suivants :

   - `Master_Host`
   - `Master_Port`
   - `Master_Log_File`
   - `Exec_Master_Log_Pos`

2. Utilisez l'utilitaire mysqldump pour créer un instantané qui copie les données Amazon RDS à partir de votre ordinateur client local. Ensuite, exécutez un autre utilitaire pour charger les données dans la base de données MySQL externe. Assurez-vous que votre ordinateur client possède assez d'espace disque pour contenir les fichiers `mysqldump` des bases de données à répliquer. Ce processus peut prendre plusieurs heures pour les bases de données très volumineuses. Suivez les instructions de la partie Création d'un instantané de données à l'aide de mysqldump dans la documentation MySQL.

   L'exemple suivant montre comment exécuter `mysqldump` sur un client, puis achemine le vidage vers l'utilitaire client `mysql`, qui charge les données dans l'instance MySQL externe.

   Pour Linux, macOS ou Unix :

```
mysqldump -h source_MySQL_DB_instance_endpoint \
    -u user \
    -ppassword \
    --port=3306 \
    --single-transaction \
    --routines \
    --triggers \
    --databases  database database2 \
    --compress  \
    --port 3306
```

   Pour Windows :

```
mysqldump -h source_MySQL_DB_instance_endpoint ^
    -u user ^
    -ppassword ^
    --port=3306 ^
    --single-transaction ^
    --routines ^
    --triggers ^
    --databases  database database2 ^
    --compress  ^
    --port 3306
```

   L'exemple suivant exécute `mysqldump` sur un client et écrit le vidage dans un fichier.

   Pour Linux, macOS ou Unix :

```
mysqldump -h source_MySQL_DB_instance_endpoint \
    -u user \
    -ppassword \
    --port=3306 \
    --single-transaction \
    --routines \
    --triggers \
    --databases  database database2 > path/rds-dump.sql
```

Pour Windows :

```
mysqldump -h source_MySQL_DB_instance_endpoint ^
    -u user ^
    -ppassword ^
    --port=3306 ^
    --single-transaction ^
    --routines ^
    --triggers ^
    --databases  database database2 > path\rds-dump.sql
```

Terminer l'exportation

Effectuez les étapes suivantes pour terminer l'exportation.

Pour terminer l'exportation

1. Chargez les fichiers mysqldump pour créer les bases de données sur la base de données MySQL externe.
2. Sur le réplica en lecture Amazon RDS, appelez la procédure stockée `mysql.rds_start_replication`. Cela démarre la réplication à partir de l'instance de base de données MySQL source et exporte toutes les modifications de source qui se sont produites après l'arrêt de la réplication à partir du réplica en lecture Amazon RDS.
3. Utilisez l'instruction MySQL `CHANGE MASTER` pour configurer l'instance MySQL externe. Spécifiez l'ID et le mot de passe de l'utilisateur auquel ont été attribuées les autorisations `REPLICATION SLAVE`. Spécifiez les valeurs `Master_Host`, `Master_Port`, `Relay_Master_Log_File` et `Exec_Master_Log_Pos` obtenues à partir de l'instruction `SHOW SLAVE STATUS\G` MySQL que vous avez exécutée sur le réplica en lecture RDS. Pour de plus amples informations, veuillez consulter la documentation MySQL.
4. Utilisez la commande `START SLAVE` MySQL pour lancer la réplication à partir de l'instance de base de données MySQL source vers la base de données MySQL externe.
5. Exécutez la commande `SHOW SLAVE STATUS\G` MySQL sur la base de données MySQL externe pour vérifier qu'elle fonctionne comme un réplica en lecture. Pour de plus amples informations sur l'interprétation des résultats, veuillez consulter la documentation MySQL.
6. Une fois que la réplication sur la base de données MySQL externe a rattrapé l'instance de base de données MySQL source, utilisez la commande `STOP SLAVE` MySQL pour arrêter la réplication à partir de l'instance de base de données MySQL source.
7. Sur le réplica en lecture Amazon RDS, appelez la procédure stockée `mysql.rds_start_replication`. Cela permet à Amazon RDS de démarrer la purge des fichiers journaux binaires à partir de l'instance de base de données MySQL source.

Options pour les instances de base de données MySQL

Cette annexe décrit les options, ou fonctions supplémentaires, disponibles pour les instances Amazon RDS exécutant le moteur de base de données MySQL. Pour activer ces options, vous pouvez les ajouter à un groupe d'options personnalisé, puis associer ce dernier à votre instance de base de données. Pour plus d'informations sur l'utilisation de groupes d'options, consultez Utilisation de groupes d'options (p. 209).

Amazon RDS prend en charge les options suivantes pour MySQL :

Option	ID d'option	Versions du moteur
Prise en charge du plug-in d'audit MariaDB (p. 874)	`MARIADB_AUDIT_PLUGIN`	Toutes les versions MySQL 5.6 Version MySQL 5.7.16 et versions 5.7 ultérieures
Prise en charge memcached MySQL (p. 877)	`MEMCACHED`	Toutes les versions MySQL 5.6, 5.7 et 8.0

Prise en charge du plug-in d'audit MariaDB

Amazon RDS prend en charge l'utilisation du plug-in d'audit MariaDB sur les instances de base de données MySQL. Le plug-in d'audit MariaDB enregistre l'activité de la base de données, telle que les utilisateurs qui se connectent à la base de données, les requêtes exécutées sur la base de données et plus encore. L'enregistrement de l'activité de la base de données est stocké dans un fichier journal.

> **Note**
>
> Actuellement, le plug-in d'audit MariaDB est uniquement pris en charge pour les versions Amazon RDS MySQL suivantes :
>
> - Toutes les versions 5.6
> - Version MySQL 5.7.16 et versions 5.7 ultérieures

Paramètres de l'option du plug-in d'audit

Amazon RDS prend en charge les paramètres suivants pour l'option de plug-in d'audit MariaDB.

Paramètre d'option	Valeurs valides	Valeur par défaut	Description
`SERVER_AUDIT_FILE_PATH`	`/rdsdbdata/log/audit/`	`/rdsdbdata/log/audit/`	Emplacement du fichier journal. Le fichier journal contient l'enregistrement de l'activité spécifiée dans `SERVER_AUDIT_EVENTS`. Pour plus d'informations, consultez Liste et affichage des fichiers journaux de base de données (p. 491) et Fichiers journaux de base de données MySQL (p. 506).
`SERVER_AUDIT_FILE_ROTATION_SIZE`	1–1 000 000 000	1 000 000	Taille en octets qui, lorsqu'elle est atteinte, entraîne la rotation du fichier. Pour plus d'informations, consultez Taille des fichiers journaux (p. 512).
`SERVER_AUDIT_FILE_ROTATIONS`	0–100	9	Nombre de rotations de journaux à enregistrer. Pour plus d'informations, consultez Taille des fichiers journaux (p. 512) et Téléchargement d'un fichier journal de base de données (p. 491).
`SERVER_AUDIT_EVENTS`	`CONNECT`, `QUERY`, `QUERY_DDL`, `QUERY_DML`, `QUERY_DCL`	`CONNECT`, `QUERY`	Types d'activités à enregistrer dans le journal. L'installation du plug-in d'audit MariaDB est elle-même enregistrée.

Paramètre d'option	Valeurs valides	Valeur par défaut	Description
			• `CONNECT` : Permet d'enregistrer les connexions à la base de données, réussies ou non, et les déconnexions de la base de données. • `QUERY` : Permet d'enregistrer le texte de toutes les requêtes exécutées sur la base de données. • `QUERY_DDL` : semblable à l'événement `QUERY`, mais renvoie uniquement les requêtes en langage de définition de données (DDL) (`CREATE`, `ALTER`, etc.). • `QUERY_DML` : semblable à l'événement `QUERY`, mais renvoie uniquement les requêtes en langage de manipulation de données (DML) (`INSERT`, `UPDATE`, `SELECT`, etc.). • `QUERY_DCL` : semblable à l'événement `QUERY`, mais renvoie uniquement les requêtes en langage de contrôle de données (DCL) (`GRANT`, `REVOKE`, etc.). Pour MySQL, `TABLE` n'est pas pris en charge.
`SERVER_AUDIT_INCL_USERS`	Plusieurs valeurs séparées par des virgules	Aucune	Incluez uniquement l'activité des utilisateurs spécifiés. Par défaut, l'activité est enregistrée pour tous les utilisateurs. Si un utilisateur est spécifié dans `SERVER_AUDIT_EXCL_USERS` et `SERVER_AUDIT_INCL_USERS`, l'activité est alors enregistrée pour l'utilisateur.
`SERVER_AUDIT_EXCL_USERS`	Plusieurs valeurs séparées par des virgules	Aucune	Excluez l'activité des utilisateurs spécifiés. Par défaut, l'activité est enregistrée pour tous les utilisateurs. Si un utilisateur est spécifié dans `SERVER_AUDIT_EXCL_USERS` et `SERVER_AUDIT_INCL_USERS`, l'activité est alors enregistrée pour l'utilisateur. L'utilisateur `rdsadmin` interroge la base de données par seconde pour vérifier l'intégrité de la base de données. En fonction de vos autres paramètres, cette activité peut éventuellement provoquer un accroissement considérable et rapide de la taille de votre fichier journal. Si vous n'avez pas besoin d'enregistrer cette activité, ajoutez l'utilisateur `rdsadmin` à la liste `SERVER_AUDIT_EXCL_USERS`. Note L'activité `CONNECT` est toujours enregistrée pour tous les utilisateurs, même si l'utilisateur est spécifié pour ce paramètre d'option.

Paramètre d'option	Valeurs valides	Valeur par défaut	Description
`SERVER_AUDIT_LOGGING`	`ON`	`ON`	La journalisation est active. La seule valeur valide est `ON`. Amazon RDS ne prend pas en charge la désactivation de la journalisation. Si vous souhaitez désactiver la journalisation, supprimez le plug-in d'audit MariaDB. Pour plus d'informations, consultez Suppression du plug-in d'audit MariaDB (p. 877).

Ajout du plug-in d'audit MariaDB

Le processus général pour ajouter le plug-in d'audit MariaDB à une instance de base de données est le suivant :

- Créez un groupe d'options ou copiez ou modifiez un groupe d'options existant.
- Ajouter l'option au groupe d'options
- Associer un groupe d'options à une instance de base de données

Une fois que vous ajoutez le plug-in d'audit MariaDB, vous n'avez pas besoin de redémarrer votre instance de base de données. Dès que le groupe d'options est actif, l'audit commence immédiatement.

> **Important**
>
> L'ajout du plug-in d'audit MariaDB à une instance de base de données peut entraîner une interruption de service. Nous vous recommandons d'ajouter le plug-in d'audit MariaDB pendant une fenêtre de maintenance ou lorsque la charge de travail de base de données est faible.

Pour ajouter le plug-in d'audit MariaDB

1. Déterminez le groupe d'options que vous voulez utiliser. Vous pouvez créer un groupe d'options ou utiliser un groupe d'options existant. Si vous souhaitez utiliser un groupe d'options existant, passez à l'étape suivante. Sinon, créez un groupe d'options de base de données personnalisé. Choisissez mysql pour Moteur, puis 5.6 ou 5.7 pour Version majeure du moteur. Pour plus d'informations, consultez Création d'un groupe d'options (p. 212).
2. Ajoutez l'option MARIADB_AUDIT_PLUGIN pour le groupe d'options et configurez les paramètres de l'option. Pour plus d'informations sur l'ajout d'options, consultez Ajout d'une option à un groupe d'options (p. 214). Pour plus d'informations sur chaque paramètre, consultez Paramètres de l'option du plug-in d'audit (p. 874).
3. Appliquez le groupe d'options à une instance de base de données nouvelle ou existante.
   - Pour une nouvelle instance de base de données, vous appliquez le groupe d'options lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).
   - Pour une instance de base de données existante, vous appliquez le groupe d'options en modifiant l'instance et en attachant le nouveau groupe d'options. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Affichage et téléchargement du journal du plug-in d'audit MariaDB

Une fois que vous activez le plug-in d'audit MariaDB, vous accéder aux résultats dans les fichiers journaux de la même manière que tous les autres fichiers journaux texte. Les fichiers journaux d'audit se trouvent dans `/rdsdbdata/log/audit/`. Pour plus d'informations sur l'affichage du fichier journal dans la

console, consultez Liste et affichage des fichiers journaux de base de données (p. 491). Pour plus d'informations sur le téléchargement du fichier journal, consultez Téléchargement d'un fichier journal de base de données (p. 491).

Modification des paramètres de plug-in d'audit MariaDB

Une fois que vous activez le plug-in d'audit MariaDB, vous pouvez modifier les paramètres. Pour plus d'informations sur la modification des paramètres d'options, consultez Modification d'un paramètre d'option (p. 219). Pour plus d'informations sur chaque paramètre, consultez Paramètres de l'option du plug-in d'audit (p. 874).

Suppression du plug-in d'audit MariaDB

Amazon RDS ne prend pas en charge la désactivation de la journalisation du plug-in d'audit MariaDB. Toutefois, vous pouvez supprimer le plug-in dans une instance de base de données. Lorsque vous supprimez le plug-in d'audit MariaDB, l'instance de base de données est automatiquement redémarrée pour cesser l'audit.

Pour supprimer le plug-in d'audit MariaDB d'une instance de base de données, effectuez l'une des actions suivantes :

- Supprimez l'option de plug-in d'audit MariaDB du groupe d'options auquel elle appartient. Ce changement affecte toutes les instances de bases de données qui utilisent le groupe d'options. Pour de plus amples informations, veuillez consulter Suppression d'une option d'un groupe d'options (p. 222)
- Modifiez l'instance de base de données et spécifiez un groupe d'options différent qui n'inclut pas le plug-in. Ce changement affecte une seule instance de base de données. Vous pouvez spécifier le groupe d'options (vide) par défaut, ou un groupe d'options personnalisées différent. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Prise en charge memcached MySQL

Amazon RDS prend en charge l'utilisation de l'interface `memcached` pour les tableaux InnoDB introduits dans MySQL 5.6. L'API `memcached` permet aux applications d'utiliser les tables InnoDB de la même façon que les magasins de données clé-valeur NoSQL.

L'interface `memcached` est un cache simple basé sur les clés. Les applications utilisent `memcached` pour insérer, manipuler et récupérer les paires de données clé-valeur du cache. MySQL 5.6 a présenté un plug-in qui implémente un service démon exposant les données des tables InnoDB via le protocole `memcached`. Pour de plus amples informations sur le plug-in MySQL `memcached`, veuillez consulter InnoDB Integration with memcached.

Pour activer la prise en charge memcached pour une instance Amazon RDS MySQL 5.6 ou version ultérieure

1. Déterminez le groupe de sécurité à utiliser pour contrôler l'accès à l'interface `memcached`. Si l'ensemble d'applications qui utilise déjà l'interface SQL est identique à celui qui accède à l'interface `memcached`, vous pouvez utiliser le groupe de sécurité VPC ou DB existant utilisé par l'interface SQL. Si un ensemble différent d'applications accède à l'interface `memcached`, définissez un nouveau groupe de sécurité VPC ou DB. Pour plus d'informations sur la gestion des groupes de sécurité, consultez Contrôle d'accès par groupe de sécurité (p. 1590).
2. Créez un groupe d'options DB personnalisé, en sélectionnant MySQL comme type de moteur et une version 5.6 ou supérieure. Pour plus d'informations sur la création d'un groupe d'options, consultez Création d'un groupe d'options (p. 212).
3. Ajoutez l'option `MEMCACHED` au groupe d'options. Spécifiez le port que l'interface `memcached` utilisera, et le groupe de sécurité à utiliser pour contrôler l'accès à l'interface. Pour plus d'informations sur l'ajout d'options, consultez Ajout d'une option à un groupe d'options (p. 214).

4. Modifiez les options pour configurer les paramètres `memcached`, le cas échéant. Pour plus d'informations sur la modification des paramètres d'options, consultez Modification d'un paramètre d'option (p. 219).
5. Appliquer le groupe d'options à une instance. Amazon RDS active la prise en charge `memcached` pour cette instance lorsque le groupe d'options est appliqué :
   - Vous activez la prise en charge `memcached` pour une nouvelle instance en spécifiant le groupe d'options personnalisé lorsque vous lancez l'instance. Pour plus d'informations sur le lancement d'une instance MySQL, consultez Création d'une instance de base de données Amazon RDS (p. 146).
   - Vous activez la prise en charge `memcached` pour une instance existante en spécifiant le groupe d'options personnalisé lorsque vous modifiez l'instance. Pour de plus amples informations sur la modification d'une instance de base de données, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).
6. Spécifiez les colonnes de vos tables MySQL accessibles via l'interface `memcached`. Le plug-in `memcached` crée une table de catalogue appelée `containers` dans une base de données dédiée appelée `innodb_memcache`. Vous insérez une ligne dans la table `containers` pour mapper une table InnoDB et y accéder via `memcached`. Vous spécifiez une colonne dans la table InnoDB qui est utilisée pour stocker les valeurs de clé `memcached`, et une ou plusieurs colonnes qui sont utilisées pour stocker les valeurs de données associées à la clé. Vous spécifiez également un nom qu'une application `memcached` utilise pour faire référence à cet ensemble de colonnes. Pour de plus amples informations sur l'insertion de lignes dans la table `containers`, veuillez consulter Internals of the InnoDB memcached Plugin. Pour obtenir un exemple de mappage d'une table InnoDB et y accéder via `memcached`, veuillez consulter Writing Applications for the InnoDB memcached Plugin.
7. Si les applications qui accèdent à l'interface `memcached` sont sur différents ordinateurs ou instances EC2 que les applications qui utilisent l'interface SQL, ajoutez les informations de connexion de ces ordinateurs au groupe de sécurité VPC et DB associé à l'instance MySQL. Pour plus d'informations sur la gestion des groupes de sécurité, consultez Contrôle d'accès par groupe de sécurité (p. 1590).

Vous désactivez la prise en charge `memcached` pour une instance en modifiant l'instance et en spécifiant le groupe d'options par défaut pour votre version MySQL. Pour de plus amples informations sur la modification d'une instance de base de données, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

Considérations de sécurité memcached MySQL

Le protocole `memcached` ne prend pas en charge l'authentification utilisateur. Pour plus d'informations sur les considérations de sécurité MySQL `memcached`, consultez memcached Deployment et Using memcached as a MySQL Caching Layer.

Vous pouvez prendre les mesures suivantes pour aider à augmenter la sécurité de l'interface `memcached` :

- Spécifiez un port différent du port par défaut 11211 lorsque vous ajoutez l'option `MEMCACHED` au groupe d'options.
- Veillez à associer l'interface `memcached` avec un groupe de sécurité VPC ou DB qui limite l'accès aux adresses client ou instances EC2 fiables et connues. Pour plus d'informations sur la gestion des groupes de sécurité, consultez Contrôle d'accès par groupe de sécurité (p. 1590).

Informations de connexion memcached MySQL

Pour accéder à l'interface `memcached`, une application doit spécifier le nom DNS de l'instance Amazon RDS et le numéro de port `memcached`. Par exemple, si une instance possède un nom DNS de `my-cache-instance.cg034hpkmmjt.region.rds.amazonaws.com` et l'interface memcached utilise le port 11212, les informations de connexion spécifiées dans PHP seront :

```
<?php

$cache = new Memcache;
$cache->connect('my-cache-instance.cg034hpkmmjt.region.rds.amazonaws.com',11212);
?>
```

Pour trouver le nom DNS et le port memcached d'une instance MySQL Amazon RDS

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le coin supérieur droit de la AWS Management Console, sélectionnez la région qui contient l'instance de base de données.
3. Dans la panneau de navigation, choisissez Databases (Bases de données).
4. Choisissez le nom de l'instance de base de données MySQL pour afficher ses détails.
5. Dans la section Connexion, notez la valeur du champ Point de terminaison. Le nom DNS est le même que le point de terminaison. Veuillez également noter que le port dans la section Connexion n'est pas utilisé pour accéder à l'interface `memcached`.
6. Dans la section Détails, notez le nom répertorié dans le champ Groupe d'options.
7. Dans le panneau de navigation, choisissez Groupes d'options.
8. Choisissez le nom du groupe d'options utilisé par l'instance de base de données MySQL pour afficher les détails du groupe d'options. Dans la section Options, notez la valeur du paramètre Port pour l'option MEMCACHED.

Paramètres d'option memcached MySQL

Amazon RDS expose les paramètres `memcached` MySQL comme paramètres d'option dans l'option Amazon RDS `MEMCACHED`.

Paramètres memcached MySQL

- `DAEMON_MEMCACHED_R_BATCH_SIZE` – Nombre entier qui spécifie combien d'opérations de lecture (get) `memcached` doivent être effectuées avant d'exécuter un COMMIT pour lancer une nouvelle transaction. Les valeurs autorisées sont comprises entre 1 et 4294967295, et celle par défaut est 1. L'option ne prend pas effet tant que l'instance n'est pas redémarrée.
- `DAEMON_MEMCACHED_W_BATCH_SIZE` – Nombre entier qui spécifie combien d'opérations d'écriture `memcached` comme add, set ou incr doivent être effectuées avant d'exécuter un COMMIT pour lancer une nouvelle transaction. Les valeurs autorisées sont comprises entre 1 et 4294967295, et celle par défaut est 1. L'option ne prend pas effet tant que l'instance n'est pas redémarrée.
- `INNODB_API_BK_COMMIT_INTERVAL` – Nombre entier qui spécifie la fréquence d'auto-commit des connexions inactives qui utilisent l'interface `memcached` InnoDB. Les valeurs autorisées sont comprises entre 1 et 1073741824, et celle par défaut est 5. L'option prend effet immédiatement, sans que vous ayez besoin de redémarrer l'instance.
- `INNODB_API_DISABLE_ROWLOCK` – Valeur booléenne qui désactive (1 (vrai)) ou active (0 (faux)) l'utilisation des verrouillages de ligne lorsque vous utilisez l'interface `memcached` InnoDB. La valeur par défaut est 0 (faux). L'option ne prend pas effet tant que l'instance n'est pas redémarrée.
- `INNODB_API_ENABLE_MDL` – Valeur booléenne qui, lorsqu'elle est configurée sur 0 (faux), verrouille la table utilisée par le plug-in `memcached` InnoDB pour ne pas qu'il puisse être abandonné ou modifié par une instruction DDL via l'interface SQL. La valeur par défaut est 0 (faux). L'option ne prend pas effet tant que l'instance n'est pas redémarrée.
- `INNODB_API_TRX_LEVEL` – Nombre entier qui spécifie le niveau d'isolation de la transaction pour les requêtes traitées par l'interface `memcached`. Les valeurs autorisées sont comprises entre 0 et 3. La valeur par défaut est 0. L'option ne prend pas effet tant que l'instance n'est pas redémarrée.

Amazon RDS configure ces paramètres `memcached` MySQL, ils ne peuvent pas être modifiés : `DAEMON_MEMCACHED_LIB_NAME`, `DAEMON_MEMCACHED_LIB_PATH` et `INNODB_API_ENABLE_BINLOG`. Les paramètres que les administrateurs MySQL configurent en utilisant `daemon_memcached_options` sont disponibles comme paramètres d'options `MEMCACHED` individuels dans Amazon RDS.

Paramètres MySQL daemon_memcached_options

- `BINDING_PROTOCOL`– Chaîne qui spécifie le protocole de liaison à utiliser. Les valeurs autorisées sont `auto`, `ascii` ou `binary`. La valeur par défaut est `auto`, ce qui signifie que le serveur négocie automatiquement le protocole avec le client. L'option ne prend pas effet tant que l'instance n'est pas redémarrée.
- `BACKLOG_QUEUE_LIMIT` – Nombre entier qui spécifie combien de connexions réseau peuvent être en attente de traitement par `memcached`. L'augmentation de cette limite peut réduire les erreurs reçues par un client qui ne peut pas se connecter à l'instance `memcached`, mais n'améliore pas les performances du serveur. Les valeurs autorisées sont comprises entre 1 et 2048, et celle par défaut est 1024. L'option ne prend pas effet tant que l'instance n'est pas redémarrée.
- `CAS_DISABLED` – Valeur booléenne qui active (1 (vrai)) ou désactive (0 (faux)) l'utilisation de la fonction CAS (Compare and Swap), ce qui réduit la taille par élément de 8 octets. La valeur par défaut est 0 (faux). L'option ne prend pas effet tant que l'instance n'est pas redémarrée.
- `CHUNK_SIZE` – Nombre entier qui spécifie la taille minimum du bloc, en octets, à attribuer à la clé, à la valeur et aux indicateurs de l'élément le plus petit. Les valeurs autorisées sont comprises entre 1 et 48. La valeur par défaut est 48 et vous pouvez considérablement améliorer l'efficacité de la mémoire avec une valeur inférieure. L'option ne prend pas effet tant que l'instance n'est pas redémarrée.
- `CHUNK_SIZE_GROWTH_FACTOR` – Nombre flottant qui contrôle la taille des nouveaux blocs. La taille d'un nouveau bloc correspond à la taille du bloc précédent multipliée par `CHUNK_SIZE_GROWTH_FACTOR`. Les valeurs autorisées sont comprises entre 1 et 2, et celle par défaut est 1.25. L'option ne prend pas effet tant que l'instance n'est pas redémarrée.
- `ERROR_ON_MEMORY_EXHAUSTED` – Valeur booléenne qui, lorsqu'elle est configurée sur 1 (vrai), spécifie que `memcached` renverra une erreur plutôt que d'expulser les éléments lorsqu'il n'y a plus de mémoire pour les stocker. S'il est configuré sur 0 (faux), `memcached` expulse les éléments s'il n'y a plus de mémoire. La valeur par défaut est 0 (faux). L'option ne prend pas effet tant que l'instance n'est pas redémarrée.
- `MAX_SIMULTANEOUS_CONNECTIONS` – Nombre entier qui spécifie le nombre maximum de connexions simultanées. La configuration de cette valeur sur n'importe quel chiffre inférieur à 10 empêche MySQL de démarrer. Les valeurs autorisées sont comprises entre 10 et 1024, et celle par défaut est 1024. L'option ne prend pas effet tant que l'instance n'est pas redémarrée.
- `VERBOSITY` – Chaîne qui spécifie le niveau d'informations consignées dans le journal d'erreurs MySQL par le service `memcached`. La valeur est v. L'option ne prend pas effet tant que l'instance n'est pas redémarrée. Les valeurs autorisées sont :
  - `v` – Journalise les erreurs et avertissements pendant l'exécution de la boucle principale d'évènements.
  - `vv` – Outre les informations consignées par v, journalise également la commande de chaque client et la réponse.
  - `vvv` – Outre les informations consignées par vv, journalise également les transitions d'état interne.

Amazon RDS configure ces paramètres MySQL `DAEMON_MEMCACHED_OPTIONS`, ils ne peuvent pas être modifiés : `DAEMON_PROCESS`, `LARGE_MEMORY_PAGES`, `MAXIMUM_CORE_FILE_LIMIT`, `MAX_ITEM_SIZE`, `LOCK_DOWN_PAGE_MEMORY`, `MASK`, `IDFILE`, `REQUESTS_PER_EVENT`, `SOCKET` et `USER`.

Tâches DBA courantes pour les instances de base de données MySQL

Cette section décrit les implémentations spécifiques à Amazon RDS de certaines tâches d'administration de base de données courantes pour les instances de base de données exécutant le moteur de base de données MySQL. Pour offrir une expérience de service géré, Amazon RDS ne fournit pas l'accès shell aux instances de bases de données et limite l'accès à certaines tables et procédures système qui requièrent des privilèges avancés.

Pour de plus amples informations sur l'utilisation des fichiers journaux MySQL sur Amazon RDS, veuillez consulter Fichiers journaux de base de données MySQL (p. 506)

Rubriques

- Mettre fin à une session ou à une requête (p. 881)
- Ignorer une erreur de réplication (p. 881)
- Utilisation des tablespaces InnoDB pour améliorer les temps de récupération sur incident (p. 882)
- Gestion de l'historique global des statuts (p. 884)

Mettre fin à une session ou à une requête

Vous pouvez mettre fin aux sessions d'utilisateur ou requêtes sur les instances de base de données à l'aide des commandes `rds_kill` et `rds_kill_query`. Connectez-vous d'abord à votre instance de base de données MySQL, puis émettez la commande appropriée comme illustré ci-après. Pour plus d'informations, consultez Connexion à une instance de base de données exécutant le moteur de base de données MySQL (p. 793).

```
CALL mysql.rds_kill(thread-ID)
CALL mysql.rds_kill_query(thread-ID)
```

Par exemple, pour arrêter la session qui s'exécute sur le thread 99, entrez la commande suivante :

```
CALL mysql.rds_kill(99);
```

Pour arrêter la requête qui s'exécute sur le thread 99, entrez la commande suivante :

```
CALL mysql.rds_kill_query(99);
```

Ignorer une erreur de réplication

Amazon RDS fournit un mécanisme qui vous permet d'ignorer une erreur sur vos réplicas en lecture, si l'erreur entraîne une absence de réponse du réplica en lecture et qu'elle n'affecte pas l'intégrité de vos données. Connectez-vous d'abord à votre instance de base de données MySQL, puis émettez les commandes appropriées comme illustré ci-après. Pour plus d'informations, consultez Connexion à une instance de base de données exécutant le moteur de base de données MySQL (p. 793).

> Note
>
> D'abord, vérifiez que l'erreur peut être ignorée en toute sécurité. Dans un utilitaire MySQL, connectez-vous au réplica en lecture et exécutez la commande MySQL suivante :

```
SHOW SLAVE STATUS\G
```

Pour de plus amples informations sur les valeurs renvoyées, veuillez consulter la documentation MySQL.

Pour ignorer l'erreur, vous pouvez émettre la commande suivante :

```
CALL mysql.rds_skip_repl_error;
```

Cette commande n'a aucun effet si vous l'exécutez sur l'instance de base de données source ou sur un réplica en lecture qui n'a rencontré aucune erreur de réplication.

Pour plus d'informations, telles que les versions de MySQL qui prennent en charge `mysql.rds_skip_repl_error`, consultez mysql.rds_skip_repl_error (p. 917).

> **Important**
>
> Si vous essayez d'appeler mysql.rds_skip_repl_error et que vous rencontrez l'erreur suivante : `ERROR 1305 (42000): PROCEDURE mysql.rds_skip_repl_error does not exist`, mettez à niveau votre instance de base de données MySQL avec la dernière version mineure ou avec l'une des versions mineures minimales répertoriées dans mysql.rds_skip_repl_error (p. 917).

Utilisation des tablespaces InnoDB pour améliorer les temps de récupération sur incident

Chaque table de MySQL se compose d'une définition de table, de données et d'index. Le moteur de stockage MySQL InnoDB stocke les données de table et les index dans un tablespace. InnoDB crée un espace de table global partagé qui contient un dictionnaire de données et autres métadonnées pertinentes, et peut contenir des données de table et des index. InnoDB peut aussi créer des espaces de table distincts pour chaque table et partition. Ces espaces de table distincts sont stockés dans des fichiers ayant .ibd comme extension et l'en-tête de chaque espace de table contient un numéro qui l'identifie de façon unique.

Amazon RDS fournit un paramètre dans un groupe de paramètres MySQL appelé `innodb_file_per_table`. Ce paramètre contrôle le fait qu'InnoDB ajoute ou non de nouvelles données et de nouveaux index de tableaux au tablespace partagé (en réglant la valeur du paramètre à 0) ou à des tablespaces individuels (en réglant la valeur du paramètre à 1). Amazon RDS règle la valeur par défaut pour le paramètre `innodb_file_per_table` à 1, ce qui vous permet de vous débarrasser de tableaux InnoDB individuels afin de libérer de l'espace de stockage utilisé par ces tableaux pour l'instance de base de données. Dans la plupart des cas d'utilisation, la définition du paramètre `innodb_file_per_table` à la valeur 1 est celle recommandée.

Vous devez définir le paramètre `innodb_file_per_table` à la valeur 0 quand vous avez un nombre important de tables, tel que plus de 1 000 tables quand vous utilisez le stockage SSD standard (magnétique) ou à visée générale, ou plus de 10 000 tables quand vous utilisez le stockage IOPS provisionnées. Lorsque vous définissez ce paramètre à la valeur 0, les espaces de table individuels ne sont pas créés et cela peut améliorer le temps nécessaire pour la récupération sur incident de base de données.

MySQL traite chaque fichier de métadonnées, espaces de tables inclus, pendant le cycle de récupération sur incident. Le temps nécessaire à MySQL pour traiter les informations de métadonnées dans l'espace de table partagé est négligeable en comparaison du temps qu'il faut pour traiter des milliers de fichiers d'espace de table quand il y a plusieurs espaces de table. Comme le nombre d'espaces de table est stocké au sein de l'en-tête de chaque fichier, le temps total nécessaire pour lire tous les fichiers d'espace de table peut prendre jusqu'à plusieurs heures. Par exemple, un million d'espaces de table InnoDB sur un stockage

standard peut nécessiter entre cinq et huit heures de traitement pendant un cycle de récupération sur incident. Dans certains, InnoDB peut déterminer qu'il a besoin d'un nettoyage supplémentaire après un cycle de récupération sur incident et, par conséquent, entamera un autre cycle de récupération sur incident, ce qui augmente le temps total de récupération. Gardez à l'esprit qu'un cycle de récupération sur incident implique aussi la restauration de transactions, la correction des pages rompues et autres opérations en plus du traitement des informations sur les espaces de table.

Comme le paramètre `innodb_file_per_table` réside dans un groupe de paramètres, vous pouvez modifier la valeur du paramètre en modifiant le groupe de paramètres utilisé par votre instance de base de données sans avoir à redémarrer celle-ci. Une fois que la valeur est modifiée, de la valeur 1 (créer des tables individuelles) à la valeur 0 (utiliser un espace de table partagé), par exemple, les nouvelles tables InnoDB sont ajoutées à l'espace de table partagé, pendant que les tables existantes continuent d'avoir des espaces de table individuels. Pour déplacer une table InnoDB vers l'espace de table partagé, vous devez utiliser la commande `ALTER TABLE`.

Migration de plusieurs espaces de table vers l'espace de table partagé

Vous pouvez déplacer les métadonnées d'une table InnoDB de son propre espace de table vers l'espace de table partagé, ce qui recrée les métadonnées de la table selon la valeur du paramètre `innodb_file_per_table`. Connectez-vous d'abord à votre instance de base de données MySQL, puis émettez les commandes appropriées comme illustré ci-après. Pour plus d'informations, consultez Connexion à une instance de base de données exécutant le moteur de base de données MySQL (p. 793).

```
ALTER TABLE table_name ENGINE = InnoDB, ALGORITHM=COPY;
```

Par exemple, la requête suivante retourne une instruction `ALTER TABLE` pour chaque table InnoDB qui ne figure pas dans l'espace de table partagé.

Pour les instances de base de données MySQL 5.6 et 5.7 :

```
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','');
```

Pour les instances de base de données MySQL 8.0 :

```
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','');
```

La reconstruction d'une table MySQL pour déplacer les métadonnées de la table vers l'espace de table partagé nécessite temporairement un espace de stockage supplémentaire pour recréer la table et, par conséquent, l'instance de base de données doit avoir un espace de stockage disponible. Pendant la reconstruction, la table est verrouillée et inaccessible aux requêtes. Pour les petites tables ou les tables qui ne sont pas fréquemment consultées, ce n'est pas nécessairement un problème. Pour les tables volumineuses ou fréquemment consultées dans un environnement fortement concurrentiel, vous pouvez reconstruire les tables sur un réplica en lecture.

Vous pouvez créer un réplica en lecture et migrer les métadonnées de la table vers l'espace de table partagé du réplica en lecture. Tant que l'instruction ALTER TABLE bloque l'accès sur le réplica en lecture, l'instance de base de données source n'est pas impactée. L'instance de base de données source continue à générer ses journaux binaires, tandis que le réplica en lecture ralentit pendant le processus de reconstruction de la table. Étant donné que la reconstruction exige un espace de stockage supplémentaire et que le fichier journal de relecture peut devenir volumineux, vous devriez créer un réplica en lecture dont la capacité de stockage allouée est supérieure à l'instance de base de données source.

Pour créer un réplica en lecture et reconstruire les tables InnoDB afin d'utiliser l'espace de table partagé, procédez comme suit :

1. Assurez-vous que la rétention des sauvegardes est activée sur l'instance de base de données source de sorte que la journalisation binaire soit activée.
2. Utilisez AWS Management Console ou AWS CLI pour créer un réplica en lecture pour l'instance de base de données source. Étant donné que la création d'un réplica en lecture implique un grand nombre de processus semblables à ceux de la récupération sur incident, le processus de création peut prendre un certain temps si le nombre d'espaces de table InnoDB est élevé. Allouez plus d'espace de stockage sur le réplica en lecture qu'il n'en est actuellement utilisé sur l'instance de base de données source.
3. Lorsque le réplica en lecture a été créé, créez un groupe de paramètres avec les valeurs de paramètre `read_only = 0` et `innodb_file_per_table = 0`. Associez ensuite le groupe de paramètres au réplica en lecture.
4. Émettez l'instruction SQL suivante pour toutes les tables que vous souhaitez migrer sur le réplica :

```
ALTER TABLE name ENGINE = InnoDB
```

5. Une fois que toutes vos instructions `ALTER TABLE` sont terminées sur le réplica en lecture, vérifiez que celui-ci est connecté à l'instance de base de données source et que les deux instances sont synchronisées.
6. Utilisez la console ou l'interface de ligne de commande pour promouvoir le réplica en lecture comme instance. Assurez-vous que le groupe de paramètres utilisé pour la nouvelle instance de base de données autonome a le paramètre `innodb_file_per_table` défini sur 0. Modifiez le nom de la nouvelle instance de base de données autonome et pointez toutes les applications vers la nouvelle instance de base de données autonome.

Gestion de l'historique global des statuts

MySQL gère de nombreuses variables d'état qui fournissent des informations sur son fonctionnement. Leur valeur peut vous aider à détecter les problèmes de verrouillage ou de mémoire d'une instance de base de données. Les valeurs de ces variables d'état se cumulent depuis le dernier démarrage de l'instance de base de données. Vous pouvez réinitialiser à la valeur 0 la plupart des variables d'état à l'aide de la commande `FLUSH STATUS`.

Pour autoriser la surveillance de ces valeurs au fil du temps, Amazon RDS fournit un ensemble de procédures qui prennent un instantané des valeurs de ces variables et les écrivent dans une table, ainsi que toutes les modifications intervenues depuis le dernier instantané. Cette infrastructure, appelée historique global des statuts (GoSH, Global Status History), est installée sur toutes les instances de base de données MySQL à partir des versions 5.5.23. GoSH est désactivé par défaut.

Pour activer GoSH, vous devez d'abord activer le planificateur d'événement à partir d'un groupe de paramètres DB en définissant le paramètre event_scheduler avec la valeur ON. Pour plus d'informations sur la création et la modification d'un groupe de paramètres DB, consultez Utilisation de groupes de paramètres de base de données (p. 225).

Vous pouvez ensuite utiliser les procédures du tableau suivant pour activer et configurer GoSH. Connectez-vous d'abord à votre instance de base de données MySQL, puis émettez les commandes

appropriées comme illustré ci-après. Pour plus d'informations, consultez Connexion à une instance de base de données exécutant le moteur de base de données MySQL (p. 793). Pour chaque procédure, entrez ce qui suit :

```
CALL procedure-name;
```

Où procedure-name est l'une des procédures du tableau.

Procédure	Description
`mysql.rds_enable_gsh_collector`	Active l'infrastructure GoSH pour prendre des instantanés par défaut à intervalles spécifiés par `rds_set_gsh_collector`.
`mysql.rds_set_gsh_collector`	Spécifie l'intervalle, en minutes, entre les instantanés. La valeur par défaut est 5.
`mysql.rds_disable_gsh_collector`	Désactive les instantanés.
`mysql.rds_collect_global_status_history`	Prend un instantané sur demande.
`mysql.rds_enable_gsh_rotation`	Active la rotation du contenu de la table `mysql.rds_global_status_history` en `mysql.rds_global_status_history_old` à intervalles spécifiés par `rds_set_gsh_rotation`.
`mysql.rds_set_gsh_rotation`	Spécifie l'intervalle, en jours, entre deux rotations de table. La valeur par défaut est 7.
`mysql.rds_disable_gsh_rotation`	Désactive la rotation de table.
`mysql.rds_rotate_global_status_history`	Effectue une rotation du contenu de la table `mysql.rds_global_status_history` en `mysql.rds_global_status_history_old` à la demande.

Lorsque l'infrastructure GoSH est en cours d'exécution, vous pouvez interroger les tables sur lesquelles elle écrit. Par exemple, pour interroger le taux d'accès du groupe de tampons Innodb, vous devez émettre la requête suivante :

```
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'
```

Utilisation de l'authentification Kerberos pour MySQL

Vous pouvez utiliser l'authentification Kerberos pour authentifier les utilisateurs lorsqu'ils se connectent à votre instance de base de données MySQL. L'instance de base de données fonctionne avec AWS Directory Service for Microsoft Active Directory (Enterprise Edition) (AWS Managed Microsoft AD) pour permettre l'authentification Kerberos. Lorsque les utilisateurs s'authentifient avec une instance de base de

données MySQL jointe au domaine d'approbation, les demandes d'authentification sont transférées. Les demandes transférées vont dans l'annuaire de domaine que vous créez avec AWS Directory Service.

Vous pouvez gagner du temps et de l'argent en conservant toutes les informations d'identification dans le même annuaire. Cette approche vous permet d'avoir un endroit centralisé de stockage et de gestion des informations d'identification pour plusieurs instances de base de données. L'utilisation d'un annuaire peut également améliorer votre profil de sécurité global.

Amazon RDS prend en charge l'authentification Kerberos pour les instances de base de données MySQL dans les régions AWS suivantes :

- USA Est (Ohio)
- USA Est (Virginie du Nord)
- USA Ouest (Californie du Nord)
- USA Ouest (Oregon)
- Asie-Pacifique (Mumbai)
- Asie-Pacifique (Séoul)
- Asie-Pacifique (Singapour)
- Asie-Pacifique (Sydney)
- Asie-Pacifique (Tokyo)
- Canada (Centre)
- Europe (Francfort)
- Europe (Irlande)
- Europe (Londres)
- Europe (Stockholm)
- Amérique du Sud (São Paulo)
- Chine (Pékin)
- Chine (Ningxia)

Pour configurer l'authentification Kerberos pour une instance de base de données MySQL, effectuez les étapes générales suivantes, décrites plus en détails par la suite :

1. Utilisez AWS Managed Microsoft AD pour créer un annuaire AWS Managed Microsoft AD. Vous pouvez utiliser l'AWS Management Console, l'AWS CLI ou l'API AWS Directory Service pour créer l'annuaire. Pour de plus amples informations à ce sujet, veuillez consulter Créez votre annuaire AWS Managed Microsoft AD dans le AWS Directory Service Administration Guide.
2. Créez un rôle AWS Identity and Access Management (IAM) qui utilise la stratégie IAM `AmazonRDSDirectoryServiceAccess` gérée. Le rôle autorise Amazon RDS à effectuer des appels vers votre annuaire.

   Pour que le rôle autorise l'accès, le point de terminaison AWS Security Token Service (AWS STS) doit être activé dans la région AWS pour votre compte AWS. Les points de terminaison AWS STS sont actifs par défaut dans toutes les régions AWS et vous pouvez les utiliser sans qu'aucune autre action soit nécessaire. Pour de plus amples informations, veuillez consulter Activation et désactivation d'AWS STS dans une région AWS dans le Guide de l'utilisateur IAM.
3. Créez et configurez des utilisateurs dans l'annuaire AWS Managed Microsoft AD à l'aide des outils Microsoft Active Directory. Pour de plus amples informations sur la création des utilisateurs dans votre annuaire Active Directory, veuillez consulter Gérer des utilisateurs et des groupes dans AWS Managed Microsoft AD dans le AWS Directory Service Administration Guide.
4. Créez ou modifiez une instance de base de données MySQL. Si vous utilisez l'interface de ligne de commande ou l'API RDS dans la demande de création, spécifiez un identificateur de domaine avec le

paramètre `Domain`. Utilisez l'identificateur `d-*` généré lors de la création de votre annuaire et le nom du rôle que vous avez créé.

Si vous modifiez une instance de base de données MySQL existante pour utiliser l'authentification Kerberos, définissez les paramètres de domaine et de rôle IAM pour l'instance de base de données. Recherchez l'instance de base de données dans le même VPC que l'annuaire de domaine.

5. Utilisez les informations d'identification de l'utilisateur principal Amazon RDS pour vous connecter à l'instance de base de données MySQL. Créez l'utilisateur dans MySQL en utilisant la clause `CREATE USER IDENTIFIED WITH 'auth_pam'`. Les utilisateurs que vous créez de cette façon peuvent se connecter à l'instance de base de données MySQL en utilisant l'authentification Kerberos.

Configuration de l'authentification Kerberos pour les instances de base de données MySQL

Vous utilisez AWS Managed Microsoft AD pour configurer l'authentification Kerberos pour une instance de base de données MySQL. Pour configurer l'authentification Kerberos, procédez comme suit :

Étape 1 : Créer un annuaire à l'aide d'AWS Managed Microsoft AD

AWS Directory Service crée un annuaire Active Directory totalement géré dans le Cloud AWS. Lorsque vous créez un annuaire AWS Managed Microsoft AD, AWS Directory Service crée deux contrôleurs de domaine et serveurs de système de noms de domaine (DNS) en votre nom. Les serveurs de répertoire sont créés dans des sous-réseaux différents d'un VPC. Cette redondance permet de s'assurer que votre annuaire reste accessible, y compris en cas de défaillance.

Lorsque vous créez un annuaire AWS Managed Microsoft AD, AWS Directory Service effectue les tâches suivantes en votre nom :

- Configuration d'un annuaire Active Directory dans le VPC.
- Création d'un compte d'administrateur d'annuaire avec le nom d'utilisateur Admin et le mot de passe spécifié. Ce compte est utilisé pour gérer votre annuaire.

  Note

  Assurez-vous d'enregistrer ce mot de passe, car AWS Directory Service ne le stocke pas. Vous pouvez le réinitialiser, mais vous ne pouvez pas le récupérer.
- Création d'un groupe de sécurité pour les contrôleurs de l'annuaire.

Lorsque vous lancez un AWS Managed Microsoft AD, AWS crée une unité d'organisation (UO) qui contient tous les objets de votre annuaire. Cette unité d'organisation, qui porte le nom NetBIOS que vous avez saisi lorsque vous avez créé votre annuaire, est située dans la racine du domaine. La racine du domaine appartient à AWS, qui la gère.

Le compte Admin qui a été créé avec votre annuaire AWS Managed Microsoft AD dispose des autorisations nécessaires pour les activités administratives les plus courantes pour votre unité d'organisation :

- Création, mise à jour et suppression des utilisateurs
- Ajouter des ressources à votre domaine, comme des serveurs de fichiers ou d'impression, puis attribuer des autorisations pour ces ressources aux utilisateurs dans votre unité d'organisation
- Créer des unités d'organisation et des conteneurs supplémentaires
- Déléguer des autorités

- Restaurer des objets supprimés de la corbeille Active Directory
- Exécuter des modules AD et DNS Windows PowerShell sur le service Web Active Directory

Le compte Admin dispose également de droits pour exécuter les activités suivantes au niveau du domaine :

- Gérer les configurations DNS (ajouter, supprimer ou mettre à jour des enregistrements, des zones et des redirecteurs)
- Afficher les journaux d'événements DNS
- Afficher les journaux d'événements de sécurité

Pour créer un annuaire avec AWS Managed Microsoft AD

1. Connectez-vous à la AWS Management Console et ouvrez la console AWS Directory Service à l'adresse https://console.aws.amazon.com/directoryservicev2/.
2. Dans le panneau de navigation, choisissez Annuaires, puis Configurer un annuaire.
3. Choisissez AWS Managed Microsoft AD. AWS Managed Microsoft AD est la seule option que vous pouvez utiliser actuellement avec Amazon RDS.
4. Entrez les informations suivantes :

   Nom de DNS de l'annuaire

   Nom complet de l'annuaire, par exemple **`corp.example.com`**.

   Nom NetBIOS de l'annuaire

   Nom court de l'annuaire, par exemple **`CORP`**.

   Description de l'annuaire

   (Facultatif) Une description de l'annuaire.

   Mot de passe administrateur

   Mot de passe de l'administrateur de l'annuaire. Le processus de création d'un annuaire crée un compte d'administrateur avec le nom d'utilisateur Admin et ce mot de passe.

   Le mot de passe de l'administrateur de l'annuaire ne peut pas contenir le terme « admin ». Le mot de passe est sensible à la casse et doit comporter entre 8 et 64 caractères. Il doit également contenir au moins un caractère de trois des quatre catégories suivantes :

   - Lettres minuscules (a–z)
   - Lettres majuscules (A–Z)
   - Chiffres (0–9)
   - Caractères non alphanumériques (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

   Confirmer le mot de passe

   Saisissez à nouveau le mot de passe de l'administrateur.
5. Choisissez Suivant.
6. Entrez les informations suivantes dans la section Mise en réseau, puis choisissez Suivant :

   VPC

   VPC de l'annuaire. Créez l'instance de base de données MySQL dans ce même VPC.

   Sous-réseaux

   Sous-réseaux pour les serveurs d'annuaires. Les deux sous-réseaux doivent être dans des zones de disponibilité différentes.

7. Vérifiez les informations concernant l'annuaire et effectuez les modifications nécessaires. Lorsque les informations sont correctes, choisissez Create directory (Créer l'annuaire).

La création de l'annuaire prend plusieurs minutes. Lorsqu'il est créé, la valeur du champ Statut devient Actif.

Pour consulter les informations relatives à votre annuaire, choisissez le nom de l'annuaire dans la liste. Notez la valeur ID de l'annuaire, car vous avez besoin de cette valeur lorsque vous créez ou modifiez votre instance de base de données MySQL.

Étape 2 : Créer le rôle IAM qui sera utilisé par Amazon RDS

Pour qu'Amazon RDS appelle AWS Directory Service pour vous, il est nécessaire de disposer d'un rôle IAM qui utilise la stratégie IAM gérée `AmazonRDSDirectoryServiceAccess`. Ce rôle permet à Amazon RDS d'effectuer des appels vers AWS Directory Service.

Lorsqu'une instance de base de données est créée à l'aide de l'AWS Management Console et que l'utilisateur de la console dispose de l'autorisation `iam:CreateRole`, la console crée ce rôle automatiquement. Dans ce cas, le nom du rôle est `rds-directoryservice-kerberos-access-role`. Sinon, vous devez créer le rôle IAM manuellement. Lorsque vous créez ce rôle IAM, choisissez `Directory Service` et attachez-lui la stratégie gérée AWS `AmazonRDSDirectoryServiceAccess`.

Pour de plus amples informations sur la création de rôles IAM pour un service, veuillez consulter Création d'un rôle pour déléguer des autorisations à un service AWS dans le IAM Guide de l'utilisateur.

> **Note**
>
> Le rôle IAM utilisé pour l'authentification Windows pour RDS for Microsoft SQL Server ne peut pas être utilisé pour RDS for MySQL.

Vous pouvez également créer des stratégies avec les autorisations obligatoires au lieu d'utiliser la stratégie gérée IAM `AmazonRDSDirectoryServiceAccess`. Dans ce cas, le rôle IAM doit avoir la stratégie d'approbation IAM suivante :

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "directoryservice.rds.amazonaws.com",
          "rds.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Le rôle doit également avoir la stratégie de rôle IAM suivante.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
    "Effect": "Allow",
    "Resource": "*"
    }
  ]
}
```

Étape 3 : Créer et configurer des utilisateurs

Vous pouvez créer des utilisateurs avec l'outil Active Directory Users and Computers (Utilisateurs et ordinateurs Active Directory). Cet outil fait partie des outils Active Directory Domain Services et Active Directory Lightweight Directory Services (Services de domaine Active Directory et Services d'annuaire légers Active Directory). Les utilisateurs représentent des individus ou des entités individuelles qui ont accès à votre annuaire.

Pour créer des utilisateurs dans un annuaire AWS Directory Service, vous devez être connecté à une instance Amazon EC2 basée sur Microsoft Windows. Cette instance doit être membre de l'annuaire AWS Directory Service et doit être connectée en tant qu'utilisateur disposant des privilèges nécessaires pour créer des utilisateurs. Pour de plus amples informations, veuillez consulter Gérer des utilisateurs et des groupes dans AWS Managed Microsoft AD dans le Guide d'administration d'AWS Directory Service.

Étape 4 : Créer ou modifier une instance de base de données MySQL

Créez ou modifiez une instance de base de données MySQL à utiliser avec votre annuaire. Vous pouvez utiliser la console, l'interface de ligne de commande ou l'API RDS pour associer une instance de base de données à un annuaire. Vous pouvez effectuer cette opération de différentes manières :

- Créez une instance de base de données MySQL à l'aide de la console, de la commande de l'interface de ligne de commande create-db-instance ou de l'opération d'API RDS CreateDBInstance.

  Pour obtenir des instructions, consultez Création d'une instance de base de données Amazon RDS (p. 146).

- Modifiez une instance de base de données MySQL existante à l'aide de la console, de la commande de l'interface de ligne de commande modify-db-instance ou de l'opération d'API RDS ModifyDBInstance.

  Pour obtenir des instructions, consultez Modification d'une instance de base de données Amazon RDS (p. 243).
- Restaurez une instance de base de données MySQL à partir d'un instantané de bases de données à l'aide de la console, de la commande d'interface de ligne de commande restore-db-instance-from-db-snapshot ou de l'opération d'API RDS RestoreDBInstanceFromDBSnapshot.

  Pour obtenir des instructions, consultez Restauration à partir d'un instantané de base de données (p. 329).
- Restaurez une instance de base de données MySQL à un moment donné en utilisant la console, la commande d'interface de ligne de commande restore-db-instance-to-point-in-time ou l'opération d'API RDS RestoreDBInstanceToPointInTime.

  Pour obtenir des instructions, consultez Restauration d'une instance de base de données à une date spécifiée (p. 365).

L'authentification Kerberos est uniquement prise en charge pour les instances de base de données MySQL dans un VPC. L'instance de base de données peut être dans le même VPC que l'annuaire ou dans un VPC différent. L'instance de base de données doit utiliser un groupe de sécurité qui accepte les sorties du VPC, afin que l'instance de base de données puisse communiquer avec l'annuaire.

Lorsque vous utilisez la console pour créer une instance de base de données, choisissez Mot de passe et authentification Kerberos dans la section Authentification de base de données. Choisissez Parcourir les annuaires, puis sélectionnez l'annuaire, ou choisissez Créer un nouvel annuaire.

Lorsque vous utilisez la console pour modifier ou restaurer une instance de base de données, choisissez l'annuaire dans la section Authentification Kerberos ou choisissez Créer un nouvel annuaire.

Vous pouvez utiliser l'interface de ligne de commande ou l'API RDS pour associer une instance de base de données à un annuaire. Les paramètres suivants sont nécessaires pour que l'instance de base de données puisse utiliser l'annuaire du domaine que vous avez créé :

- Pour le paramètre `--domain`, vous devez indiquer l'identifiant du domaine (identifiant « d-* ») généré lors de la création de l'annuaire.
- Pour le paramètre `--domain-iam-role-name`, utilisez le rôle que vous avez créé qui utilise la stratégie IAM gérée `AmazonRDSDirectoryServiceAccess`.

Par exemple, la commande d'interface de ligne de commande suivante modifie une instance de base de données de façon à utiliser un annuaire.

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --domain d-ID \
    --domain-iam-role-name role-name
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --domain d-ID ^
    --domain-iam-role-name role-name
```

> **Important**
>
> Si vous modifiez une instance de base de données de façon à activer l'authentification Kerberos, redémarrez l'instance de base de données après avoir effectué la modification.

Étape 5 : Créer les connexions MySQL d'authentification Kerberos

Utilisez les informations d'identification de l'utilisateur principal Amazon RDS pour vous connecter à l'instance de base de données MySQL comme vous le faites pour n'importe quelle instance de base de données. L'instance de base de données est jointe au domaine AWS Managed Microsoft AD. Vous pouvez ainsi allouer les connexions et utilisateurs MySQL depuis les utilisateurs Active Directory de votre domaine. Les autorisations de base de données sont gérées via des autorisations MySQL standard qui sont accordées et révoquées à partir de ces connexions.

Vous pouvez autoriser un utilisateur Active Directory à s'authentifier avec MySQL. Pour ce faire, utilisez d'abord les informations d'identification de l'utilisateur principal Amazon RDS pour vous connecter à l'instance de base de données MySQL comme avec n'importe quelle autre instance de base de données. Une fois connecté, créez un utilisateur authentifié en externe avec PAM (Pluggable Authentication Modules) dans MySQL comme indiqué ci-dessous.

```
CREATE USER 'testuser'@'%' IDENTIFIED WITH 'auth_pam';
UPDATE mysql.user SET ssl_type = 'any' WHERE ssl_type = '' AND PLUGIN = 'auth_pam' and USER
 = 'testuser';
FLUSH PRIVILEGES;
```

Remplacez *testuser* par le nom de l'utilisateur. Les utilisateurs (personnes et applications) de votre domaine peuvent désormais se connecter à l'instance de base de données à partir d'un ordinateur client joint au domaine à l'aide de l'authentification Kerberos.

> **Important**
>
> Nous recommandons fortement aux clients d'utiliser des connexions SSL/TLS lors de l'utilisation de l'authentification PAM. S'ils n'utilisent pas de connexions SSL/TLS, le mot de passe peut être envoyé sous forme de texte clair dans certains cas.

Gestion d'une instance de base de données dans un domaine

Vous pouvez utiliser l'interface de ligne de commande ou l'API RDS pour gérer votre instance de base de données et sa relation avec votre annuaire géré Active Directory. Par exemple, vous pouvez associer un annuaire Active Directory pour l'authentification Kerberos et dissocier un annuaire Active Directory pour désactiver l'authentification Kerberos. Vous pouvez également transférer une instance de base de données vers une autre afin qu'elle soit authentifiée en externe par un annuaire Active Directory.

Par exemple, l'API Amazon RDS vous permet d'effectuer les actions suivantes :

- Pour retenter l'activation de l'authentification Kerberos en cas d'échec d'appartenance, utilisez l'opération d'API `ModifyDBInstance` et spécifiez l'ID d'annuaire d'appartenance actuelle.
- Pour mettre à jour le nom du rôle IAM de l'appartenance, utilisez l'opération d'API `ModifyDBInstance` et spécifiez l'ID d'annuaire de l'appartenance actuelle et le nouveau rôle IAM.
- Pour désactiver l'authentification Kerberos sur une instance de base de données, utilisez l'opération d'API `ModifyDBInstance` et spécifiez `none` comme paramètre de domaine.
- Pour déplacer une instance de base de données d'un domaine à un autre, utilisez l'opération d'API `ModifyDBInstance` et spécifiez l'identifiant du nouveau domaine en tant que paramètre de domaine.
- Pour répertorier l'appartenance pour chaque instance de base de données, utilisez l'opération d'API `DescribeDBInstances`.

Présentation de l'appartenance au domaine

Après la création ou la modification de votre instance de base de données, elle devient un membre du domaine. Vous pouvez consulter le statut de l'appartenance au domaine pour l'instance de base de données en exécutant la commande d'interface de ligne de commande describe-db-instances. Le statut de l'instance de base de données peut avoir les valeurs suivantes :

- `kerberos-enabled` – L'instance de base de données a l'authentification Kerberos activée.
- `enabling-kerberos` – AWS est en train d'activer l'authentification Kerberos sur cette instance de base de données.
- `pending-enable-kerberos` – L'activation de l'authentification Kerberos est en attente sur cette instance de base de données.
- `pending-maintenance-enable-kerberos` – AWS tentera d'activer l'authentification Kerberos sur cette instance de base de données lors de la prochaine fenêtre de maintenance planifiée.
- `pending-disable-kerberos` – La désactivation de l'authentification Kerberos est en attente sur cette instance de base de données.
- `pending-maintenance-disable-kerberos` – AWS tentera de désactiver l'authentification Kerberos sur cette instance de base de données lors de la prochaine fenêtre de maintenance planifiée.
- `enable-kerberos-failed` – Un problème de configuration a empêché AWS d'activer l'authentification Kerberos sur l'instance de base de données. Vérifiez et corrigez votre configuration avant d'émettre à nouveau la commande de modification de l'instance de base de données.

- `disabling-kerberos` – AWS est en train de désactiver l'authentification Kerberos sur cette instance de base de données.

Une demande d'activation de l'authentification Kerberos peut échouer à cause d'un problème de connectivité réseau ou d'un rôle IAM incorrect. Par exemple, supposons que vous créez une instance de base de données ou modifiez une instance de base de données et que la tentative d'activation de l'authentification Kerberos échoue. Si cela se produit, réémettez la commande modify ou modifiez l'instance de base de données nouvellement créée pour joindre le domaine.

Connexion à MySQL avec l'authentification Kerberos

Pour vous connecter à MySQL avec l'authentification Kerberos, vous devez vous connecter à l'aide du type d'authentification Kerberos.

Pour créer un utilisateur de base de données auquel vous pouvez vous connecter à l'aide de l'authentification Kerberos, utilisez une clause `IDENTIFIED WITH` avec l'instruction `CREATE USER`. Pour obtenir des instructions, consultez Étape 5 : Créer les connexions MySQL d'authentification Kerberos (p. 893).

Pour éviter les erreurs, utilisez le client `mysql` MariaDB. Vous pouvez télécharger le logiciel MariaDB à l'adresse https://downloads.mariadb.org/.

À partir d'une invite de commande, connectez-vous à un des points de terminaison associés à votre instance de base de données MySQL. Suivez les procédures générales décrites dans Connexion à une instance de base de données exécutant le moteur de base de données MySQL (p. 793). Lorsque vous êtes invité à entrer le mot de passe, entrez le mot de passe Kerberos associé à ce nom d'utilisateur.

Restauration d'une instance de base de données MySQL et ajout de cette instance à un domaine

Vous pouvez restaurer un instantané de base de données ou effectuer une restauration à un instant donné pour une instance de base de données MySQL, puis l'ajouter à un domaine. Une fois que l'instance de base de données est restaurée, modifiez l'instance de base de données à l'aide du processus expliqué dans Étape 4 : Créer ou modifier une instance de base de données MySQL (p. 891) afin d'ajouter l'instance de base de données à un domaine.

Limitations MySQL de l'authentification Kerberos

Les limitations suivantes s'appliquent à l'authentification Kerberos pour MySQL :

- Il n'y a pas de prise en charge des répertoires Active Directory gérés ayant été partagés avec vous.
- L'authentification Kerberos est prise en charge pour les versions Amazon RDS for MySQL suivantes :
  - Amazon RDS for MySQL version 8.0.13, 8.0.15 et 8.0.16
  - Amazon RDS for MySQL version 5.7.24, 5.7.25 et 5.7.26
- Vous devez redémarrer l'instance de base de données après avoir activé la fonctionnalité.
- La longueur du nom de domaine ne peut pas dépasser 61 caractères.
- Vous ne pouvez pas activer l'authentification Kerberos et l'authentification IAM en même temps. Choisissez l'une ou l'autre des méthodes d'authentification pour votre instance de base de données MySQL.
- Ne modifiez pas le port d'instance de base de données après avoir activé la fonctionnalité.
- N'utilisez pas l'authentification Kerberos avec les réplicas en lecture.
- Pour supprimer une instance de base de données pour laquelle cette fonctionnalité est activée, désactivez d'abord la fonctionnalité. Pour ce faire, utilisez la commande d'interface de ligne de

commande `modify-db-instance` pour l'instance de base de données et spécifiez `none` pour le paramètre `--domain`.

Si vous utilisez l'interface de ligne de commande ou l'API RDS pour supprimer une instance de base de données pour laquelle cette fonctionnalité est activée, laissez s'écouler un délai.

Limites et problèmes connus pour MySQL sur Amazon RDS

Les limites et les problèmes connus liés à l'utilisation de MySQL sur Amazon RDS sont répertoriés ci-dessous.

Rubriques

- Taille de pool de mémoires tampons InnoDB incohérente (p. 896)
- L'optimisation de la fusion d'index retourne des résultats erronés (p. 896)
- Taille des fichiers journaux (p. 897)
- Exceptions des paramètres MySQL pour les instances de base de données Amazon RDS (p. 897)
- Limites de taille des fichiers MySQL dans Amazon RDS (p. 898)
- Plug-in MySQL Keyring non pris en charge (p. 899)

Taille de pool de mémoires tampons InnoDB incohérente

Pour MySQL 5.7, il y a actuellement un bogue dans la manière dont la taille du pool de mémoires tampons InnoDB est gérée. MySQL 5.7 peut ajuster la valeur du paramètre `innodb_buffer_pool_size` sur une valeur importante qui peut entraîner un développement trop important du pool de mémoires tampons InnoDB et l'utilisation d'un trop gros volume de mémoire. Cet effet peut entraîner l'arrêt de l'exécution du moteur de base de données MySQL ou empêcher le démarrage du moteur de base de données MySQL. Ce problème est plus courant pour des classes d'instance de base de données dont l'espace mémoire disponible est moindre.

Pour résoudre ce problème, définissez la valeur du paramètre `innodb_buffer_pool_size` sur un multiple du produit des valeurs de paramètre `innodb_buffer_pool_instances` et `innodb_buffer_pool_chunk_size`. Par exemple, vous pouvez définir la valeur de paramètre `innodb_buffer_pool_size` sur un multiple de huit fois le produit des valeurs de paramètre `innodb_buffer_pool_instances` et `innodb_buffer_pool_chunk_size`, comme illustré dans l'exemple suivant.

```
innodb_buffer_pool_chunk_size = 536870912
innodb_buffer_pool_instances = 4
innodb_buffer_pool_size = (536870912 * 4) * 8 = 17179869184
```

Pour plus d'informations sur le bogue MySQL 5.7, consultez https://bugs.mysql.com/bug.php?id=79379 dans la documentation MySQL.

L'optimisation de la fusion d'index retourne des résultats erronés

Les requêtes qui utilisent d'optimisation de fusionnement d'index peuvent produire des résultats fautifs en raison d'un bogue dans l'optimiseur de requête MySQL introduit avec MySQL 5.5.37. Lorsque vous publiez

une requête contre un tableau avec plusieurs index, l'optimiseur analyse des plages de rangées selon les multiples index, mais il ne fusionne pas correctement les résultats. Pour plus d'informations sur le bogue de l'optimiseur de requête, accédez à http://bugs.mysql.com/bug.php?id=72745 et http://bugs.mysql.com/bug.php?id=68194 dans la base de données des bogues MySQL.

Par exemple, imaginons une requête sur une table avec deux index où les arguments de la recherche font référence aux colonnes indexées.

```
SELECT * FROM table1
WHERE indexed_col1 = 'value1' AND indexed_col2 = 'value2';
```

Dans ce cas, le moteur de recherche analysera les deux index. Néanmoins, en raison du bogue, les résultats fusionnés sont incorrects.

Pour résoudre ce problème, vous pouvez procéder de l'une des manières suivantes :

- Définissez le paramètre `optimizer_switch` sur `index_merge=off` dans le groupe de paramètres DB de votre instance de base de données MySQL. Pour plus d'informations sur la définition des paramètres d'un groupe de paramètres DB, consultez Utilisation de groupes de paramètres de base de données (p. 225).
- Mettez à niveau votre instance de base de données vers MySQL version 5.6, 5.7 ou 8.0. Pour plus d'informations, consultez Mise à niveau d'un instantané de base de données MySQL (p. 813).
- Si vous ne pouvez pas mettre à niveau votre instance ou modifier le paramètre `optimizer_switch`, vous pouvez contourner le bogue en identifiant explicitement un index pour la requête, par exemple :

```
SELECT * FROM table1
USE INDEX covering_index
WHERE indexed_col1 = 'value1' AND indexed_col2 = 'value2';
```

Pour de plus amples informations, veuillez consulter Optimisation de la fusion d'index.

Taille des fichiers journaux

Pour MySQL, une taille limite est appliquée aux objets BLOB écrits dans le fichier journal redo. Pour prendre en compte cette limite, vérifiez que le paramètre `innodb_log_file_size` de votre instance de base de données MySQL est dix fois supérieur à la taille des données BLOB les plus volumineuses figurant dans vos tables, plus la longueur des autres champs de longueur variable (`VARCHAR`, `VARBINARY`, `TEXT`) dans ces tables. Pour plus d'informations sur la manière de définir les valeurs des paramètres, consultez Utilisation de groupes de paramètres de base de données (p. 225). Pour plus d'informations sur la taille limite des objets BLOB du fichier journal redo, accédez à Changements dans MySQL 5.6.20.

Exceptions des paramètres MySQL pour les instances de base de données Amazon RDS

Certains paramètres MySQL nécessitent des considérations spéciales lors d'une utilisation avec une instance de base de données Amazon RDS.

lower_case_table_names

Du fait que Amazon RDS utilise un système de fichiers qui respecte la casse, la définition de la valeur du paramètre du serveur `lower_case_table_names` sur 2 (« noms stockés comme donnés mais comparés en minuscules ») n'est pas prise en charge. Voici les valeurs prises en charge pour les instances de base de données Amazon RDS pour MySQL :

- 0 (« les noms stockés tels quels et les comparaisons sont sensibles à la casse ») est pris en charge pour toutes les versions de Amazon RDS pour MySQL.
- 1 (« les noms stockés en minuscules et les comparaisons ne sont pas sensibles à la casse ») est pris en charge pour Amazon RDS pour les version 5.5, 5.6, 5.7 et 8.0.19 et 8.0 ultérieures de MySQL.

Le paramètre `lower_case_table_names` doit être défini dans le cadre d'un groupe de paramètres DB personnalisé avant de créer une instance de base de données. Vous devez éviter de changer le paramètre `lower_case_table_names` pour les instances de base de données existantes, car cela pourrait entraîner des incohérences avec les sauvegardes de restauration à un instant dans le passé et les instances de base de données de réplica en lecture.

Les réplicas en lecture doivent toujours utiliser la même valeur de paramètre `lower_case_table_names` que l'instance de base de données source.

long_query_time

Vous pouvez définir le paramètre `long_query_time` sur une valeur à virgule flottante qui vous permet de consigner des requêtes lentes dans le journal des requêtes lentes MySQL avec une résolution en microseconde. Vous pouvez définir une valeur telle que 0,1 seconde, ce qui correspondrait à 100 millisecondes, pour aider lors du débogage de transactions lentes qui durent moins d'une seconde.

Limites de taille des fichiers MySQL dans Amazon RDS

Pour les instances de base de données Amazon RDS MySQL, la limite maximale de stockage alloué restreint la taille d'une table à un maximum de 16 To lors de l'utilisation des espaces de table file-per-table InnoDB. Cette limite restreint également l'espace de table du système à une taille maximum de 16 To. Les espaces de table file-per-table InnoDB (avec des tables chacun dans leur propre espace de table) sont définis par défaut pour les instances de base de données Amazon RDS MySQL.

> **Note**
>
> Certaines instances de bases de données existantes ont une limite inférieure. Par exemple, les instances de base de données MySQL créées avant avril 2014 ont une limite de taille de fichier et de table de 2 To. Cette limite de taille de fichier de 2 To s'applique également aux instances de bases de données ou aux réplicas en lecture créés à partir d'instantanés de bases de données pris avant avril 2014, quel que soit le moment de la création de l'instance de base de données.

Selon votre application, l'utilisation des espaces de table file-per-table InnoDB présente des avantages et des inconvénients. Pour déterminer l'approche optimale pour votre application, veuillez consulter File-Per-Table Tablespaces dans la documentation MySQL.

Il est déconseillé d'autoriser les tables à dépasser la taille maximale de fichier. En général, une meilleure pratique consiste à partitionner les données en tables plus petites, ce qui peut améliorer la performance et les temps de récupération.

Une option que vous pouvez utiliser pour diviser une grande table en plus petites consiste à partitionner. Le partitionnement répartit des portions de votre grande table en fichiers distincts basés sur des règles que vous spécifiez. Par exemple, si vous stockez des transactions par date, vous pouvez créer des règles de partitionnement qui répartissent des transactions plus anciennes en fichiers distincts en utilisant le partitionnement. Ensuite, vous pouvez archiver régulièrement les données de transaction historiques qui n'ont pas besoin d'être rapidement utilisables par votre application. Pour de plus amples informations, veuillez consulter Partitionnement dans la documentation MySQL.

Pour déterminer la taille de fichier d'une table

- Utilisez la commande SQL suivante pour déterminer si certaines de vos tables sont trop volumineuses et peuvent faire l'objet d'un partitionnement.

```
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');
```

Pour activer les espaces de table file-per-table InnoDB

- Pour activer les tablespaces file-per-table d'InnoDB, affectez au paramètre innodb_file_per_table la valeur `1` dans le groupe de paramètres relatif à l'instance de base de données.

Pour désactiver les espaces de table file-per-table InnoDB

- Pour désactiver les tablespaces file-per-table d'InnoDB, affectez au paramètre innodb_file_per_table la valeur `0` dans le groupe de paramètres relatif à l'instance de base de données.

Pour plus d'informations sur la mise à jour d'un groupe de paramètres, consultez Utilisation de groupes de paramètres de base de données (p. 225).

Après avoir activé ou désactivé les espaces de table file-per-table InnoDB, vous pouvez émettre une commande `ALTER TABLE` pour déplacer une table à partir de l'espace de table global vers son propre espace de table, ou à partir de son propre espace de table vers l'espace de table global, comme illustré dans l'exemple suivant :

```
ALTER TABLE table_name ENGINE=InnoDB;
```

Plug-in MySQL Keyring non pris en charge

Pour l'instant, Amazon RDS pour MySQL ne prend pas en charge le plug-in MySQL `keyring_aws` Amazon Web Services Keyring.

Référence SQL de MySQL sur Amazon RDS

Cette annexe décrit les procédures stockées système disponibles pour les instances Amazon RDS exécutant le moteur de base de données MySQL.

Présentation

Les procédures stockées système suivantes sont prises en charge pour les instances de base de données Amazon RDS exécutant MySQL.

Réplication

- mysql.rds_set_master_auto_position (p. 901)
- mysql.rds_set_external_master (p. 901)
- mysql.rds_set_external_master_with_delay (p. 904)
- mysql.rds_set_external_master_with_auto_position (p. 907)

- mysql.rds_reset_external_master (p. 909)
- mysql.rds_import_binlog_ssl_material (p. 910)
- mysql.rds_remove_binlog_ssl_material (p. 912)
- mysql.rds_set_source_delay (p. 912)
- mysql.rds_start_replication (p. 913)
- mysql.rds_start_replication_until (p. 914)
- mysql.rds_start_replication_until_gtid (p. 915)
- mysql.rds_stop_replication (p. 916)
- mysql.rds_skip_transaction_with_gtid (p. 916)
- mysql.rds_skip_repl_error (p. 917)
- mysql.rds_next_master_log (p. 918)

Préparation du cache InnoDB

- mysql.rds_innodb_buffer_pool_dump_now (p. 920)
- mysql.rds_innodb_buffer_pool_load_now (p. 920)
- mysql.rds_innodb_buffer_pool_load_abort (p. 920)

Gestion de configuration supplémentaire (rétention des fichiers journaux binaires, par exemple)

- mysql.rds_set_configuration (p. 921)
- mysql.rds_show_configuration (p. 922)

Mettre fin à une session ou à une requête

- mysql.rds_kill (p. 923)
- mysql.rds_kill_query (p. 924)

Journalisation

- mysql.rds_rotate_general_log (p. 924)
- mysql.rds_rotate_slow_log (p. 924)

Gestion de l'historique global des statuts

- mysql.rds_enable_gsh_collector (p. 925)
- mysql.rds_set_gsh_collector (p. 925)
- mysql.rds_disable_gsh_collector (p. 925)
- mysql.rds_collect_global_status_history (p. 926)
- mysql.rds_enable_gsh_rotation (p. 926)
- mysql.rds_set_gsh_rotation (p. 926)
- mysql.rds_disable_gsh_rotation (p. 926)
- mysql.rds_rotate_global_status_history (p. 926)

Conventions du guide de référence SQL

La section suivante explique les conventions utilisées pour décrire les tables et les procédures stockées système présentées dans la section de référence SQL.

Caractère	Description
MAJUSCULE	Les mots en lettres majuscules sont des mots clés.
[ ]	Les crochets indiquent des arguments facultatifs.
{ }	Les accolades indiquent que vous devez choisir l'un des arguments proposés.
|	Le caractère « pipe » sépare les arguments entre lesquels vous pouvez choisir.
italique	Les mots en italique correspondent à des espaces réservés. Vous devez insérer la valeur appropriée à la place du mot en italique.
…	Les trois points de suspension indiquent que vous pouvez répéter l'élément précédent.
'	Les mots entres apostrophes droits signifient que vous devez taper les apostrophes.

mysql.rds_set_master_auto_position

Définit le mode de réplication mode de manière à ce qu'il soit basé sur des positions de fichier journal binaire ou sur des identifiants de transaction globaux (GTID).

Syntaxe

```
CALL mysql.rds_set_master_auto_position (
auto_position_mode
);
```

Paramètres

auto_position_mode

Valeur qui indique si la réplication à utiliser est la réplication basée sur la position de fichier ou la réplication basée sur les identifiants de transaction globaux :

- `0` – Utiliser la méthode de réplication basée sur la position du fichier journal binaire. La valeur par défaut est `0`.
- `1` – Utiliser la méthode de réplication basée sur les identifiants de transaction globaux.

Notes d'utilisation

L'utilisateur principal doit exécuter la procédure `mysql.rds_set_master_auto_position`.

Pour Amazon RDS MySQL 5.7, cette procédure est prise en charge pour MySQL 5.7.23 et versions MySQL 5.7 ultérieures. Cette procédure n'est pas prise en charge pour Amazon RDS MySQL 5.5, 5.6 ou 8.0.

mysql.rds_set_external_master

Configure une instance de base de données MySQL comme réplica en lecture d'une instance de MySQL s'exécutant à l'extérieur d'Amazon RDS.

Important

Pour exécuter cette procédure, `autocommit` doit être activé. Pour l'activer, définissez le paramètre `autocommit` sur `1`. Pour de plus amples informations sur la modification des paramètres d'instance, veuillez consulter Modification de paramètres dans un groupe de paramètres de bases de données (p. 229).

Note

Vous pouvez utiliser la procédure stockée mysql.rds_set_external_master_with_delay (p. 904) pour configurer une instance de base de données source externe et une réplication différée.

Syntaxe

```
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
);
```

Paramètres

host_name

Nom d'hôte ou adresse IP de l'instance MySQL s'exécutant à l'extérieur d'Amazon RDS pour devenir l'instance de base de données source.

host_port

Port utilisé par l'instance MySQL s'exécutant à l'extérieur d'Amazon RDS et à configurer comme instance de base de données source. Si votre configuration réseau inclut une réplication de port Secure Shell (SSH) qui convertit le numéro de port, spécifiez le numéro de port qui est exposé par SSH.

replication_user_name

ID d'un utilisateur disposant des autorisations `REPLICATION CLIENT` et `REPLICATION SLAVE` sur l'instance MySQL s'exécutant à l'extérieur d'Amazon RDS. Nous vous recommandons de fournir un compte qui soit utilisé uniquement pour la réplication avec l'instance externe.

replication_user_password

Mot de passe de l'ID utilisateur spécifié dans `replication_user_name`.

mysql_binary_log_file_name

Nom du journal binaire sur l'instance de base de données source qui contient les informations de réplication.

mysql_binary_log_file_location

Emplacement dans le journal binaire `mysql_binary_log_file_name` à partir duquel la réplication commence à lire les informations de réplication.

ssl_encryption

Valeur indiquant si le chiffrement Secure Socket Layer (SSL) est utilisé sur la connexion de réplication. 1 spécifie d'utiliser le chiffrement SSL, 0 spécifie de ne pas utiliser le chiffrement. La valeur par défaut est 0.

> **Note**
>
> L'option `MASTER_SSL_VERIFY_SERVER_CERT` n'est pas prise en charge. Cette option est définie sur 0, ce qui signifie que la connexion est chiffrée, mais que les certificats ne sont pas vérifiés.

Notes d'utilisation

L'utilisateur principal doit exécuter la procédure `mysql.rds_set_external_master`. Cette procédure doit être exécutée sur l'instance de base de données MySQL qui doit être configurée comme réplica en lecture d'une instance MySQL s'exécutant en dehors d'Amazon RDS.

Avant d'exécuter `mysql.rds_set_external_master`, vous devez configurer l'instance de MySQL s'exécutant en dehors de Amazon RDS comme instance de base de données source. Pour vous connecter à l'instance MySQL en cours d'exécution en dehors de Amazon RDS, vous devez spécifier des valeurs `replication_user_name` et `replication_user_password` qui indiquent un utilisateur de réplication possédant des autorisations `REPLICATION CLIENT` et `REPLICATION SLAVE` sur l'instance externe de MySQL.

Pour configurer une instance externe de MySQL en tant qu'instance de base de données source

1. A l'aide du client MySQL de votre choix, connectez-vous à l'instance externe de MySQL et créez un compte d'utilisateur à utiliser pour la réplication. Voici un exemple de.

   ```
   CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'password'
   ```

2. Sur l'instance externe de MySQL, accordez les privilèges `REPLICATION CLIENT` et `REPLICATION SLAVE` à votre utilisateur de réplication. L'exemple suivant accorde les privilèges `REPLICATION CLIENT` et `REPLICATION SLAVE` sur toutes les bases de données pour l'utilisateur « repl_user » de votre domaine.

   ```
   GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'
   IDENTIFIED BY 'password'
   ```

Pour utiliser la réplication chiffrée, configurez l'instance de base de données source de façon à utiliser les connexions SSL. De plus, importez le certificat de l'autorité de certification, le certificat du client et la clé du client dans l'instance de base de données ou le cluster de bases de données à l'aide de la procédure mysql.rds_import_binlog_ssl_material (p. 910).

> **Note**
>
> Nous vous conseillons d'utiliser des réplicas en lecture pour gérer la réplication entre deux instances de base de données Amazon RDS dès que possible. Dans ce cas, nous vous conseillons d'utiliser seulement cette procédure et d'autres procédures stockées liées à la réplication. Ces pratiques permettent d'obtenir des topologies de réplication plus complexes entre des instances de base de données Amazon RDS. Nous proposons ces procédures stockées avant tout pour permettre la réplication avec les instances MySQL s'exécutant en dehors d'Amazon RDS. Pour plus d'informations sur la gestion de la réplication entre les instances de base de données Amazon RDS, consultez Utilisation des réplicas en lecture (p. 275).

Après avoir appelé `mysql.rds_set_external_master` pour configurer une instance de base de données Amazon RDS comme réplica en lecture, vous pouvez appeler mysql.rds_start_replication (p. 913) sur le réplica en lecture pour démarrer le processus de réplication. Vous pouvez appeler mysql.rds_reset_external_master (p. 909) pour supprimer la configuration du réplica en lecture.

Quand la procédure `mysql.rds_set_external_master` est appelée, Amazon RDS enregistre l'heure, l'utilisateur et une action de `set master` dans les tables `mysql.rds_history` et `mysql.rds_replication_status`.

Exemples

Lors d'une exécution sur une instance de base de données MySQL, l'exemple suivant configure l'instance de base de données comme réplica en lecture d'une instance de MySQL s'exécutant à l'extérieur d'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

Configure une instance de base de données MySQL Amazon RDS comme réplica en lecture d'une instance de MySQL s'exécutant à l'extérieur d'Amazon RDS et configure une réplication retardée.

> **Important**
>
> Pour exécuter cette procédure, `autocommit` doit être activé. Pour l'activer, définissez le paramètre `autocommit` sur `1`. Pour de plus amples informations sur la modification des paramètres d'instance, veuillez consulter Modification de paramètres dans un groupe de paramètres de bases de données (p. 229).

Syntaxe

```
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
);
```

Paramètres

host_name

Nom d'hôte ou adresse IP de l'instance MySQL s'exécutant à l'extérieur d'Amazon RDS et qui deviendra l'instance de base de données source.

host_port

Port utilisé par l'instance MySQL s'exécutant à l'extérieur d'Amazon RDS et à configurer comme instance de base de données source. Si votre configuration réseau inclut une réplication de port SSH qui convertit le numéro de port, spécifiez le numéro de port qui est exposé par SSH.

replication_user_name

ID d'un utilisateur disposant des autorisations `REPLICATION CLIENT` et `REPLICATION SLAVE` sur l'instance MySQL s'exécutant à l'extérieur d'Amazon RDS. Nous vous recommandons de fournir un compte qui soit utilisé uniquement pour la réplication avec l'instance externe.

replication_user_password

Mot de passe de l'ID utilisateur spécifié dans `replication_user_name`.

mysql_binary_log_file_name

Le nom du journal binaire sur l'instance de base de données source contient les informations de réplication.

mysql_binary_log_file_location

Emplacement dans le journal binaire `mysql_binary_log_file_name` à partir duquel la réplication commence à lire les informations de réplication.

ssl_encryption

Valeur indiquant si le chiffrement Secure Socket Layer (SSL) est utilisé sur la connexion de réplication. 1 spécifie d'utiliser le chiffrement SSL, 0 spécifie de ne pas utiliser le chiffrement. La valeur par défaut est 0.

Note

L'option `MASTER_SSL_VERIFY_SERVER_CERT` n'est pas prise en charge. Cette option est définie sur 0, ce qui signifie que la connexion est chiffrée, mais que les certificats ne sont pas vérifiés.

delay

Nombre minimum de secondes pour retarder la réplication à partir de l'instance de base de données source.

La limite de ce paramètre est une journée (soit 86 400 secondes).

Notes d'utilisation

L'utilisateur principal doit exécuter la procédure `mysql.rds_set_external_master_with_delay`. Cette procédure doit être exécutée sur l'instance de base de données MySQL qui doit être configurée comme réplica en lecture d'une instance MySQL s'exécutant en dehors d'Amazon RDS.

Avant d'exécuter `mysql.rds_set_external_master_with_delay`, vous devez configurer l'instance de MySQL s'exécutant en dehors de Amazon RDS comme instance de base de données source. Pour vous connecter à l'instance MySQL s'exécutant en dehors d'Amazon RDS, vous devez spécifier des valeurs pour `replication_user_name` et `replication_user_password`. Ces valeurs doivent indiquer un utilisateur de réplication disposant des autorisations `REPLICATION CLIENT` et `REPLICATION SLAVE` sur l'instance externe de MySQL.

Pour configurer une instance externe de MySQL en tant qu'instance de base de données source

1. A l'aide du client MySQL de votre choix, connectez-vous à l'instance externe de MySQL et créez un compte d'utilisateur à utiliser pour la réplication. Voici un exemple de.

```
CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'SomePassW0rd'
```

2. Sur l'instance externe de MySQL, accordez les privilèges `REPLICATION CLIENT` et `REPLICATION SLAVE` à votre utilisateur de réplication. L'exemple suivant accorde les privilèges `REPLICATION CLIENT` et `REPLICATION SLAVE` sur toutes les bases de données pour l'utilisateur `'repl_user'` de votre domaine.

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'
IDENTIFIED BY 'SomePassW0rd'
```

Pour plus d'informations, consultez Réplication avec une instance MySQL ou MariaDB s'exécutant à l'extérieur d'Amazon RDS (p. 863).

> **Note**
>
> Nous vous conseillons d'utiliser des réplicas en lecture pour gérer la réplication entre deux instances de base de données Amazon RDS dès que possible. Dans ce cas, nous vous conseillons d'utiliser seulement cette procédure et d'autres procédures stockées liées à la réplication. Ces pratiques permettent d'obtenir des topologies de réplication plus complexes entre des instances de base de données Amazon RDS. Nous proposons ces procédures stockées avant tout pour permettre la réplication avec les instances MySQL s'exécutant en dehors d'Amazon RDS. Pour plus d'informations sur la gestion de la réplication entre les instances de base de données Amazon RDS, consultez Utilisation des réplicas en lecture (p. 275).

Après avoir appelé `mysql.rds_set_external_master_with_delay` pour configurer une instance de base de données Amazon RDS comme réplica en lecture, vous pouvez appeler mysql.rds_start_replication (p. 913) sur le réplica en lecture pour démarrer le processus de réplication. Vous pouvez appeler mysql.rds_reset_external_master (p. 909) pour supprimer la configuration du réplica en lecture.

Lorsque vous appelez `mysql.rds_set_external_master_with_delay`, Amazon RDS enregistre l'heure, l'utilisateur et une action de `set master` dans les tables `mysql.rds_history` et `mysql.rds_replication_status`.

Pour la reprise après sinistre, vous pouvez utiliser cette procédure avec la procédure stockée mysql.rds_start_replication_until (p. 914) ou mysql.rds_start_replication_until_gtid (p. 915). Pour restaurer par progression les modifications dans un réplica en lecture retardé au moment précédant un sinistre, vous pouvez exécuter la procédure `mysql.rds_set_external_master_with_delay`. Une fois que la procédure `mysql.rds_start_replication_until` a arrêté la réplication, vous pouvez promouvoir le réplica en lecture pour qu'il devienne la nouvelle instance de base de données principale, en utilisant les instructions figurant dans Promotion d'un réplica en lecture en instance de bases de données autonome (p. 282).

Pour utiliser la procédure `mysql.rds_rds_start_replication_until_gtid`, la réplication basée sur des identifiants de transaction globaux (GTID) doit être activée. Pour ignorer une transaction basée sur des identifiants de transaction globaux spécifique qui est réputée pour entraîner des défaillances, vous pouvez utiliser la procédure stockée mysql.rds_skip_transaction_with_gtid (p. 916). Pour plus d'informations sur la gestion d'une réplication basée sur des identifiants de transaction globaux, consultez Utilisation de la réplication basée sur des identifiants de transaction globaux (GTID) pour Amazon RDS MySQL (p. 857).

La procédure stockée `mysql.rds_set_external_master_with_delay` est disponible dans les versions MySQL Amazon RDS suivantes :

- Version MySQL 5.6.40 et versions 5.6 ultérieures
- Version MySQL 5.7.22 et versions 5.7 ultérieures

Exemples

Lors d'une exécution sur une instance de base de données MySQL, l'exemple suivant configure l'instance de base de données comme réplica en lecture d'une instance de MySQL s'exécutant à l'extérieur d'Amazon RDS. Il définit le délai de réplication minimal à une heure (soit 3 600 secondes) sur l'instance de base de données MySQL. Une modification provenant de l'instance de base de données source MySQL exécutée à

l'extérieur d'Amazon RDS n'est pas appliquée dans le réplica en lecture de l'instance de base de données MySQL pendant au moins une heure.

```
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

Configure une instance de base de données Amazon RDS MySQL comme réplica en lecture d'une instance de MySQL s'exécutant à l'extérieur d'Amazon RDS. Cette procédure configure également la réplication retardée et la réplication basée sur des identifiants de transaction globaux.

> **Important**
>
> Pour exécuter cette procédure, `autocommit` doit être activé. Pour l'activer, définissez le paramètre `autocommit` sur `1`. Pour de plus amples informations sur la modification des paramètres d'instance, veuillez consulter Modification de paramètres dans un groupe de paramètres de bases de données (p. 229).

Syntaxe

```
CALL mysql.rds_set_external_master_with_auto_position (
  host_name
  , host_port
  , replication_user_name
  , replication_user_password
  , ssl_encryption
  , delay
);
```

Paramètres

host_name

Nom d'hôte ou adresse IP de l'instance MySQL s'exécutant à l'extérieur d'Amazon RDS pour devenir l'instance de base de données source.

host_port

Port utilisé par l'instance MySQL s'exécutant à l'extérieur d'Amazon RDS et à configurer comme instance de base de données source. Si votre configuration réseau inclut une réplication de port Secure Shell (SSH) qui convertit le numéro de port, spécifiez le numéro de port qui est exposé par SSH.

replication_user_name

ID d'un utilisateur disposant des autorisations `REPLICATION CLIENT` et `REPLICATION SLAVE` sur l'instance MySQL s'exécutant à l'extérieur d'Amazon RDS. Nous vous recommandons de fournir un compte qui soit utilisé uniquement pour la réplication avec l'instance externe.

replication_user_password

Mot de passe de l'ID utilisateur spécifié dans `replication_user_name`.

ssl_encryption

Valeur indiquant si le chiffrement Secure Socket Layer (SSL) est utilisé sur la connexion de réplication. 1 spécifie d'utiliser le chiffrement SSL, 0 spécifie de ne pas utiliser le chiffrement. La valeur par défaut est 0.

Note

L'option `MASTER_SSL_VERIFY_SERVER_CERT` n'est pas prise en charge. Cette option est définie sur 0, ce qui signifie que la connexion est chiffrée, mais que les certificats ne sont pas vérifiés.

delay

Nombre minimum de secondes pour retarder la réplication à partir de l'instance de base de données source.

La limite de ce paramètre est une journée (soit 86 400 secondes).

Notes d'utilisation

L'utilisateur principal doit exécuter la procédure `mysql.rds_set_external_master_with_auto_position`. Cette procédure doit être exécutée sur l'instance de base de données MySQL qui doit être configurée comme réplica en lecture d'une instance MySQL s'exécutant en dehors d'Amazon RDS.

Pour Amazon RDS MySQL 5.7, cette procédure est prise en charge pour MySQL 5.7.23 et versions MySQL 5.7 ultérieures. Cette procédure n'est pas prise en charge pour Amazon RDS MySQL 5.5, 5.6 ou 8.0.

Avant d'exécuter `mysql.rds_set_external_master_with_auto_position`, vous devez configurer l'instance de MySQL s'exécutant en dehors de Amazon RDS comme instance de base de données source. Pour vous connecter à l'instance MySQL s'exécutant en dehors d'Amazon RDS, vous devez spécifier des valeurs pour `replication_user_name` et `replication_user_password`. Ces valeurs doivent indiquer un utilisateur de réplication disposant des autorisations `REPLICATION CLIENT` et `REPLICATION SLAVE` sur l'instance externe de MySQL.

Pour configurer une instance externe de MySQL en tant qu'instance de base de données source

1. A l'aide du client MySQL de votre choix, connectez-vous à l'instance externe de MySQL et créez un compte d'utilisateur à utiliser pour la réplication. Voici un exemple de.

```
CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'SomePassW0rd'
```

2. Sur l'instance externe de MySQL, accordez les privilèges `REPLICATION CLIENT` et `REPLICATION SLAVE` à votre utilisateur de réplication. L'exemple suivant accorde les privilèges `REPLICATION CLIENT` et `REPLICATION SLAVE` sur toutes les bases de données pour l'utilisateur `'repl_user'` de votre domaine.

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'
IDENTIFIED BY 'SomePassW0rd'
```

Pour plus d'informations, consultez Réplication avec une instance MySQL ou MariaDB s'exécutant à l'extérieur d'Amazon RDS (p. 863).

Note

Nous vous conseillons d'utiliser des réplicas en lecture pour gérer la réplication entre deux instances de base de données Amazon RDS dès que possible. Dans ce cas, nous vous

conseillons d'utiliser seulement cette procédure et d'autres procédures stockées liées à la réplication. Ces pratiques permettent d'obtenir des topologies de réplication plus complexes entre des instances de base de données Amazon RDS. Nous proposons ces procédures stockées avant tout pour permettre la réplication avec les instances MySQL s'exécutant en dehors d'Amazon RDS. Pour plus d'informations sur la gestion de la réplication entre les instances de base de données Amazon RDS, consultez Utilisation des réplicas en lecture (p. 275).

Après avoir appelé `mysql.rds_set_external_master_with_auto_position` pour configurer une instance de base de données Amazon RDS comme réplica en lecture, vous pouvez appeler mysql.rds_start_replication (p. 913) sur le réplica en lecture pour démarrer le processus de réplication. Vous pouvez appeler mysql.rds_reset_external_master (p. 909) pour supprimer la configuration du réplica en lecture.

Lorsque vous appelez `mysql.rds_set_external_master_with_auto_position`, Amazon RDS enregistre l'heure, l'utilisateur et une action de `set master` dans les tables `mysql.rds_history` et `mysql.rds_replication_status`.

Pour la reprise après sinistre, vous pouvez utiliser cette procédure avec la procédure stockée mysql.rds_start_replication_until (p. 914) ou mysql.rds_start_replication_until_gtid (p. 915). Pour restaurer par progression les modifications dans un réplica en lecture retardé au moment précédant un sinistre, vous pouvez exécuter la procédure `mysql.rds_set_external_master_with_auto_position`. Une fois que la procédure `mysql.rds_start_replication_until_gtid` a arrêté la réplication, vous pouvez promouvoir le réplica en lecture pour qu'il devienne la nouvelle instance de base de données principale, en utilisant les instructions figurant dans Promotion d'un réplica en lecture en instance de bases de données autonome (p. 282).

Pour utiliser la procédure `mysql.rds_rds_start_replication_until_gtid`, la réplication basée sur des identifiants de transaction globaux (GTID) doit être activée. Pour ignorer une transaction basée sur des identifiants de transaction globaux spécifique qui est réputée pour entraîner des défaillances, vous pouvez utiliser la procédure stockée mysql.rds_skip_transaction_with_gtid (p. 916). Pour plus d'informations sur la gestion d'une réplication basée sur des identifiants de transaction globaux, consultez Utilisation de la réplication basée sur des identifiants de transaction globaux (GTID) pour Amazon RDS MySQL (p. 857).

Exemples

Lors d'une exécution sur une instance de base de données MySQL, l'exemple suivant configure l'instance de base de données comme réplica en lecture d'une instance de MySQL s'exécutant à l'extérieur d'Amazon RDS. Il définit le délai de réplication minimal à une heure (soit 3 600 secondes) sur l'instance de base de données MySQL. Une modification provenant de l'instance de base de données source MySQL exécutée à l'extérieur d'Amazon RDS n'est pas appliquée dans le réplica en lecture de l'instance de base de données MySQL pendant au moins une heure.

```
call mysql.rds_set_external_master_with_auto_position(
  'Externaldb.some.com',
  3306,
  'repl_user',
  'SomePassW0rd',
  0,
  3600);
```

mysql.rds_reset_external_master

Reconfigure une instance de base de données MySQL comme n'étant plus un réplica en lecture d'une instance de MySQL s'exécutant à l'extérieur d'Amazon RDS.

Important

Pour exécuter cette procédure, `autocommit` doit être activé. Pour l'activer, définissez le paramètre `autocommit` sur `1`. Pour de plus amples informations sur la modification des paramètres d'instance, veuillez consulter Modification de paramètres dans un groupe de paramètres de bases de données (p. 229).

Syntaxe

```
CALL mysql.rds_reset_external_master;
```

Notes d'utilisation

L'utilisateur principal doit exécuter la procédure `mysql.rds_reset_external_master`. Cette procédure doit être exécutée sur l'instance de base de données MySQL à supprimer comme réplica en lecture d'une instance MySQL s'exécutant en dehors d'Amazon RDS.

Note

Nous vous conseillons d'utiliser des réplicas en lecture pour gérer la réplication entre deux instances de base de données Amazon RDS dès que possible. Dans ce cas, nous vous conseillons d'utiliser seulement cette procédure et d'autres procédures stockées liées à la réplication. Ces pratiques permettent d'obtenir des topologies de réplication plus complexes entre des instances de base de données Amazon RDS. Nous proposons ces procédures stockées avant tout pour permettre la réplication avec les instances MySQL s'exécutant en dehors d'Amazon RDS. Pour plus d'informations sur la gestion de la réplication entre les instances de base de données Amazon RDS, consultez Utilisation des réplicas en lecture (p. 275).

Pour plus d'informations sur l'utilisation de la réplication pour importer des données à partir d'une instance de MySQL s'exécutant à l'extérieur de Amazon RDS, consultez Restauration d'une sauvegarde dans une instance de base de données MySQL Amazon RDS (p. 821).

mysql.rds_import_binlog_ssl_material

Importe le certificat de l'autorité de certification, le certificat du client et la clé du client dans le cluster de bases de données Aurora MySQL. Les informations sont requises pour la communication SSL et la réplication chiffrée.

Note

Actuellement, cette procédure est uniquement prise en charge pour Aurora MySQL version 5.6.

Syntaxe

```
CALL mysql.rds_import_binlog_ssl_material (
  ssl_material
);
```

Paramètres

ssl_material

Charge utile JSON contenant le contenu des fichiers au format .pem suivants pour un client MySQL :

- "ssl_ca":"*Certificat de l'autorité de certification*"
- "ssl_cert":"*Certificat du client*"
- "ssl_key":"*Clé du client*"

Notes d'utilisation

Avant d'exécuter cette procédure, préparez-vous à la réplication chiffrée :

- Si le protocole SSL n'est pas activé sur l'instance de base de données source MySQL externe et que vous ne disposez pas d'une clé client et d'un certificat client prêts, activez le protocole SSL sur le serveur de base de données MySQL et générez la clé client et le certificat client requis.
- Si le protocole SSL est activé sur l'instance de base de données source externe, fournissez une clé et un certificat client pour le cluster de bases de données Aurora MySQL. En leur absence, générez une nouvelle clé et un nouveau certificat pour le cluster de bases de données Aurora MySQL. Pour signer le certificat client, vous devez disposer de la clé d'autorité de certification utilisée pour configurer le protocole SSL sur l'instance de base de données source MySQL externe.

Pour de plus amples informations, veuillez consulter Création de certificats et clés SSL à l'aide d'openssl dans la documentation MySQL.

> **Important**
>
> Après vous être préparé à la réplication chiffrée, utilisez une connexion SSL pour exécuter cette procédure. La clé du client ne doit pas être transférée au moyen d'une connexion non sécurisée.

Cette procédure permet d'importer des informations SSL entre une base de données MySQL externe et un cluster de bases de données Aurora MySQL. Les informations SSL se trouvent dans des fichiers au format .pem contenant les informations SSL du cluster de bases de données Aurora MySQL. Pendant la réplication chiffrée, le cluster de bases de données Aurora MySQL agit comme client du serveur de base de données MySQL. Les certificats et les clés privées du client Aurora MySQL sont au format .pem dans les fichiers.

Vous pouvez copier les informations de ces fichiers dans le paramètre `ssl_material` de la charge utile JSON correspondante. Pour prendre en charge la réplication chiffrée, importez les informations SSL dans le cluster de bases de données Aurora MySQL.

La charge utile JSON doit être au format suivant.

```
'{"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"}'
```

Exemples

L'exemple suivant importe des informations SSL dans un cluster de bases de données Aurora MySQL. Dans les fichiers au format .pem, le code du corps est généralement plus long que le code du corps affiché dans l'exemple.

```
call mysql.rds_import_binlog_ssl_material(
'{"ssl_ca":"-----BEGIN CERTIFICATE-----
AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
-----END CERTIFICATE-----\n","ssl_cert":"-----BEGIN CERTIFICATE-----
```

```
AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
-----END CERTIFICATE-----\n","ssl_key":"-----BEGIN RSA PRIVATE KEY-----
AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
-----END RSA PRIVATE KEY-----\n"}');
```

Note

Pour plus d'informations sur l'utilisation d'Amazon Aurora, consultez le Guide de l'utilisateur Amazon Aurora.

mysql.rds_remove_binlog_ssl_material

Supprime le certificat de l'autorité de certification, le certificat du client et la clé du client pour la communication SSL et la réplication chiffrée. Ces informations sont importées à l'aide de mysql.rds_import_binlog_ssl_material (p. 910).

Note

Actuellement, cette procédure est uniquement prise en charge pour Aurora MySQL version 5.6.

Syntaxe

```
CALL mysql.rds_remove_binlog_ssl_material;
```

mysql.rds_set_source_delay

Définit le nombre minimum de secondes pour retarder la réplication de l'instance de base de données source vers le réplica en lecture actuel. Utilisez cette procédure lorsque vous êtes connecté à un réplica en lecture afin de retarder la réplication à partir de l'instance de base de données source.

Syntaxe

```
CALL mysql.rds_set_source_delay(
delay
);
```

Paramètres

delay

Nombre minimum de secondes pour retarder la réplication à partir de l'instance de base de données source.

La limite de ce paramètre est une journée (soit 86 400 secondes).

Notes d'utilisation

L'utilisateur principal doit exécuter la procédure `mysql.rds_set_source_delay`.

Pour la reprise après sinistre, vous pouvez utiliser cette procédure avec la procédure stockée mysql.rds_start_replication_until (p. 914) ou mysql.rds_start_replication_until_gtid (p. 915). Pour restaurer par progression les modifications dans un réplica en lecture retardé au moment précédant un sinistre, vous pouvez exécuter la procédure `mysql.rds_set_source_delay`. Une fois que la procédure `mysql.rds_start_replication_until` ou `mysql.rds_start_replication_until_gtid` a arrêté la réplication, vous pouvez promouvoir le réplica en lecture pour qu'il devienne la nouvelle instance de base de données principale, en utilisant les instructions figurant dans Promotion d'un réplica en lecture en instance de bases de données autonome (p. 282).

Pour utiliser la procédure `mysql.rds_rds_start_replication_until_gtid`, la réplication basée sur des identifiants de transaction globaux (GTID) doit être activée. Pour ignorer une transaction basée sur des identifiants de transaction globaux spécifique qui est réputée pour entraîner des défaillances, vous pouvez utiliser la procédure stockée mysql.rds_skip_transaction_with_gtid (p. 916). Pour plus d'informations sur la réplication basée sur des identifiants de transaction globaux, consultez Utilisation de la réplication basée sur des identifiants de transaction globaux (GTID) pour Amazon RDS MySQL (p. 857).

La procédure stockée `mysql.rds_set_source_delay` est disponible dans les versions MySQL Amazon RDS suivantes :

- Version MySQL 5.6.40 et versions 5.6 ultérieures
- Version MySQL 5.7.22 et versions 5.7 ultérieures

Exemples

Pour retarder la réplication à partir de l'instance de base de données source vers le réplica en lecture actuel pendant au moins un heure (3 600 secondes), vous pouvez appeler `mysql.rds_set_source_delay` avec le paramètre suivant :

```
CALL mysql.rds_set_source_delay(3600);
```

mysql.rds_start_replication

Démarre la réplication à partir d'une instance de base de données MySQL.

> **Note**
>
> Vous pouvez utiliser la procédure stockée mysql.rds_start_replication_until (p. 914) ou mysql.rds_start_replication_until_gtid (p. 915) pour lancer la réplication à partir d'une instance de base de données Amazon RDS MySQL et arrêter la réplication à la position spécifiée dans le fichier journal binaire.

Syntaxe

```
CALL mysql.rds_start_replication;
```

Notes d'utilisation

L'utilisateur principal doit exécuter la procédure `mysql.rds_start_replication`.

Si vous configurez la réplication pour importer des données à partir d'une instance de MySQL s'exécutant à l'extérieur d'Amazon RDS, vous appelez `mysql.rds_start_replication` sur le réplica en lecture pour démarrer le processus de réplication après avoir appelé mysql.rds_set_external_master (p. 901) pour créer la configuration de réplication. Pour plus d'informations, consultez Restauration d'une sauvegarde dans une instance de base de données MySQL Amazon RDS (p. 821).

Si vous configurez la réplication pour exporter les données vers une instance de MySQL extérieure à Amazon RDS, vous appelez `mysql.rds_start_replication` et `mysql.rds_stop_replication` sur le réplica en lecture pour contrôler certaines actions de réplication, telles que la purge des journaux binaires. Pour plus d'informations, consultez Exportation de données à partir d'une instance DB MySQL grâce à la réplication (p. 869).

Vous pouvez aussi appeler `mysql.rds_start_replication` sur le réplica en lecture pour redémarrer un processus de réplication que vous avez précédemment arrêté en appelant mysql.rds_stop_replication (p. 916). Pour plus d'informations, consultez Utilisation des réplicas en lecture (p. 275).

mysql.rds_start_replication_until

Lance la réplication à partir d'une instance de base de données MySQL Amazon RDS et arrête la réplication à la position spécifiée dans le fichier journal binaire.

Syntaxe

```
CALL mysql.rds_start_replication_until (
replication_log_file
  , replication_stop_point
);
```

Paramètres

replication_log_file

Le nom du journal binaire sur l'instance de base de données source contient les informations de réplication.

replication_stop_point

Position dans le journal binaire `replication_log_file` à laquelle la réplication s'arrêtera.

Notes d'utilisation

L'utilisateur principal doit exécuter la procédure `mysql.rds_start_replication_until`.

Vous pouvez utiliser cette procédure avec la réplication retardée pour la reprise après sinistre. Si vous avez configuré la réplication retardée, vous pouvez utiliser cette procédure pour restaurer par progression les modifications dans un réplica en lecture retardé au moment précédant un sinistre. Une fois que cette procédure a arrêté la réplication, vous pouvez promouvoir le réplica en lecture pour qu'il devienne la nouvelle instance de base de données principale, en utilisant les instructions figurant dans Promotion d'un réplica en lecture en instance de bases de données autonome (p. 282).

Vous pouvez configurer la réplication retardée en utilisant les procédures stockées suivantes :

- mysql.rds_set_configuration (p. 921)
- mysql.rds_set_external_master_with_delay (p. 904)
- mysql.rds_set_source_delay (p. 912)

Le nom de fichier spécifié pour le paramètre `replication_log_file` doit correspondre au nom du fichier binlog de l'instance de base de données source.

Lorsque le paramètre `replication_stop_point` spécifie une position d'arrêt survenant dans le passé, la réplication est arrêtée immédiatement.

La procédure stockée `mysql.rds_start_replication_until` est disponible dans les versions MySQL Amazon RDS suivantes :

- Version MySQL 5.6.40 et versions 5.6 ultérieures
- Version MySQL 5.7.22 et versions 5.7 ultérieures

Exemples

L'exemple suivant lance la réplication et réplique les modifications jusqu'à ce qu'il atteigne la position `120` dans le fichier journal binaire `mysql-bin-changelog.000777`.

```
call mysql.rds_start_replication_until(
  'mysql-bin-changelog.000777',
  120);
```

mysql.rds_start_replication_until_gtid

Lance la réplication à partir d'une instance de base de données Amazon RDS MySQL et arrête la réplication immédiatement après l'identifiant de transaction global spécifié.

Syntaxe

```
CALL mysql.rds_start_replication_until_gtid (
gtid
);
```

Paramètres

gtid

Identifiant de transaction global (GTID) après lequel la réplication s'arrête.

Notes d'utilisation

L'utilisateur principal doit exécuter la procédure `mysql.rds_start_replication_until_gtid`.

Pour Amazon RDS MySQL 5.7, cette procédure est prise en charge pour MySQL 5.7.23 et versions MySQL 5.7 ultérieures. Cette procédure n'est pas prise en charge pour Amazon RDS MySQL 5.5, 5.6 ou 8.0.

Vous pouvez utiliser cette procédure avec la réplication retardée pour la reprise après sinistre. Si vous avez configuré la réplication retardée, vous pouvez utiliser cette procédure pour restaurer par progression les modifications dans un réplica en lecture retardé au moment précédant un sinistre. Une fois que cette procédure a arrêté la réplication, vous pouvez promouvoir le réplica en lecture pour qu'il devienne la nouvelle instance de base de données principale, en utilisant les instructions figurant dans Promotion d'un réplica en lecture en instance de bases de données autonome (p. 282).

Vous pouvez configurer la réplication retardée en utilisant les procédures stockées suivantes :

- mysql.rds_set_configuration (p. 921)
- mysql.rds_set_external_master_with_auto_position (p. 907)
- mysql.rds_set_source_delay (p. 912)

Lorsque le paramètre `gtid` spécifie une transaction ayant déjà été exécutée par le réplica, la réplication est immédiatement arrêtée.

Exemples

L'exemple suivant lance la réplication et réplique les modifications jusqu'à ce que le GTID soit atteint `3E11FA47-71CA-11E1-9E33-C80AA9429562:23`.

```
call mysql.rds_start_replication_until_gtid('3E11FA47-71CA-11E1-9E33-C80AA9429562:23');
```

mysql.rds_stop_replication

Arrête la réplication à partir d'une instance de base de données MySQL.

Syntaxe

```
CALL mysql.rds_stop_replication;
```

Notes d'utilisation

L'utilisateur principal doit exécuter la procédure `mysql.rds_stop_replication`.

Si vous configurez la réplication pour importer des données à partir d'une instance de MySQL s'exécutant à l'extérieur d'Amazon RDS, vous appelez `mysql.rds_stop_replication` sur le réplica en lecture pour arrêter le processus de réplication après que l'importation soit terminée. Pour plus d'informations, consultez Restauration d'une sauvegarde dans une instance de base de données MySQL Amazon RDS (p. 821).

Si vous configurez la réplication pour exporter les données vers une instance de MySQL extérieure à Amazon RDS, vous appelez `mysql.rds_start_replication` et `mysql.rds_stop_replication` sur le réplica en lecture pour contrôler certaines actions de réplication, telles que la purge des journaux binaires. Pour plus d'informations, consultez Exportation de données à partir d'une instance DB MySQL grâce à la réplication (p. 869).

Vous pouvez aussi utiliser `mysql.rds_stop_replication` pour arrêter la réplication entre deux instances de base de données Amazon RDS. Vous arrêtez généralement la réplication pour exécuter une longue opération sur le réplica en lecture, comme la création d'un index volumineux sur le réplica en lecture. Vous pouvez redémarrer tout processus de réplication que vous avez arrêté en appelant mysql.rds_start_replication (p. 913) sur le réplica en lecture. Pour plus d'informations, consultez Utilisation des réplicas en lecture (p. 275).

mysql.rds_skip_transaction_with_gtid

Ignore la réplication d'une transaction avec l'identifiant de transaction global (GTID) spécifié sur une instance de base de données MySQL.

Vous pouvez utiliser cette procédure pour la reprise après sinistre lorsqu'il est avéré qu'une transaction GTID entraîne des problèmes. Utilisez cette procédure stockée pour ignorer la transaction problématique. Les transactions problématiques sont par exemple celles qui désactivent la réplication, suppriment des données importantes ou entraînent l'indisponibilité de l'instance de base de données.

Syntaxe

```
CALL mysql.rds_skip_transaction_with_gtid (
```

```
gtid_to_skip
);
```

Paramètres

gtid_to_skip

GTID de la transaction de réplication à ignorer.

Notes d'utilisation

L'utilisateur principal doit exécuter la procédure `mysql.rds_skip_transaction_with_gtid`.

Pour Amazon RDS MySQL 5.7, cette procédure est prise en charge pour MySQL 5.7.23 et versions MySQL 5.7 ultérieures. Cette procédure n'est pas prise en charge pour Amazon RDS MySQL 5.5, 5.6 ou 8.0.

Exemples

L'exemple suivant ignore la réplication de la transaction avec le 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

Ignore et supprime une erreur de réplication sur une instance de base de données MySQL.

Syntaxe

```
CALL mysql.rds_skip_repl_error;
```

Notes d'utilisation

L'utilisateur principal doit exécuter la procédure `mysql.rds_skip_repl_error`.

Pour déterminer s'il y a des erreurs, exécutez la commande MySQL `show slave status\G`. Si une erreur de réplication n'est pas critique, vous pouvez exécuter `mysql.rds_skip_repl_error` pour ignorer l'erreur. S'il y a plusieurs erreurs, `mysql.rds_skip_repl_error` supprime la première erreur, puis avertit qu'il y a d'autres erreurs. Vous pouvez alors utiliser `show slave status\G` pour déterminer l'action appropriée pour l'erreur suivante. Pour de plus amples informations sur les valeurs renvoyées, veuillez consulter la documentation MySQL.

Pour plus d'informations sur le traitement des erreurs de réplication avec Amazon RDS, consultez Résolution d'un problème de réplica en lecture MySQL (p. 856).

> **Important**
>
> Si vous essayez d'appeler `mysql.rds_skip_repl_error`, il se peut que vous receviez l'erreur suivante : `ERROR 1305 (42000): PROCEDURE mysql.rds_skip_repl_error does not exist`. Dans ce cas, mettez à niveau votre instance de base de données MySQL sur la dernière version mineure ou sur l'une des versions mineures minimales répertoriées dans cette rubrique.

Erreur d'arrêt de réplication

Lorsque vous appelez la commande `mysql.rds_skip_repl_error`, vous pouvez recevoir le message d'erreur suivant : `Slave is down or disabled.`

Ce message d'erreur s'affiche parce que la réplication a été arrêtée et ne peut pas être redémarrée.

Si vous avez besoin d'ignorer un grand nombre d'erreurs, le retard de réplication peut augmenter et dépasser la période de rétention par défaut pour les fichiers journaux binaires (binlog). Dans ce cas, vous pouvez rencontrer une erreur irrécupérable due à des fichiers journaux binaires purgés avant d'avoir été réutilisés sur le réplica en lecture. Cette purge entraîne l'arrêt de la réplication et vous ne pouvez plus appeler la commande `mysql.rds_skip_repl_error` pour ignorer les erreurs de réplication.

Vous pouvez atténuer ce problème en augmentant le nombre d'heures pendant lequel les fichiers journaux binaires sont conservés sur votre instance de base de données source. Une fois que vous avez augmenté le temps de rétention de journaux binaires, vous pouvez redémarrer la réplication et appeler la commande `mysql.rds_skip_repl_error` en fonction des besoins.

Pour définir la période de rétention des journaux binaires, utilisez la procédure mysql.rds_set_configuration (p. 921) et spécifiez un paramètre de configuration `'binlog retention hours'`, ainsi que le nombre d'heures pendant lequel conserver les fichiers journaux binaires sur le cluster de bases de données. L'exemple suivant définit la période de rétention des fichiers journaux binaires à 48 heures.

```
CALL mysql.rds_set_configuration('binlog retention hours', 48);
```

mysql.rds_next_master_log

Modifie la position du journal de l'instance de base de données source au début du journal binaire suivant sur l'instance de base de données source. N'utilisez cette procédure que si vous recevez une erreur 1236 d'I/O de réplication sur un réplica en lecture.

Syntaxe

```
CALL mysql.rds_next_master_log(
curr_master_log
);
```

Paramètres

curr_master_log

Index du fichier journal maître actif. Par exemple, si le fichier en cours se nomme `mysql-bin-changelog.012345`, l'index est 12345. Pour déterminer le nom du fichier journal maître actif, exécutez la commande `SHOW SLAVE STATUS` et affichez le champ `Master_Log_File`.

Notes d'utilisation

L'utilisateur principal doit exécuter la procédure `mysql.rds_next_master_log`.

Warning

Appelez `mysql.rds_next_master_log` uniquement si la réplication échoue après le basculement d'une instance de base de données multi-AZ qui est la source de la réplication, et que le champ `Last_IO_Errno` de `SHOW SLAVE STATUS` signale une erreur d'I/O 1236.

L'appel de `mysql.rds_next_master_log` peut se traduire par une perte des données dans le réplica en lecture si les transactions de l'instance source n'ont pas été écrites dans le journal binaire sur disque avant que le basculement n'intervienne. Vous pouvez réduire la probabilité que cela se produise en configurant les paramètres de l'instance source sync_binlog = 1 et innodb_support_xa = 1, même si les performances peuvent s'en trouver réduites. Pour plus d'informations, consultez Utilisation des réplicas en lecture (p. 275).

Exemples

Supposons que la réplication ait échoué sur un réplica en lecture Amazon RDS. L'exécution de `SHOW SLAVE STATUS\G` sur le réplica en lecture retourne le résultat suivant :

```
*************************** 1. row ***************************
               Slave_IO_State:
                  Master_Host: myhost.XXXXXXXXXXXXXXX.rr-rrrr-1.rds.amazonaws.com
                  Master_User: MasterUser
                  Master_Port: 3306
                Connect_Retry: 10
              Master_Log_File: mysql-bin-changelog.012345
          Read_Master_Log_Pos: 1219393
               Relay_Log_File: relaylog.012340
                Relay_Log_Pos: 30223388
        Relay_Master_Log_File: mysql-bin-changelog.012345
             Slave_IO_Running: No
            Slave_SQL_Running: Yes
              Replicate_Do_DB:
          Replicate_Ignore_DB:
           Replicate_Do_Table:
       Replicate_Ignore_Table:
      Replicate_Wild_Do_Table:
  Replicate_Wild_Ignore_Table:
                   Last_Errno: 0
                   Last_Error:
                 Skip_Counter: 0
          Exec_Master_Log_Pos: 30223232
              Relay_Log_Space: 5248928866
              Until_Condition: None
               Until_Log_File:
                Until_Log_Pos: 0
           Master_SSL_Allowed: No
           Master_SSL_CA_File:
           Master_SSL_CA_Path:
              Master_SSL_Cert:
            Master_SSL_Cipher:
               Master_SSL_Key:
        Seconds_Behind_Master: NULL
Master_SSL_Verify_Server_Cert: No
                Last_IO_Errno: 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_Errno: 0
               Last_SQL_Error:
  Replicate_Ignore_Server_Ids:
             Master_Server_Id: 67285976
```

Le champ `Last_IO_Errno` montre que l'instance reçoit une erreur 1236 d'I/O. Le champ `Master_Log_File` montre que le nom du fichier est `mysql-bin-changelog.012345`, ce qui signifie que l'index du fichier journal est `12345`. Pour résoudre l'erreur, vous pouvez appeler `mysql.rds_next_master_log` avec le paramètre suivant :

```
CALL mysql.rds_next_master_log(12345);
```

mysql.rds_innodb_buffer_pool_dump_now

Vide l'état actuel du pool de tampons sur le disque. Pour plus d'informations, consultez Préparation du cache InnoDB (p. 790).

Syntaxe

```
CALL mysql.rds_innodb_buffer_pool_dump_now();
```

Notes d'utilisation

L'utilisateur principal doit exécuter la procédure `mysql.rds_innodb_buffer_pool_dump_now`.

La procédure stockée `mysql.rds_innodb_buffer_pool_dump_now` est disponible dans les versions MySQL Amazon RDS suivantes :

- MySQL 5.6
- MySQL 5.7
- MySQL 8.0

mysql.rds_innodb_buffer_pool_load_now

Charge l'état enregistré du pool de tampons à partir du disque. Pour plus d'informations, consultez Préparation du cache InnoDB (p. 790).

Syntaxe

```
CALL mysql.rds_innodb_buffer_pool_load_now();
```

Notes d'utilisation

L'utilisateur principal doit exécuter la procédure `mysql.rds_innodb_buffer_pool_load_now`.

La procédure stockée `mysql.rds_innodb_buffer_pool_load_now` est disponible dans les versions MySQL Amazon RDS suivantes :

- MySQL 5.6
- MySQL 5.7
- MySQL 8.0

mysql.rds_innodb_buffer_pool_load_abort

Annule un chargement en cours de l'état du groupe de tampons enregistré. Pour plus d'informations, consultez Préparation du cache InnoDB (p. 790).

Syntaxe

```
CALL mysql.rds_innodb_buffer_pool_load_abort();
```

Notes d'utilisation

L'utilisateur principal doit exécuter la procédure `mysql.rds_innodb_buffer_pool_load_abort`.

La procédure stockée `mysql.rds_innodb_buffer_pool_load_abort` est disponible dans les versions MySQL Amazon RDS suivantes :

- MySQL 5.6
- MySQL 5.7
- MySQL 8.0

mysql.rds_set_configuration

Spécifie le nombre d'heures pendant lequel les journaux binaires doivent être conservés ou le nombre de secondes pendant lequel retarder la réplication.

Syntaxe

```
CALL mysql.rds_set_configuration(name,value);
```

Paramètres

nom

Nom du paramètre de configuration à définir.

valeur

Valeur du paramètre de configuration.

Notes d'utilisation

La procédure stockée `mysql.rds_set_configuration` est disponible dans les versions de Amazon RDS MySQL suivantes :

- MySQL 5.6
- MySQL 5.7
- MySQL 8.0

La procédure `mysql.rds_set_configuration` prend en charge des paramètres de configuration suivants :

- Nombre d'heures de conservation du journal binaire (p. 921)
- Délai cible (p. 922)

Nombre d'heures de conservation du journal binaire

Le paramètre `binlog retention hours` est utilisé pour spécifier le nombre d'heures de rétention de fichiers de journaux binaires. Amazon RDS purge normalement un journal binaire dès que possible, mais il se peut que le journal binaire continue d'être requis pour la réplication avec une base de données MySQL extérieure à Amazon RDS. La valeur par défaut de `binlog retention hours` est NULL (ne pas conserver les journaux binaires).

Pour spécifier le nombre d'heures pendant lequel Amazon RDS doit conserver les journaux binaires sur une instance de base de données, utilisez la procédure stockée `mysql.rds_set_configuration` et spécifiez une période suffisamment longue pour que la réplication se produise, comme illustré dans l'exemple suivant.

```
call mysql.rds_set_configuration('binlog retention hours', 24);
```

Pour les instances de base de données MySQL, la valeur `binlog retention hours` maximale est 168 (7 jours).

Après avoir défini la période de rétention, surveillez l'utilisation du stockage de l'instance de base de données afin de garantir que les journaux binaires conservés n'utilisent pas un espace de stockage trop grand.

Délai cible

Utilisez le paramètre `target delay` pour spécifier le nombre de secondes dont il faut retarder la réplication à partir de la base de données source vers le réplica en lecture. Le décalage spécifie s'applique aux nouveaux réplicas créés à partir de l'instance de base de données actuelle. Amazon RDS réplique normalement les modifications dès que possible, mais certains environnement peuvent vouloir retarder la réplication. Par exemple, lorsque la réplication est retardée, vous pouvez restaurer par progression un réplica en lecture retardé au moment précédant un sinistre. Si une table est supprimée par mégarde, vous pouvez utiliser la réplication retardée pour la récupérer rapidement. La valeur par défaut de `target delay` est `0` (ne pas retarder la réplication).

Pour la reprise après sinistre, vous pouvez utiliser ce paramètre de configuration avec la procédure stockée mysql.rds_start_replication_until (p. 914) ou mysql.rds_start_replication_until_gtid (p. 915). Pour restaurer par progression les modifications dans un réplica en lecture retardé au moment précédant un sinistre, vous pouvez exécuter la procédure `mysql.rds_set_configuration` avec ce paramètre défini. Une fois que la procédure `mysql.rds_start_replication_until` ou `mysql.rds_start_replication_until_gtid` a arrêté la réplication, vous pouvez promouvoir le réplica en lecture pour qu'il devienne la nouvelle instance de base de données principale, en utilisant les instructions figurant dans Promotion d'un réplica en lecture en instance de bases de données autonome (p. 282).

Pour utiliser la procédure `mysql.rds_rds_start_replication_until_gtid`, la réplication basée sur des identifiants de transaction globaux (GTID) doit être activée. Pour ignorer une transaction basée sur des identifiants de transaction globaux spécifique qui est réputée pour entraîner des défaillances, vous pouvez utiliser la procédure stockée mysql.rds_skip_transaction_with_gtid (p. 916). Pour plus d'informations sur la gestion d'une réplication basée sur des identifiants de transaction globaux, consultez Utilisation de la réplication basée sur des identifiants de transaction globaux (GTID) pour Amazon RDS MySQL (p. 857).

Pour spécifier le nombre de secondes pendant lesquelles Amazon RDS retardera la réplication vers un réplica en lecture, utilisez la procédure stockée `mysql.rds_set_configuration` et spécifiez le nombre de secondes dont il faut retarder la réplication. L'exemple suivant spécifie que la réplication est retardée d'au moins une heure (3 600 secondes).

```
call mysql.rds_set_configuration('target delay', 3600);
```

La limite du paramètre `target delay` est une journée (soit 86 400 secondes).

> **Note**
>
> Le paramètre `target delay` est pris en charge uniquement pour Amazon RDS MySQL.
> Le paramètre `target delay` n'est pas pris en charge pour Amazon RDS MySQL version 8.0.

mysql.rds_show_configuration

Nombre d'heures pendant lequel les journaux binaires sont conservés.

Syntaxe

```
CALL mysql.rds_show_configuration;
```

Notes d'utilisation

Pour vérifier le nombre d'heures pendant lequel Amazon RDS conserve les journaux binaires, utilisez la procédure stockée `mysql.rds_show_configuration`.

La procédure stockée `mysql.rds_show_configuration` est disponible dans les versions MySQL Amazon RDS suivantes :

- MySQL 5.6
- MySQL 5.7
- MySQL 8.0

Exemples

L'exemple suivant affiche la période de rétention :

```
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

Termine une connexion au serveur MySQL.

Syntaxe

```
CALL mysql.rds_kill(processID);
```

Paramètres

processID

Identité du thread de connexion à terminer.

Notes d'utilisation

Chaque connexion au serveur MySQL s'exécute dans un thread distinct. Pour terminer une connexion, utilisez la procédure `mysql.rds_kill` et transmettez-lui l'ID de thread de cette connexion. Pour obtenir l'ID de thread, utilisez la commande MySQL SHOW PROCESSLIST.

Exemples

L'exemple suivant termine une connexion avec l'ID de thread 4243 :

```
call mysql.rds_kill(4243);
```

mysql.rds_kill_query

Termine une requête s'exécutant sur le serveur MySQL.

Syntaxe

```
CALL mysql.rds_kill_query(queryID);
```

Paramètres

queryID

L'identité de la requête à terminer.

Notes d'utilisation

Pour terminer une requête s'exécutant sur le serveur MySQL, utilisez la procédure `mysql_rds_kill_query` et transmettez-lui l'ID de cette requête. Pour obtenir l'ID de requête, utilisez la table MySQL INFORMATION_SCHEMA PROCESSLIST. La connexion au serveur MySQL est conservée.

Exemples

L'exemple suivant termine une requête avec l'ID de thread 230040 :

```
call mysql.rds_kill_query(230040);
```

mysql.rds_rotate_general_log

Convertit la table `mysql.general_log` en table de sauvegarde. Pour plus d'informations, consultez Fichiers journaux de base de données MySQL (p. 506).

Syntaxe

```
CALL mysql.rds_rotate_general_log;
```

Notes d'utilisation

Vous pouvez convertir la table `mysql.general_log` en table de sauvegarde en appelant la procédure `mysql.rds_rotate_general_log`. Lors de la rotation des tables de journaux, la table de journal actuelle est copiée vers une table de journal de sauvegarde et les entrées de la table de journal actuelle sont supprimées. Si la table du journal de sauvegarde existe déjà, elle est supprimée avant que la table du journal active ne soit copiée dans la sauvegarde. Si besoin, vous pouvez interroger la table de journal de sauvegarde. La table de journal de sauvegarde de la table `mysql.general_log` est nommée `mysql.general_log_backup`.

mysql.rds_rotate_slow_log

Convertit la table `mysql.slow_log` en table de sauvegarde. Pour plus d'informations, consultez Fichiers journaux de base de données MySQL (p. 506).

Syntaxe

```
CALL mysql.rds_rotate_slow_log;
```

Notes d'utilisation

Vous pouvez convertir la table `mysql.slow_log` en table de sauvegarde en appelant la procédure `mysql.rds_rotate_slow_log`. Lors de la rotation des tables de journaux, la table de journal actuelle est copiée vers une table de journal de sauvegarde et les entrées de la table de journal actuelle sont supprimées. Si la table du journal de sauvegarde existe déjà, elle est supprimée avant que la table du journal active ne soit copiée dans la sauvegarde.

Si besoin, vous pouvez interroger la table de journal de sauvegarde. La table de journal de sauvegarde de la table `mysql.slow_log` est nommée `mysql.slow_log_backup`.

mysql.rds_enable_gsh_collector

Active l'historique global des statuts (GoSH) pour prendre des instantanés par défaut aux intervalles spécifiés par `rds_set_gsh_collector`. Pour plus d'informations, consultez Gestion de l'historique global des statuts (p. 884).

Syntaxe

```
CALL mysql.rds_enable_gsh_collector;
```

mysql.rds_set_gsh_collector

Spécifie l'intervalle, en minutes, entre les instantanés pris par l'historique global des statuts (GoSH). Pour plus d'informations, consultez Gestion de l'historique global des statuts (p. 884).

Syntaxe

```
CALL mysql.rds_set_gsh_collector(intervalPeriod);
```

Paramètres

intervalPeriod

Intervalle, en minutes, entre les instantanés. La valeur par défaut est

mysql.rds_disable_gsh_collector

Désactive les instantanés pris par l'historique global des statuts (GoSH). Pour plus d'informations, consultez Gestion de l'historique global des statuts (p. 884).

Syntaxe

```
CALL mysql.rds_disable_gsh_collector;
```

mysql.rds_collect_global_status_history

Prend un instantané sur demande pour l'historique global des statuts (GosH). Pour plus d'informations, consultez Gestion de l'historique global des statuts (p. 884).

Syntaxe

```
CALL mysql.rds_collect_global_status_history;
```

mysql.rds_enable_gsh_rotation

Active la rotation du contenu de la table `mysql.global_status_history` en `mysql.global_status_history_old` à intervalles spécifiés par `rds_set_gsh_rotation`. Pour plus d'informations, consultez Gestion de l'historique global des statuts (p. 884).

Syntaxe

```
CALL mysql.rds_enable_gsh_rotation;
```

mysql.rds_set_gsh_rotation

Spécifie l'intervalle, en jours, entre deux rotations de la table `mysql.global_status_history`. La valeur par défaut est 7. Pour plus d'informations, consultez Gestion de l'historique global des statuts (p. 884).

Syntaxe

```
CALL mysql.rds_set_gsh_rotation(intervalPeriod);
```

Paramètres

intervalPeriod

Intervalle, en jours, entre deux rotations de table. La valeur par défaut est 7.

mysql.rds_disable_gsh_rotation

Désactive la rotation de table `mysql.global_status_history`. Pour plus d'informations, consultez Gestion de l'historique global des statuts (p. 884).

Syntaxe

```
CALL mysql.rds_disable_gsh_rotation;
```

mysql.rds_rotate_global_status_history

Effectue une rotation du contenu de la table `mysql.global_status_history` en `mysql.global_status_history_old` à la demande. Pour plus d'informations, consultez Gestion de l'historique global des statuts (p. 884).

Syntaxe

```
CALL mysql.rds_rotate_global_status_history;
```

Oracle sur Amazon RDS

Amazon RDS prend en charge les instances de base de données qui exécutent les versions et éditions d'Oracle Database suivantes :

- Oracle 19c, version 19.0.0.0
- Oracle 18c, version 18.0.0.0
- Oracle 12c, version 12.2.0.1
- Oracle 12c, version 12.1.0.2

> **Note**
>
> Amazon RDS prend également en charge Oracle 11g, version 11.2.0.4. Cette version devrait bientôt devenir obsolète, car Oracle ne fournit plus de correctifs pour 11.2.0.4 après la date de fin d'assistance. Pour de plus amples informations, veuillez consulter Obsolescence d'Oracle 11.2.0.4 (p. 953).

Vous pouvez créer des instances de bases de données et des instantanés de base de données, des restaurations à un moment donné, ainsi que des sauvegardes automatiques ou manuelles. Vous pouvez utiliser des instances DB exécutant Oracle dans un VPC. Vous pouvez également ajouter des fonctionnalités à votre instance de base de données DB en activant diverses options. Amazon RDS prend en charge les déploiements multi-AZ pour Oracle en tant que solution de basculement à haute disponibilité.

Pour offrir une expérience de service géré, Amazon RDS ne fournit pas l'accès shell aux instances de base de données. Il restreint également l'accès à certaines procédures système et tables qui requièrent des privilèges avancés. Vous pouvez accéder à des bases de données sur une instance de base de données en utilisant toute application client SQL standard, telle qu'Oracle SQL*Plus. Toutefois, vous ne pouvez pas accéder directement à l'hôte en utilisant Telnet ou Secure Shell (SSH).

Lorsque vous créez une instance de base de données à l'aide de votre compte principal, le compte bénéficie des privilèges DBA, avec certaines limitations. Utilisez ce compte pour des tâches administratives telles que la création de comptes de base de données supplémentaires. Vous ne pouvez pas utiliser SYS, SYSTEM ou d'autres comptes administratifs fournis par Oracle.

Avant de créer une instance de base de données, suivez la procédure de la section Configuration pour Amazon RDS (p. 62) du présent guide.

Tâches courantes de gestion pour Oracle sur Amazon RDS

Vous trouverez ci-après les tâches courantes de gestion que vous exécutez avec une instance de base de données Amazon RDS Oracle, avec des liens vers la documentation appropriée relative à chaque tâche.

Type de tâche	Documentation
Classes d'instance, stockage et PIOPS Si vous créez une instance de production, découvrez comment fonctionnent les classes d'instance, les types de stockage et les IOPS provisionnées dans Amazon RDS.	Prise en charge des classes d'instance de base de données pour Oracle (p. 933) Types de stockage Amazon RDS (p. 30)

Type de tâche	Documentation
Déploiements multi-AZ Une instance de base de données de production doit utiliser des déploiements multi-AZ. Les déploiements Multi-AZ améliorent la disponibilité, la durabilité des données et la tolérance aux pannes pour les instances de bases de données.	Haute disponibilité (multi-AZ) pour Amazon RDS (p. 43)
Amazon Virtual Private Cloud (VPC) Si votre compte AWS possède un VPC par défaut, votre instance de base de données est automatiquement créée dans le VPC par défaut. Si votre compte n'a pas de VPC par défaut et que vous voulez que l'instance de base de données soit dans un VPC, créez le VPC et les groupes de sous-réseaux avant de créer l'instance.	Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611) Utilisation d'une instance de base de données dans un VPC (p. 1620)
Groupes de sécurité Par défaut, les instances de base de données utilisent un pare-feu qui empêche l'accès. Veillez à créer un groupe de sécurité avec les adresses IP et la configuration réseau voulues pour accéder à l'instance de base de données. Le groupe de sécurité que vous créez dépend de la plateforme Amazon EC2 sur laquelle se trouve votre instance de base de données et du fait que vous accédiez ou non à votre instance de base de données depuis une instance Amazon EC2. En général, si votre instance de base de données se trouve sur la plateforme EC2-Classic, vous devez créer un groupe de sécurité de base de données. De plus, si votre instance se trouve sur la plateforme EC2-VPC, vous devez créer un groupe de sécurité VPC.	Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611) Contrôle d'accès par groupe de sécurité (p. 1590)
Groupes de paramètres Si votre instance de base de données doit nécessiter des paramètres de base de données spécifiques, vous devez créer un groupe de paramètres avant de créer l'instance de base de données.	Utilisation de groupes de paramètres de base de données (p. 225)
Groupes d'options Si votre instance de base de données doit nécessiter des options de base de données spécifiques, vous devez créer un groupe d'options avant de créer l'instance de base de données.	Options propres aux instances de bases de données Oracle (p. 1013)
Connexion à votre instance de base de données Après avoir créé un groupe de sécurité et l'avoir associé à une instance de base de données, vous pouvez vous connecter à l'instance de base de données en utilisant une application cliente SQL standard quelconque telle qu'Oracle SQL*Plus.	Connexion à une instance de base de données Oracle (p. 961)
Sauvegarde et restauration Vous pouvez configurer votre instance de base de données pour que les sauvegardes soient exécutées automatiquement ou que les instantanés soient créés manuellement, puis que les instances soient restaurées à partir des sauvegardes ou des instantanés.	Sauvegarde et restauration d'une instance de base de données Amazon RDS (p. 317)

Type de tâche	Documentation
Surveillance Vous pouvez surveiller une instance de base de données Oracle en utilisant les métriques CloudWatch Amazon RDS, les événements et la supervision améliorée.	Affichage des métriques d'instances de base de données (p. 384) Affichage d'événements Amazon RDS (p. 486)
Fichiers journaux Vous pouvez accéder aux fichiers journaux de votre instance de base de données Oracle.	Amazon RDS Fichiers journaux de base de données (p. 490)

L'utilisation d'instances de bases de données Oracle implique également des tâches avancées et des fonctions facultatives. Pour plus d'informations, consultez la documentation suivante.

- Pour plus d'informations sur les tâches d'administrateur de base de données courantes pour Oracle sur Amazon RDS, consultez Tâches DBA courantes pour les instances de bases de données Oracle (p. 1097).
- Pour plus d'informations sur la prise en charge d'Oracle GoldenGate, consultez la page Utilisation d'Oracle GoldenGate avec Amazon RDS (p. 1188).
- Pour plus d'informations sur la prise en charge de Siebel Customer Relationship Management (CRM), consultez la page Installation d'une base de données Siebel sur Oracle sur Amazon RDS (p. 1205).

Options de licence Oracle

Amazon RDS pour Oracle dispose de deux options de licence : Licence Inclus (LI) et Bring Your Own License (BYOL). Après avoir créé une instance de base de données Oracle sur Amazon RDS, vous pouvez modifier le modèle de licence en modifiant l'instance de base de données. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Licence incluse

Dans le modèle Licence incluse, vous n'avez pas besoin d'acheter séparément les licences Oracle. AWS gère la licence du logiciel de base de données Oracle. Dans ce modèle, si vous disposez d'un compte AWS Support avec assistance, contactez AWS Support pour les demandes de service relatives à Amazon RDS, comme pour celles relatives à Oracle Database.

Amazon RDS prend en charge le modèle « Licence incluse » pour les éditions suivantes d'Oracle Database :

- Oracle Database Standard Edition One (SE1)
- Oracle Database Standard Edition Two (SE2)

> **Note**
>
> Le modèle Oracle Database SE1 avec licence incluse n'est pas pris en charge dans les régions d'adhésion AWS suivantes :
>
> - Afrique (Le Cap)
> - Asie-Pacifique (Hong Kong)

- Europe (Milan)
- Moyen-Orient (Bahreïn)

Bring Your Own License (Licence à fournir)

Dans le modèle BYOL, vous pouvez utiliser vos licences de bases de données Oracle existantes pour exécuter vos déploiements Oracle sur Amazon RDS. Vous devez posséder la licence Oracle Database appropriée (avec la licence de mise à jour du logiciel et le support) pour la classe d'instance de base de données et l'édition d'Oracle Database que vous souhaitez exécuter. Vous devez aussi suivre les stratégies d'Oracle pour obtenir la licence du logiciel de base de données Oracle dans l'environnement de cloud computing. Pour plus d'informations sur la politique de gestion des licences Oracle pour Amazon EC2, consultez Licensing Oracle Software in the Cloud Computing Environment (Gestion des licences de logiciels Oracle dans l'environnement d'informatique sur le cloud).

Dans ce modèle, vous continuez d'utiliser votre compte de support Oracle actif et vous contactez Oracle directement pour les demandes de service propres à Oracle Database. Si vous disposez d'un compte AWS Support avec assistance, vous pouvez contacter AWS Support en cas de problèmes avec Amazon RDS. Amazon Web Services et Oracle disposent de processus de support multi-vendeurs pour les cas qui nécessitent une assistance de la part des deux organisations.

Amazon RDS prend en charge le modèle « Réutilisez vos licences » pour les éditions suivantes d'Oracle Database :

- Oracle Database Enterprise Edition (EE)
- Oracle Database Standard Edition (SE)
- Oracle Database Standard Edition One (SE1)
- Oracle Database Standard Edition Two (SE2)

Intégration avec AWS License Manager

Pour faciliter la surveillance de l'utilisation des licences Oracle dans le modèle BYOL, AWS License Manager s'intègre à Amazon RDS pour Oracle. License Manager prend en charge le suivi des éditions de moteur RDS pour Oracle et des packs de licences basés sur des cœurs virtuels (vCPU). Vous pouvez également utiliser License Manager avec AWS Organizations pour gérer l'ensemble de vos comptes organisationnels de manière centralisée.

> **Note**
>
> L'intégration de RDS for Oracle avec License Manager n'est pas prise en charge dans la région Asie-Pacifique (Osaka-Local).

Le tableau suivant présente les filtres d'informations sur le produit RDS for Oracle.

Filtre	Nom	Description
Engine Edition	`oracle-ee`	Oracle Database Enterprise Edition (EE)
	`oracle-se`	Oracle Database Standard Edition (SE)
	`oracle-se1`	Oracle Database Standard Edition One (SE1)
	`oracle-se2`	Oracle Database Standard Edition Two (SE2)
Pack de licence	`data guard`	Voir Utilisation des réplicas Oracle pour Amazon RDS (p. 1003) (Oracle Active Data Guard)

Filtre	Nom	Description
	`olap`	Voir Oracle OLAP (p. 1066)
	`ols`	Voir Oracle Label Security (p. 1054)
	`diagnostic pack sqlt`	Voir Oracle SQLT (p. 1080)
	`tuning pack sqlt`	Voir Oracle SQLT (p. 1080)

Vous pouvez créer une configuration de licence pour suivre l'utilisation des licences de vos instances de base de données Oracle. Dans ce cas, les ressources RDS pour Oracle qui correspondent au filtre d'informations produit sont automatiquement associées à la configuration de licence. La détection des instances de base de données Oracle peut prendre jusqu'à 24 heures.

Console

Pour créer une configuration de licence pour suivre l'utilisation des licences de vos instances de base de données Oracle

1. Accédez à https://console.aws.amazon.com/license-manager/.
2. Créez une configuration de licence.

   Pour obtenir des instructions, veuillez consulter Créer une configuration de licence dans le Guide de l'utilisateur AWS License Manager.

   Ajoutez une règle pour un RDS Product Information Filter (Filtre d'informations produit RDS) dans le panneau Product Information (Informations produit) .

   Pour de plus amples informations, veuillez consulter Informations produit dans la Référence de l'API AWS License Manager.

AWS CLI

Pour créer une configuration de licence à l'aide de AWS CLI, appelez la commande create-license-configuration. Vous pouvez utiliser les paramètres `--cli-input-json` ou `--cli-input-yaml` pour transmettre les paramètres à la commande.

Example

Le code suivant crée une configuration de licence pour Oracle Enterprise Edition.

```
aws license-manager create-license-configuration -cli-input-json file://rds-oracle-ee.json
```

Voici l'exemple de fichier `rds-oracle-ee.json` utilisé dans l'exemple.

```
{
    "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"
                }
            ]
        }
    ]
}
```

Pour de plus amples informations sur les informations produit, veuillez consulter Détection automatique de l'inventaire des ressources dans le Guide de l'utilisateur AWS License Manager.

Pour de plus amples informations sur le paramètre `--cli-input`, veuillez consulter Génération du squelette de l'interface de ligne de commande AWS et des paramètres d'entrée à partir d'un fichier d'entrée JSON ou YAML dans le Guide de l'utilisateur de l'AWS CLI.

Licences des déploiements multi-AZ Oracle

Amazon RDS prend en charge les déploiements Multi-AZ pour Oracle comme solution de basculement haute disponibilité. Le déploiement multi-AZ est conseillé pour les charges de travail de production. Pour plus d'informations, consultez Haute disponibilité (multi-AZ) pour Amazon RDS (p. 43).

Si vous utilisez le modèle Réutilisez vos licences, vous devez disposer d'une licence à la fois pour l'instance de base de données principale et l'instance de base de données de secours dans un déploiement multi-AZ.

Migration d'une édition Oracle à une autre

Pour le modèle BYOL, vous pouvez migrer depuis une édition standard (SE, SE2 ou SE2) vers une édition Enterprise Edition (EE), à condition de posséder une licence Oracle non utilisée et appropriée pour l'édition et la classe d'instance de base de données que vous prévoyez d'exécuter. En revanche, il n'est pas possible de migrer d'une édition Entreprise Edition vers d'autres éditions.

Pour changer d'édition et conserver vos données

1. Créez un snapshot de l'instance DB.

   Pour plus d'informations, consultez Création d'un instantané de base de données (p. 327).
2. Restaurez l'instantané dans une nouvelle instance de base de données et sélectionnez l'édition de base de données Oracle que vous souhaitez utiliser.

   Pour plus d'informations, consultez Restauration à partir d'un instantané de base de données (p. 329).
3. (Facultatif) Supprimez l'ancienne instance de base de données, sauf si vous souhaitez continuer de l'exécuter et que vous disposez des licences Oracle Database appropriées.

   Pour plus d'informations, consultez Suppression d'une instance de base de données (p. 313).

Prise en charge des classes d'instance de base de données pour Oracle

Les capacités de calcul et de mémoire d'une instance de base de données sont déterminées par sa classe d'instance de base de données. La classe d'instance de bases de données dont vous avez besoin

varie selon vos exigences en mémoire et en puissance de traitement. Pour plus d'informations, consultez Classes d'instances de base de données (p. 6).

Les classes d'instance de base de données prises en charge pour Oracle sont répertoriées ci-dessous.

Édition Oracle	Prise en charge d'Oracle 19c, 18c et 12c version 12.2.0.1	Prise en charge d'Oracle 12c version 12.1.0.2	Prise en charge d'Oracle 11g version 11.2.0.4
Enterprise Edition (EE) Bring Your Own License (Licence à fournir)	db.m5.large–db.m5.24xlarge db.m4.large–db.m4.16xlarge db.z1d.large–db.z1d.12xlarge db.x1e.xlarge–db.x1e.32xlarge db.x1.16xlarge–db.x1.32xlarge db.r5.large–db.r5.24xlarge db.r4.large–db.r4.16xlarge db.t3.small–db.t3.2xlarge	db.m5.large–db.m5.24xlarge db.m4.large–db.m4.16xlarge db.z1d.large–db.z1d.12xlarge db.x1e.xlarge–db.x1e.32xlarge db.x1.16xlarge–db.x1.32xlarge db.r5.large–db.r5.24xlarge db.r4.large–db.r4.16xlarge db.t3.micro–db.t3.2xlarge	db.m5.large–db.m5.24xlarge db.m4.large–db.m4.16xlarge db.z1d.large–db.z1d.12xlarge db.x1e.xlarge–db.x1e.32xlarge db.x1.16xlarge–db.x1.32xlarge db.r5.large–db.r5.24xlarge db.r4.large–db.r4.16xlarge db.t3.micro–db.t3.2xlarge
Standard Edition 2 (SE2) Bring Your Own License (Licence à fournir)	db.m5.large–db.m5.4xlarge db.m4.large–db.m4.4xlarge db.z1d.large–db.z1d.3xlarge db.x1e.xlarge–db.x1e.4xlarge db.r5.large–db.r5.4xlarge db.r4.large–db.r4.4xlarge db.t3.small–db.t3.2xlarge	db.m5.large–db.m5.4xlarge db.m4.large–db.m4.4xlarge db.z1d.large–db.z1d.3xlarge db.x1e.xlarge–db.x1e.4xlarge db.r5.large–db.r5.4xlarge db.r4.large–db.r4.4xlarge db.t3.micro–db.t3.2xlarge	—
Standard Edition 2 (SE2) Licence incluse	db.m5.large–db.m5.4xlarge db.m4.large–db.m4.4xlarge db.r5.large–db.r5.4xlarge db.r4.large–db.r4.4xlarge db.t3.small–db.t3.2xlarge	db.m5.large–db.m5.4xlarge db.m4.large–db.m4.4xlarge db.r5.large–db.r5.4xlarge db.r4.large–db.r4.4xlarge db.t3.micro–db.t3.2xlarge	—
Standard Edition 1 (SE1) Bring Your Own License	—	—	db.m5.large–db.m5.4xlarge db.m4.large–db.m4.4xlarge db.z1d.large–db.z1d.3xlarge db.x1e.xlarge–db.x1e.4xlarge

Édition Oracle	Prise en charge d'Oracle 19c, 18c et 12c version 12.2.0.1	Prise en charge d'Oracle 12c version 12.1.0.2	Prise en charge d'Oracle 11g version 11.2.0.4
(Licence à fournir)			db.r5.large–db.r5.4xlarge db.r4.large–db.r4.4xlarge db.t3.micro–db.t3.2xlarge
Standard Edition 1 (SE1) Licence incluse	—	—	db.m5.large–db.m5.4xlarge db.m4.large–db.m4.4xlarge db.r5.large–db.r5.4xlarge db.t3.micro–db.t3.2xlarge
Standard Edition (SE) Bring Your Own License (Licence à fournir)	—	—	db.m5.large–db.m5.8xlarge db.m4.large–db.m4.4xlarge db.z1d.large–db.z1d.6xlarge db.x1e.xlarge–db.x1e.8xlarge db.r5.large–db.r5.8xlarge db.r4.large–db.r4.8xlarge db.t3.micro–db.t3.2xlarge

Note

Nous invitions tous les clients Bring-Your-Own-License (Réutilisez vos licences) à consulter leur contrat de licence pour évaluer l'impact de Amazon RDS sur les obsolescences d'Oracle. Pour de plus amples informations sur la capacité de calcul des classes d'instance de base de données prises en charge par Amazon RDS for Oracle, veuillez consulter Classes d'instances de base de données (p. 6) et Configuration du processeur pour une classe d'instance de base de données (p. 13).

Classes d'instance de base de données db.t2 pour Oracle obsolètes

Les classes d'instance de base de données db.t2 sont obsolètes pour Amazon RDS for Oracle. Les classes d'instance de base de données db.t2 ont été remplacées par les classes d'instance de base de données db.t3 plus performantes et généralement meilleur marché. À partir du 15 janvier 2020, Amazon RDS pour Oracle mettra automatiquement à échelle les instances de base de données db.t2 DB aux classes d'instances de base de données db.t3 comparables.

Si vous disposez d'instances de base de données qui utilisent des classes d'instance de base de données db.t2, Amazon RDS modifiera automatiquement chacune d'entre elles pour utiliser une classe d'instance de base de données non obsolète. Vous pouvez vous-même échanger la classe d'instance de base de données pour une instance de base de données en modifiant l'instance de base de données. Pour de plus amples informations, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

Si vous disposez d'instantanés de base de données d'instances de base de données qui utilisaient des classes d'instance de base de données db.t2, vous pouvez choisir une classe d'instance de base de données non obsolète lorsque vous restituez les instantanés de base de données. Pour plus d'informations, consultez Restauration à partir d'un instantané de base de données (p. 329).

> Note
>
> L'hyper-threading est activé par défaut pour les classes d'instances de base de données db.t3. Lorsque les instances de base de données exécutant la classe d'instance de base de données db.t2 sont migrées, le nombre de vCPU est défini automatiquement sur le nombre associé à la classe d'instance de base de données db.t3 comparable. Pour en savoir plus sur les fonctionnalités de gestion des vCPU disponibles dans Amazon RDS pour Oracle et les paramètres par défaut de chaque classe d'instance de base de données db.t3, consultez Configuration du processeur pour une classe d'instance de base de données (p. 13).

Classes d'instance de base de données db.m3 et db.r3 pour Oracle obsolètes

Les classes d'instance de base de données db.m3 et db.r3 de Amazon RDS pour Oracle sont obsolètes. Ces classes d'instance de base de données ont été remplacées par des classes d'instance de base de données qui offrent un meilleur profil de performances et qui sont généralement disponibles à moindre coût. À partir du 30 septembre 2019, Amazon RDS pour Oracle mettra automatiquement à échelle les instances de base de données aux classes d'instances de base de données non-obsolètes.

Si vous disposez d'instances de base de données qui utilisent des classes d'instance de base de données db.m3 et db.r3, Amazon RDS modifiera automatiquement chacune d'entre elles pour utiliser une classe d'instance de base de données non obsolète. Vous pouvez vous-même échanger la classe d'instance de base de données pour une instance de base de données en modifiant l'instance de base de données. Pour de plus amples informations, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

Si vous disposez d'instantanés de base de données d'instances de base de données qui utilisaient des classes d'instance de base de données db.m3 ou db.r3, vous pouvez choisir une classe d'instance de base de données non obsolète lorsque vous restituez les instantanés de base de données. Pour plus d'informations, consultez Restauration à partir d'un instantané de base de données (p. 329).

Classes d'instance de base de données db.m1 et db.m2 pour Oracle obsolètes

Les classes d'instance de base de données db.m1 et db.m2 de Amazon RDS pour Oracle sont obsolètes. Ces classes d'instance de base de données ont été remplacées par des classes d'instance de base de données qui offrent un meilleur profil de performances et qui sont généralement disponibles à moindre coût. À partir du 12 septembre 2018, Amazon RDS pour Oracle mettra automatiquement à échelle les instances de base de données aux classes d'instances de base de données non-obsolètes.

Si vous disposez d'instances de base de données qui utilisent des classes d'instance de base de données db.m1 et db.m2, Amazon RDS modifiera automatiquement chacune d'entre elles pour utiliser une classe d'instance de base de données non obsolète. Vous pouvez vous-même échanger la classe d'instance de base de données pour une instance de base de données en modifiant l'instance de base de données. Pour de plus amples informations, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

Si vous disposez d'instantanés de base de données d'instances de base de données qui utilisaient des classes d'instance de base de données db.m1 ou db.m2, vous pouvez choisir une classe d'instance de base de données non obsolète lorsque vous restituez les instantanés de base de données. Pour plus d'informations, consultez Restauration à partir d'un instantané de base de données (p. 329).

Limites de taille des fichiers Oracle dans Amazon RDS

La taille maximale des fichiers sur les instances de base de données Oracle dans Amazon RDS est de 16 TiO (tébioctets). Si vous essayez de redimensionner un fichier de données dans un tablespace bigfile vers une valeur supérieure à la limite, une erreur comme la suivante se produit.

```
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
```

Sécurité Oracle

Le moteur de base de données Oracle utilise une sécurité basée sur le rôle. Un rôle est un ensemble de privilèges pouvant être accordés ou révoqués à un utilisateur. Un rôle prédéfini, appelé `DBA`, autorise normalement tous les privilèges d'administration sur une base de données Oracle. Les privilèges suivants ne sont pas disponibles pour le rôle DBA sur une instance de base de données Amazon RDS en utilisant le moteur Oracle :

- `ALTER DATABASE`
- `ALTER SYSTEM`
- `CREATE ANY DIRECTORY`
- `DROP ANY DIRECTORY`
- `GRANT ANY PRIVILEGE`
- `GRANT ANY ROLE`

Lorsque vous créez une instance de base de données, le compte utilisateur principal que vous utilisez pour créer l'instance obtient des privilèges DBA (avec certaines restrictions). Utilisez ce compte utilisateur principal pour toutes les tâches administratives comme la création de comptes utilisateurs supplémentaires dans la base de données. Vous ne pouvez pas utiliser l'utilisateur `SYS`, l'utilisateur `SYSTEM` et d'autres comptes administratifs fournis par Oracle.

Amazon RDS Oracle prend en charge les connexions chiffrées SSL/TLS ainsi que l'option Oracle Native Network Encryption (NNE) pour chiffrer les connexions entre votre application et votre instance de base de données Oracle. Pour plus d'informations sur l'utilisation de SSL avec Oracle sur Amazon RDS, consultez Utilisation de SSL avec une instance de base de données Oracle (p. 937). Pour plus d'informations sur l'option Oracle Native Network Encryption, consultez Oracle NNE (Native Network Encryption) (p. 1062).

Utilisation de SSL avec une instance de base de données Oracle

Secure Sockets Layer (SSL) est un protocole de norme industrielle utilisé pour sécuriser les connexions réseau entre client et serveur. Après la version 3.0 de SSL, le nom du protocole a été changé à Transport Layer Security (TLS), mais il est encore souvent désigné par SSL et nous y faisons référence sous le nom de SSL. Amazon RDS prend en charge le chiffrement pour les instances de base de données Oracle. En utilisant SSL, vous pouvez chiffrer une connexion entre votre application client et votre instance de base de données Oracle. Le support SSL est disponible dans toutes les régions AWS pour Oracle.

Vous activez le chiffrement SSL (Secure Sockets Layer) pour une instance de base de données Oracle en ajoutant l'option Oracle SSL au groupe d'options associé à l'instance de base de données Oracle. Amazon RDS utilise un deuxième port requis par Oracle pour les connexions SSL. Cette approche permet aussi bien aux communications en texte clair que celles à chiffrement SSL de se produire simultanément entre une instance de base de données et un client Oracle. Par exemple, vous pouvez utiliser le port avec une communication en texte clair pour communiquer avec d'autres ressources à l'intérieur d'un VPC, tout en utilisant le port avec une communication à chiffrement SSL pour communiquer avec des ressources extérieures au VPC.

Pour plus d'informations, consultez Oracle Secure Sockets Layer (SSL) (p. 1068).

> **Note**
>
> Vous ne pouvez pas utiliser le chiffrement SSL et le chiffrement Oracle NNE sur la même instance de base de données. Avant d'utiliser le chiffrement SSL, vous devez désactiver tout autre chiffrement de connexion.

Oracle 19c avec Amazon RDS

Amazon RDS prend en charge Oracle version 19c, qui inclut Oracle Enterprise Edition et Oracle Standard Edition Two.

Oracle 19c version 19.0.0.0 inclut beaucoup de nouvelles fonctions et mises à jour par rapport à la version précédente. Cette section couvre les fonctions et modifications importantes liées à l'utilisation d'Oracle 19c version 19.0.0.0 sur Amazon RDS. Pour obtenir la liste complète des évolutions, veuillez consulter la documentation Oracle Database 19c. Pour obtenir la liste complète des fonctionnalités prises en charge par chaque édition d'Oracle 19c, veuillez consulter Permitted Features, Options, and Management Packs by Oracle Database Offering dans la documentation Oracle.

Modifications des paramètres Amazon RDS pour Oracle 19c version 19.0.0.0

Oracle 19c version 19.0.0.0 comporte plusieurs nouveaux paramètres ainsi que des paramètres présentant de nouvelles plages et de nouvelles valeurs par défaut.

Le tableau suivant indique les nouveaux paramètres Amazon RDS pour Oracle 19c version 19.0.0.0.

Nom	Valeurs	Adapta	Description
lob_signature_enable	TRUE, FALSE (par défaut)	O	Active ou désactive la fonction de signature de localisateur LOB.
max_datapump_parallel_per_job	1 à 1 024 ou AUTO	O	Indique le nombre maximal de processus parallèles autorisés pour chaque tâche Oracle Data Pump.

Le paramètre `compatible` a une nouvelle valeur maximale pour Oracle 19c version 19.0.0.0 sur Amazon RDS. Le tableau suivant présente la nouvelle valeur par défaut.

Nom du paramètre	Valeur maximale pour Oracle 19c version 19.0.0.0	Valeur maximale pour Oracle 18c version 18.0.0.0
compatible	19.0.0	18.0.0

Les paramètres suivants ont été supprimés dans Oracle 19c version 19.0.0.0 :

- exafusion_enabled
- max_connections
- o7_dictionary_access

Oracle 18c avec Amazon RDS

Amazon RDS prend en charge Oracle version 18c, qui inclut Oracle Enterprise Edition et Oracle Standard Edition Two.

Oracle 18c version 18.0.0.0 comporte un grand nombre de nouveautés et de mises à jour par rapport à la version précédente. Dans cette section, vous allez découvrir les fonctionnalités et les évolutions liées à l'utilisation d'Oracle 18c version 18.0.0.0 sur Amazon RDS. Pour obtenir la liste complète des évolutions, consultez Oracle Database 18c. Pour obtenir la liste complète des fonctionnalités prises en charge par chaque édition d'Oracle 18c, veuillez consulter Permitted Features, Options, and Management Packs by Oracle Database Offering dans la documentation Oracle.

Évolution des paramètres Amazon RDS pour Oracle 18c version 18.0.0.0

Oracle 18c version 18.0.0.0 comporte plusieurs nouveaux paramètres ainsi que des paramètres présentant de nouvelles plages et de nouvelles valeurs par défaut.

Le tableau suivant présente les nouveaux paramètres Amazon RDS pour Oracle 18c version 18.0.0.0.

Nom	Valeurs	Adapta	Description
adg_account_info_tracking	LOCAL (par défaut), GLOBAL	N	Contrôle les tentatives de connexion d'utilisateurs sur les bases de données de veille Active Data Guard. Il étend le contrôle des informations de sécurité des comptes utilisateur.
inmemory_optimized_arithmetic	ENABLE, DISABLE (par défaut)	O	Encode le type de données `NUMBER` dans les tables en mémoire compressées avec `QUERY LOW` comme entier natif de largeur fixe mis à l'échelle par un exposant courant.
optimizer_ignore_hints	TRUE, FALSE (par défaut)	O	Précise si les indicateurs incorporés sont ignorés.
optimizer_ignore_parallel_hints	TRUE, FALSE (par défaut)	O	Précise que les indicateurs parallèles incorporés sont ignorés.
parallel_min_degree	1 (par défaut) et valeur supérieure ou CPU	O	Contrôle le degré minimum de parallélisme calculé par le degré de parallélisme automatique.

Le paramètre `compatible` présente une nouvelle valeur par défaut pour Oracle 18c version 18.0.0.0 sur Amazon RDS. Le tableau suivant présente la nouvelle valeur par défaut.

Nom du paramètre	Valeur par défaut d'Oracle 18c version 18.0.0.0	Valeur par défaut d'Oracle 12c version 12.2.0.1
compatible	18.0.0	12.2.0

Les paramètres suivants ont été supprimés dans Oracle 18c version 18.0.0.0 :

- standby_archive_dest
- utl_file_dir

Oracle 12c avec Amazon RDS

Amazon RDS prend en charge Oracle version 12c, qui inclut Oracle Enterprise Edition et Oracle Standard Edition Two. La version Oracle 12c inclut deux versions majeures :

- Oracle 12c, version 12.2.0.1 avec Amazon RDS (p. 940)
- Oracle 12c, version 12.1.0.2 avec Amazon RDS (p. 943)

Oracle 12c, version 12.2.0.1 avec Amazon RDS

Oracle 12c version 12.2.0.1 inclut beaucoup de nouvelles fonctions et mises à jour à partir de la version précédente. Cette section couvre les fonctions et modifications importantes liées à l'utilisation d'Oracle 12c version 12.2.0.1 sur Amazon RDS. Pour obtenir la liste complète des modifications, consultez la documentation Oracle 12c version 12.2. Pour obtenir la liste complète des fonctionnalités prises en charge par chaque édition d'Oracle 12c, consultez Permitted Features, Options, and Management Packs by Oracle Database Offering dans la documentation Oracle.

Modification des paramètres Amazon RDS pour Oracle 12c version 12.2.0.1

Oracle 12c version 12.2.0.1 inclut 20 nouveaux paramètres en plus de plusieurs paramètres avec de nouvelles plages et de nouvelles valeurs par défaut.

Le tableau suivant indique les nouveaux paramètres Amazon RDS pour Oracle 12c version 12.2.0.1.

Nom	Valeurs	Adapta	Description
allow_global_dblinks	TRUE, FALSE (par défaut)	O	Spécifie si la recherche LDAP est autorisée pour les liens de base de données.
approx_for_aggregation	TRUE, FALSE (par défaut)	O	Remplace le traitement exact des requêtes d'agrégation par un traitement approximatif.
approx_for_count_distinct	TRUE, FALSE (par défaut)	O	Remplace automatiquement les requêtes `COUNT (DISTINCT expr)` par des requêtes `APPROX_COUNT_DISTINCT`.

Nom	Valeurs	Adapta	Description
approx_for_percentile	NONE (par défaut), PERCENTILE_CONT, PERCENTILE_CONT DETERMINISTIC, PERCENTILE_DISC, PERCENTILE_DISC DETERMINISTIC, ALL, ALL DETERMINISTIC	O	Convertit les fonctions exactes relatives aux percentiles en fonctions équivalentes approximatives.
cursor_invalidation	DEFERRED, IMMEDIATE (par défaut)	O	Contrôle si l'invalidation de curseur utilisée par défaut pour les instructions DDL est immédiate ou reportée.
data_guard_sync_latency	Valeur comprise entre 0 (par défaut) et le nombre de secondes spécifié par l'attribut NET_TIMEOUT pour le paramètre LOG_ARCHIVE_DEST_n	O	Contrôle le nombre de secondes qu'attend le processus d'écriture de journaux (LGWR) après la réponse de la première connexion d'une série de connexions Oracle Data Guard en mode de transport SYNC redo.
data_transfer_cache_size	Valeur comprise entre 0 et 512M, arrondie au millier le plus proche	O	Définit la taille du cache de transfert des données (en octets) utilisée pour recevoir les blocs de données (généralement à partir d'une base de données principale dans un environnement Oracle Data Guard) utilisés par une instance lors de l'exécution quand une commande RMAN RECOVER... NONLOGGED BLOCK est en cours d'exécution.
inmemory_adg_enabled	TRUE (par défaut), FALSE	O	Indique si le cache en mémoire d'Active Data Guard est activé en plus de la taille du cache en mémoire.
inmemory_expressions_usage	STATIC_ONLY, DYNAMIC_ONLY,ENABLE (par défaut), DISABLE	O	Contrôle les expressions en mémoire (expressions IM) indiquées dans le stockage de colonnes en mémoire (IM column store) et disponibles pour les requêtes.
inmemory_virtual_columns	ENABLE, MANUAL (par défaut), DISABLE	O	Contrôle les expressions en mémoire (expressions IM) indiquées dans le stockage de colonnes en mémoire (IM column store) et disponibles pour les requêtes.
instance_abort_delay_time	0 (par défaut) ou valeur supérieure	O	Spécifie le délai d'attente (en secondes) au-delà duquel une instance initiée interne est abandonnée, notamment en cas d'arrêt d'un processus vital ou d'erreur d'instance non récupérable.

Nom	Valeurs	Adapta	Description
instance_mode	READ-WRITE (par défaut), READ-ONLY, READ-MOSTLY	N	Indique s'il s'agit d'une instance en lecture/écriture, en lecture ou principalement en lecture.
long_module_action	TRUE (par défaut), FALSE	O	Permet l'utilisation de plus grandes longueurs pour les modules et les actions.
max_idle_time	Valeur comprise entre 0 (par défaut) et un nombre entier maximal. Une valeur égale à 0 signifie qu'aucune limite n'est appliquée.	O	Spécifie le nombre maximal de minutes pendant lesquelles une session peut rester inactive. Passé ce délai, la session prend fin automatiquement.
optimizer_adaptive_plans	TRUE (par défaut), FALSE	O	Contrôle les plans adaptatifs. Les plans adaptatifs sont des plans d'exécution intégrant différents choix qui sont déterminés lors de l'exécution en fonction des statistiques collectées lors de l'exécution d'une requête.
optimizer_adaptive_statistics	TRUE, FALSE (par défaut)	O	Contrôle les statistiques adaptatives. Certaines formes de requêtes sont trop complexes pour ne dépendre que des statistiques de base d'une table. L'optimiseur complète donc ces dernières avec des statistiques adaptatives.
outbound_dblink_protocols	ALL (par défaut), NONE, TCP, TCPS, IPC	N	Spécifie les protocoles réseau autorisés pour la communication liées aux liens de base de données sortants.
resource_manage_goldengate	TRUE, FALSE (par défaut)	O	Détermine si les processus Oracle GoldenGate de la base de données sont gérés par les ressources.
standby_db_preserve_states	NONE (par défaut), SESSION, ALL	N	Détermine si les sessions utilisateur et les autres états internes de l'instance sont maintenus lorsqu'une base de données de secours physique est convertie en base de données principale.
uniform_log_timestamp_format	TRUE (par défaut), FALSE	O	Spécifie l'utilisation d'un format d'horodatage uniforme dans les fichiers de trace Oracle Database (.trc) et les fichiers journaux (comme le journal d'alertes).

Le paramètre `compatible` a une nouvelle valeur par défaut pour Oracle 12c version 12.2.0.1 sur Amazon RDS. Le tableau suivant présente la nouvelle valeur par défaut.

Nom du paramètre	Valeur par défaut d'Oracle 12c version 12.2.0.1	Valeur par défaut d'Oracle 12c version 12.1.0.2
compatible	12.2.0	12.0.0

Le paramètre `optimizer_features_enable` a une nouvelle plage de valeurs pour Oracle 12c version 12.2.0.1 sur Amazon RDS. Le tableau suivant montre les nouvelles et anciennes plages de valeurs.

Nom du paramètre	Plage 12c version 12.2.0.1	Plage 12c version 12.1.0.2
optimizer_features_enable	8.0.0 à 12.2.0.1	8.0.0 à 12.1.0.2

Les paramètres suivants ont été supprimés dans Oracle 12c version 12.2.0.1 :

- global_context_pool_size
- max_enabled_roles
- optimizer_adaptive_features
- parallel_automatic_tuning
- parallel_degree_level
- use_indirect_data_buffers

Le paramètre suivant n'est pas pris en charge dans Oracle 12c version 12.2.0.1 et les versions ultérieures :

- sec_case_sensitive_logon

Modification de sécurité Amazon RDS pour Oracle 12c version 12.2.0.1

Dans Oracle 12c version 12.2.0.1, l'octroi direct du privilège `ADMINISTER DATABASE TRIGGER` est obligatoire pour les propriétaires de déclencheurs au niveau de la base de données. Lors d'une mise à niveau de version majeure vers Oracle 12c version 12.2.0.1, Amazon RDS accorde ce privilège à tous les utilisateurs qui possèdent un déclencheur pour qu'ils reçoivent les privilèges requis. Pour de plus amples informations, consultez le document de support My Oracle 2275535.1.

Oracle 12c, version 12.1.0.2 avec Amazon RDS

Oracle 12c version 12.1.0.2 offre plus de 500 nouvelles fonctions et mises à jour par rapport à la version précédente. Cette section couvre les fonctions et modifications importantes liées à l'utilisation d'Oracle 12c version 12.1.0.2 sur Amazon RDS. Pour obtenir la liste complète des modifications, consultez la documentation Oracle 12c version 12.1. Pour obtenir la liste complète des fonctions prises en charge par chaque version Oracle 12c, consultez Permitted Features, Options, and Management Packs by Oracle Database Edition dans la documentation Oracle.

Oracle 12c version 12.1.0.2 inclut 16 nouveaux paramètres qui impactent votre instance de base de données Amazon RDS, ainsi que 18 nouveaux privilèges système, plusieurs packages qui ne sont plus pris en charge et plusieurs nouveaux paramètres de groupe d'options. Pour plus d'informations sur ces modifications, consultez les sections suivantes.

Modification des paramètres Amazon RDS pour Oracle 12c version 12.1.0.2

Oracle 12c version 12.1.0.2 inclut 16 nouveaux paramètres en plus de plusieurs paramètres avec de nouvelles plages et de nouvelles valeurs par défaut.

Le tableau suivant indique les nouveaux paramètres Amazon RDS pour Oracle 12c version 12.1.0.2.

Nom	Valeurs	Adapta	Description
connection_brokers	CONNECTION_BROKERS = broker_description[,...]	N	Spécifie les types de broker de connexion, le nombre de broker de connexion de chaque type et le nombre maximum de connexions par broker.
db_index_compression_inheritance	TABLESPACE, TABL, ALL, NONE	O	Affiche les options définies pour l'héritage de compression au niveau de la table ou de l'espace de table.
db_big_table_cache_percent_target	0-90	O	Spécifie la taille cible de la section cache pour mettre en cache automatiquement des tables volumineuses, comme le pourcentage du cache en mémoire.
heat_map	ON, OFF	O	Permet à la base de données de suivre l'accès en lecture et écriture de tous les segments, ainsi que les modifications des blocs de base de données, qui sont dues aux instructions DML (Data Manipulation Language) et DDL (Data Definition Language).
inmemory_clause_default	INMEMORY, NO INMEMORY	O	INMEMORY_CLAUSE_DEFAULT vous permet de spécifier une clause de stockage de colonnes en mémoire (IM column store) par défaut pour les nouvelles tables et les vues matérialisées.
inmemory_clause_default_memcompress	NO MEMCOMPRESS, MEMCOMPRESS FOR DML, MEMCOMPRESS FOR QUERY, MEMCOMPRESS FOR QUERY LOW, MEMCOMPRESS FOR QUERY HIGH, MEMCOMPRESS FOR CAPACITY, MEMCOMPRESS FOR CAPACITY LOW,	O	Consultez INMEMORY_CLAUSE_DEFAULT.

Nom	Valeurs	Adapta	Description
	MEMCOMPRESS FOR CAPACITY HIGH		
inmemory_clause_default_priority	PRIORITY LOW, PRIORITY MEDIUM, PRIORITY HIGH, PRIORITY CRITICAL, PRIORITY NONE	O	Consultez INMEMORY_CLAUSE_DEFAULT.
inmemory_force	DEFAULT, OFF	O	IINMEMORY_FORCE vous permet de spécifier si les tables et les vues matérialisées qui sont définies comme INMEMORY sont remplies ou non dans le stockage de colonnes en mémoire (IM column store).
inmemory_max_populate_servers	Null	N	INMEMORY_MAX_POPULATE_SERVERS spécifie le nombre maximum de serveurs en arrière-plan à utiliser pour le remplissage du stockage de colonnes en mémoire (IM column store), afin que ces serveurs ne surchargent pas le reste du système.
inmemory_query	ENABLE (par défaut), DISABLE	O	INMEMORY_QUERY est utilisé pour activer ou désactiver les requêtes en mémoire pour la base de données entière au niveau de la session ou du système.
inmemory_size	0, 104857600-274877906944	O	INMEMORY_SIZE définit la taille du stockage de colonnes en mémoire (IM column store) sur une instance de base de données.
inmemory_trickle_repopulate_servers_percent	0 à 50	O	INMEMORY_TRICKLE_REPOPULATE_SERVERS_P limite le nombre maximum de serveurs en arrière-plan utilisés pour le re-remplissage du stockage de colonnes en mémoire (IM column store). Cette limite est appliquée, car le re-remplissage au compte-gouttes est conçu pour utiliser uniquement un faible pourcentage de ces serveurs.
max_string_size	STANDARD (par défaut), EXTENDED	N	Contrôle la taille maximum de VARCHAR2, NVARCHAR2 et RAW. Pour plus d'informations, consultez Utilisation des types de données étendus (p. 959).
optimizer_adaptive_features	TRUE (par défaut), FALSE	O	Active ou désactive toutes les fonctions d'optimiseur adaptatives.

Nom	Valeurs	Adapta	Description
optimizer_adaptive_reporting_only	TRUE, FALSE (par défaut)	O	Contrôle le mode rapport seulement pour les optimisations adaptatives.
pdb_file_name_convert	Il n'existe aucune valeur par défaut.	N	Mappe les noms des fichiers existants vers les noms de nouveaux fichiers.
pga_aggregate_limit	0-max de mémoire	O	Spécifie une limite sur la mémoire PGA cumulée consommée par l'instance.
processor_group_name	Il n'existe aucune valeur par défaut.	N	Demande à l'instance de base de données de s'exécuter dans le groupe de processeurs du système d'exploitation spécifié.
spatial_vector_acceleration	TRUE, FALSE	N	Active ou désactive l'accélération des vecteurs spatiaux qui font partie de l'option spatiale.
temp_undo_enabled	TRUE, FALSE (par défaut)	O	Détermine si les transactions dans une session particulière peuvent avoir un journal de transaction temporaire.
threaded_execution	TRUE, FALSE	N	Active le modèle Oracle multitâches, mais empêche l'authentification du système d'exploitation.
unified_audit_sga_queue_size	1 Mo - 30 Mo	O	Spécifie la taille de la file d'attente de la zone SGA (System Global Area) pour l'audit unifié.
use_dedicated_broker	TRUE, FALSE	N	Détermine comment les serveurs dédiés sont générés.

Plusieurs paramètres ont de nouvelles plages de valeurs pour Oracle 12c version 12.1.0.2 sur Amazon RDS. Le tableau suivant montre les nouvelles et anciennes plages de valeurs.

Nom du paramètre	Plage 12c version 12.1.0.2	Plage 11g
audit_trail	os | db [, extended] | xml [, extended]	os | db [, extended] | xml [, extended] | true | false
compatible	Les exigences pour `COMPATIBLE` sont les suivantes : • Si vous effectuez une mise à niveau vers 12.1.0.2, `COMPATIBLE` doit être défini sur 12.0 ou version ultérieure. Pour les nouvelles instances de base de données 12.1.0.2, `COMPATIBLE` est défini sur 12.1.0.2. • Si vous mettez à niveau vers 12.2.0.1, 18c ou 19c, `COMPATIBLE` doit être défini sur 11.2.0 ou version ultérieure.	A partir de 11.2.0 sur Amazon RDS

Nom du paramètre	Plage 12c version 12.1.0.2	Plage 11g
	Si `COMPATIBLE` n'est pas explicitement défini, Amazon RDS définit automatiquement ce paramètre sur 12.0.0.	
db_securefile	PERMITTED | PREFERRED | ALWAYS | IGNORE | FORCE	PERMITTED | ALWAYS | IGNORE | FORCE
db_writer_processes	1-100	1-36
optimizer_features_enable	8.0.0 à 12.1.0.2	8.0.0 à 11.2.0.4
parallel_degree_policy	MANUAL,LIMITED,AUTO,ADAPTIVE	MANUAL,LIMITED,AUTO
parallel_min_server	0 à parallel_max_servers	CPU_COUNT * PARALLEL_THREADS_PER_CPU * 2 à parallel_max_servers

Un paramètre a une nouvelle valeur par défaut pour Oracle 12c sur Amazon RDS. Le tableau suivant présente la nouvelle valeur par défaut.

Nom du paramètre	Valeur par défaut d'Oracle 12c	Valeur par défaut d'Oracle 11g
job_queue_processes	50	1000

Privilèges système Amazon RDS pour Oracle 12c version 12.1.0.2

Plusieurs nouveaux privilèges système ont été accordés au compte du système pour Oracle 12c version 12.1.0.2. Ces nouveaux privilèges système incluent les suivants :

- ALTER ANY CUBE BUILD PROCESS
- ALTER ANY MEASURE FOLDER
- ALTER ANY SQL TRANSLATION PROFILE
- CREATE ANY SQL TRANSLATION PROFILE
- CREATE SQL TRANSLATION PROFILE
- DROP ANY SQL TRANSLATION PROFILE
- EM EXPRESS CONNECT
- EXEMPT DDL REDACTION POLICY
- EXEMPT DML REDACTION POLICY
- EXEMPT REDACTION POLICY
- LOGMINING
- REDEFINE ANY TABLE
- SELECT ANY CUBE BUILD PROCESS
- SELECT ANY MEASURE FOLDER
- USE ANY SQL TRANSLATION PROFILE

Options Amazon RDS pour Oracle 12c version 12.1.0.2

Plusieurs options Oracle ont changé entre les versions Oracle 11g et Oracle 12c version 12.1.0.2, bien que la plupart soient identiques entre les deux versions. Les modifications de la version Oracle 12c version 12.1.0.2 incluent les suivantes :

- Oracle Enterprise Manager Database Express 12c a remplacé Oracle Enterprise Manager 11g Database Control. Pour plus d'informations, consultez Oracle Enterprise Manager Database Express (p. 1037).
- L'option XMLDB est installée par défaut dans Oracle 12c version 12.1.0.2. Vous n'avez plus besoin d'installer cette option vous-même.

Packages PL/SQL Amazon RDS pour Oracle 12c version 12.1.0.2

Oracle 12c version 12.1.0.2 inclut plusieurs nouveaux packages PL/SQL intégrés. Les packages inclus avec Amazon RDS Oracle 12c version 12.1.0.2 sont les suivants.

Nom du package	Description
CTX_ANL	Le package CTX_ANL est utilisé avec AUTO_LEXER et fournit des procédures pour l'ajout et le dépôt d'un dictionnaire personnalisé depuis lexer.
DBMS_APP_CONT	Le package DBMS_APP_CONT fournit une interface pour déterminer si la transaction à la volée sur une session désormais indisponible est validée ou non, et si le dernier appel sur cette session est terminé ou non.
DBMS_AUTO_REPORT	Le package DBMS_AUTO_REPORT fournit une interface pour consulter les données SQL Monitoring et Real-time Automatic Database Diagnostic Monitor (ADDM) qui ont été capturées dans Automatic Workload Repository (AWR).
DBMS_GOLDENGATE_AUTH	Le package DBMS_GOLDENGATE_AUTH fournit des sous-programmes pour accorder et révoquer des privilèges aux administrateurs GoldenGate.
DBMS_HEAT_MAP	Le package DBMS_HEAT_MAP fournit une interface pour externaliser les cartes thermiques à différents niveaux de stockage dont le bloc, l'extension, le segment, l'objet et l'espace de table.
DBMS_ILM	Le package DBMS_ILM fournit une interface pour implémenter des stratégies de gestion du cycle de vie des informations en utilisant les stratégies Automatic Data Optimization (ADO).
DBMS_ILM_ADMIN	Le package DBMS_ILM_ADMIN fournit une interface pour personnaliser l'exécution de la stratégie Automatic Data Optimization (ADO).
DBMS_PART	Le package DBMS_PART fournit une interface pour les opérations de maintenance et de gestion sur les objets partitionnés.
DBMS_PRIVILEGE_CAPTURE	Le package DBMS_PRIVILEGE_CAPTURE fournit une interface pour analyser les privilèges de base de données.

Nom du package	Description
DBMS_QOPATCH	Le package DBMS_QOPATCH fournit une interface pour consulter les correctifs de base de données installés.
DBMS_REDACT	Le package DBMS_REDACT fournit une interface vers Oracle Data Redaction, qui vous permet de masquer (censurer) les données qui sont renvoyées par les requêtes émises par des utilisateurs aux privilèges restreints ou une application.
DBMS_SPD	Le package DBMS_SPD fournit des sous-programmes pour la gestion des directives de plan SQL (SPD).
DBMS_SQL_TRANSLATOR	Le package DBMS_SQL_TRANSLATOR fournit une interface pour créer, configurer et utiliser des profils de traduction SQL.
DBMS_SQL_MONITOR	Le package DBMS_SQL_MONITOR fournit des informations sur la supervision SQL en temps réel et la supervision des opérations de base de données en temps réel.
DBMS_SYNC_REFRESH	Le package DBMS_SYNC_REFRESH fournit une interface pour réaliser une actualisation synchrone des vues matérialisées.
DBMS_TSDP_MANAGE	Le package DBMS_TSDP_MANAGE fournit une interface pour importer et gérer les colonnes sensibles et les types de colonnes sensibles dans la base de données. DBMS_TSDP_MANAGE est utilisé avec le package DBMS_TSDP_PROTECT pour les stratégies de protection des données sensibles transparentes (TSDP). DBMS_TSDP_MANAGE est disponible uniquement avec la version Enterprise Edition.
DBMS_TSDP_PROTECT	Le package DBMS_TSDP_PROTECT fournit une interface pour configurer des stratégies de Transparent Sensitive Data Protection (TSDP) (Protection transparente de données sensibles) conjointement avec le package DBMS_TSDP_MANAGE. DBMS_TSDP_PROTECT est disponible uniquement avec la version Enterprise Edition.
DBMS_XDB_CONFIG	Le package DBMS_XDB_CONFIG fournit une interface pour configurer Oracle XML DB et son référentiel.
DBMS_XDB_CONSTANTS	Le package DBMS_XDB_CONSTANTS fournit une interface vers les constantes communément utilisées. Oracle recommande d'utiliser des constantes plutôt que des chaînes dynamiques pour éviter les erreurs typographiques.
DBMS_XDB_REPOS	Le package DBMS_XDB_REPOS fournit une interface pour fonctionner sur le référentiel de la base de données Oracle XML.
DBMS_XMLSCHEMA_ANNOTATE	Le package DBMS_XMLSCHEMA_ANNOTATE fournit une interface pour gérer et configurer le modèle de stockage structuré, principalement via l'utilisation des annotations de schéma de pré-inscription.
DBMS_XMLSTORAGE_MANAGE	Le package DBMS_XMLSTORAGE_MANAGE fournit une interface pour gérer et modifier le stockage XML une fois que l'inscription du schéma est terminée.

Nom du package	Description
DBMS_XSTREAM_ADM	Le package DBMS_XSTREAM_ADM fournit des interfaces pour les changements de base de données en streaming entre une base de données Oracle et d'autres systèmes. XStream permet aux applications d'envoyer ou de récupérer en streaming les changements de base de données.
DBMS_XSTREAM_AUTH	Le package DBMS_XSTREAM_AUTH fournit des sous-programmes pour accorder et révoquer des privilèges aux administrateurs XStream.
UTL_CALL_STACK	Le package UTL_CALL_STACK fournit une interface pour communiquer des informations sur les sous-programmes en cours d'exécution.

Packages Oracle 12c version 12.1.0.2 non pris en charge

Plusieurs packages PL/SQL Oracle 11g ne sont pas pris en charge dans Oracle 12c version 12.1.0.2. Ces packages sont les suivants :

- DBMS_AUTO_TASK_IMMEDIATE
- DBMS_CDC_PUBLISH
- DBMS_CDC_SUBSCRIBE
- DBMS_EXPFIL
- DBMS_OBFUSCATION_TOOLKIT
- DBMS_RLMGR
- SDO_NET_MEM

Prise en charge des fonctions Oracle Database

Amazon RDS Oracle prend en charge la plupart des fonctionnalités et fonctions d'Oracle Database. Certaines fonctions peuvent avoir une prise en charge limitée ou des privilèges restreints. Certaines fonctions sont disponibles uniquement dans Enterprise Edition et certaines fonctions nécessitent des licences supplémentaires. Pour plus d'informations sur les fonctions Oracle Database pour des versions d'Oracle Database spécifiques, consultez le document Oracle Database Licensing Information User Manual pour la version que vous utilisez.

> **Note**
>
> Ces listes ne sont pas complètes.

Amazon RDS Oracle prend en charge les fonctions Oracle Database suivantes :

- Advanced Compression
- Application Express (APEX)

  Pour plus d'informations, consultez Oracle Application Express (APEX) (p. 1026).
- Automatic Memory Management
- Automatic Undo Management
- Automatic Workload Repository (AWR)

Pour plus d'informations, consultez Génération de rapports de performance avec AWR (Automatic Workload Repository) (p. 1119).

- Active Data Guard avec des performances maximales dans la même région AWS ou dans plusieurs régions AWS

  Pour plus d'informations, consultez Utilisation des réplicas Oracle pour Amazon RDS (p. 1003).
- Continuous Query Notification (version 12.1.0.2.v7 et versions ultérieures)

  Pour de plus amples informations, veuillez consulter Using Continuous Query Notification (CQN) dans la documentation Oracle.
- Data Redaction
- Database Change Notification (version 11.2.0.4.v11 et versions 11g ultérieures)

  Pour de plus amples informations, veuillez consulter Database Change Notification dans la documentation Oracle.

  > **Note**
  >
  > Cette fonction est remplacée par la fonction Continuous Query Notification dans la version 12.1 et les versions ultérieures.
- Database In-Memory (version 12.1 ou ultérieure)
- Transactions et requêtes distribuées
- Redéfinition basée sur l'édition

  Pour plus d'informations, consultez Définition de l'édition par défaut d'une instance de base de données (p. 1123).
- Enterprise Manager Database Control (11g) et EM Express (12c)

  Pour plus d'informations, consultez Oracle Enterprise Manager (p. 1037).
- Fine-Grained Auditing
- Flashback Table, Flashback Query, Flashback Transaction Query
- Import/export (existant et Data Pump) et SQL*Loader

  Pour plus d'informations, consultez Importation de données dans Oracle sur Amazon RDS (p. 990).
- Java Virtual Machine (JVM)

  Pour plus d'informations, consultez Oracle Java Virtual Machine (p. 1052).
- Label Security (version 12.1 ou ultérieure)

  Pour plus d'informations, consultez Oracle Label Security (p. 1054).
- Locator

  Pour plus d'informations, consultez Oracle Locator (p. 1057).
- Vues matérialisées
- Multimédia

  Pour plus d'informations, consultez Oracle Multimedia (p. 1060).
- Chiffrement de réseau

  Pour plus d'informations, consultez Oracle NNE (Native Network Encryption) (p. 1062) et Oracle Secure Sockets Layer (SSL) (p. 1068).
- Partitioning

- Spatial et Graph

  Pour plus d'informations, consultez Oracle Spatial (p. 1077).
- Star Query Optimization
- Streams et Advanced Queuing
- Summary Management – Materialized View Query Rewrite
- Text (les magasins de données de type fichier et URL ne sont pas pris en charge)
- Total Recall
- Transparent Data Encryption (TDE) (Chiffrement transparent des données)

  Pour plus d'informations, consultez Oracle Transparent Data Encryption (p. 1091).
- Audit unifié, mode mixte (version 12.1 ou ultérieure)

  Pour plus d'informations, consultez Mixed Mode Auditing dans la documentation Oracle.
- XML DB (sans XML DB Protocol Server)

  Pour plus d'informations, consultez Oracle XML DB (p. 1096).
- Virtual Private Database

Amazon RDS Oracle ne prend pas en charge les fonctions Oracle Database suivantes :

- Automatic Storage Management (ASM)
- Database Vault
- Flashback Database
- Multitenant
- Oracle Enterprise Manager Cloud Control Management Repository
- Real Application Clusters (Oracle RAC)
- Real Application Testing
- Audit unifié, Pure Mode
- Schéma Workspace Manager (WMSYS)

> **Warning**
>
> En général, Amazon RDS ne vous empêche pas de créer des schémas pour des fonctions non prises en charge. Toutefois, si vous créez des schémas pour des fonctions et des composants Oracle nécessitant des privilèges SYS, vous pouvez endommager le dictionnaire de données et affecter la disponibilité de votre instance. Utilisez uniquement les fonctions et schémas pris en charge et disponibles dans Options propres aux instances de bases de données Oracle (p. 1013).

Prise en charge des paramètres Oracle Database

Dans Amazon RDS, vous gérez les paramètres à l'aide de groupes de paramètres. Pour plus d'informations, consultez Utilisation de groupes de paramètres de base de données (p. 225). Pour afficher les paramètres pris en charge pour une édition et une version spécifiques d'Oracle, exécutez la commande `describe-engine-default-parameters` de l'AWS CLI.

Par exemple, pour afficher les paramètres pris en charge pour Oracle Enterprise Edition version 12.2, exécutez la commande suivante.

```
aws rds describe-engine-default-parameters --db-parameter-group-family oracle-ee-12.2
```

Gestion des versions du moteur Oracle

La gestion de version de moteur de base de données vous permet de contrôler quand et comment le logiciel du moteur de base de données exécutant vos instances de bases de données est corrigé et mis à niveau. Avec cette fonction, vous bénéficiez de la flexibilité nécessaire pour maintenir la compatibilité avec les versions de correctifs du moteur de base de données. Vous pouvez également tester de nouvelles versions de correctifs pour vous assurer qu'elles fonctionnent efficacement avec votre application avant de les déployer en production. En outre, vous pouvez effectuer des mises à niveau de version selon vos propres conditions et échéances.

> Note
>
> Amazon RDS agrège régulièrement des correctifs de base de données Oracle officiels en utilisant une version de moteur de base de données propre à Amazon RDS. Pour obtenir une liste des correctifs Oracle inclus dans une version de moteur propre à Amazon RDS Oracle, consultez Notes de mise à jour pour le moteur de base de données Oracle (p. 1208).

Si vous activez les mises à niveau automatiques de version mineure sur votre instance de base de données, celles-ci se déclenchent automatiquement. Vous devez effectuer les mises à niveau majeures manuellement, à l'exception de la mise à niveau automatique de 11.2.0.4. Pour plus d'informations sur la mise à niveau d'une instance de base de données Oracle, consultez Mise à niveau du moteur de base de données Oracle (p. 975).

Obsolescence d'Oracle 11.2.0.4

Oracle Corporation a l'intention de rendre obsolète la prise en charge de la version 11.2.0.4 Oracle Database le 31 décembre 2020. Le 31 octobre 2020, Amazon RDS prévoit de rendre obsolète la prise en charge d'Oracle version 11.2.0.4 SE1 avec le modèle Licence Inclus. Le 31 décembre 2020, Amazon RDS prévoit de rendre obsolète la prise en charge de la version 11.2.0.4 sur toutes les éditions utilisant le modèle Bring Your Own License (BYOL).

Amazon RDS prévoit de rendre obsolète la prise en charge d'Oracle version 11.2.0.4 selon la planification suivante, qui inclut des recommandations de mise à niveau. Pour de plus amples informations, veuillez consulter Préparation de la mise à niveau automatique d'Oracle 11g SE1 (p. 982).

Action ou recommandation	11.2.0.4 sur SE1 avec licence incluse	11.2.0.4 sur EE, SE et SE1 avec BYOL
Nous vous recommandons de mettre à jour manuellement les instances de base de données 11.2.0.4 vers la version de votre choix.	Maintenant – 31 octobre 2020	Maintenant – 31 décembre 2020
Nous vous recommandons de mettre à jour manuellement les instantanés 11.2.0.4 vers la version de votre choix.	1 septembre 2020	1er octobre 2020
Vous ne pouvez plus créer de nouvelles instances avec Amazon RDS pour Oracle avec la version répertoriée.	1 septembre 2020	1er octobre 2020

Action ou recommandation	11.2.0.4 sur SE1 avec licence incluse	11.2.0.4 sur EE, SE et SE1 avec BYOL
Amazon RDS pour Oracle démarre automatiquement les mises à niveau de vos instances de base de données vers la version 19c.	1er novembre 2020	1er janvier 2021
Amazon RDS pour Oracle démarre les mises à niveau automatiques vers la version 19c pour toutes les instances de base de données restaurées à partir d'instantanés.	1er novembre 2020	1er janvier 2021

Utilisation de HugePages avec une instance de base de données Oracle

Amazon RDS pour Oracle prend en charge la fonctionnalité HugePages du noyau Linux pour obtenir une base de données plus évolutive. L'utilisation de HugePages se traduit par des tables de page réduites et une réduction du temps UC de gestion de la mémoire, ce qui augmente les performances des instances de bases de données volumineuses. Pour plus d'informations, consultez Overview of HugePages (Présentation des grandes pages) dans la documentation Oracle.

Vous pouvez utiliser HugePages avec les versions et éditions Oracle suivantes :

- 19.0.0.0, toutes les éditions
- 18.0.0.0, toutes les éditions
- 12.2.0.1, toutes les éditions
- 12.1.0.2, toutes les éditions
- 11.2.0.4, toutes les éditions

Le paramètre `use_large_pages` contrôle si HugePages est activé pour une instance de base de données. Les valeurs possibles pour ce paramètre sont `ONLY`, `FALSE` et `{DBInstanceClassHugePagesDefault}`. Le paramètre `use_large_pages` est défini sur `{DBInstanceClassHugePagesDefault}` dans le groupe de paramètres DB par défaut pour Oracle.

Pour contrôler si HugePages est activé automatiquement pour une instance de base de données, vous pouvez utiliser la variable de formule `DBInstanceClassHugePagesDefault` dans les groupes de paramètres. La valeur est déterminée comme suit :

- Pour les classes d'instance de base de données indiquées dans le tableau suivant, `DBInstanceClassHugePagesDefault` a toujours la valeur `FALSE` par défaut, et `use_large_pages` a la valeur `FALSE`. Vous pouvez activer HugePages manuellement pour ces instances de base de données si la classe d'instance de bases de données dispose d'au moins 14 Gio de mémoire.
- Pour les classes d'instance de base de données non mentionnées dans le tableau suivant, si la classe d'instance de base de données possède au moins 14 Gio de mémoire, `DBInstanceClassHugePagesDefault` a toujours la valeur `FALSE`. En outre, `use_large_pages` a la valeur `FALSE`.
- Pour les classes d'instance de base de données non mentionnées dans le tableau suivant, si la classe d'instance possède au moins 14 Gio de mémoire et moins de 100 Gio de mémoire, `DBInstanceClassHugePagesDefault` a la valeur `TRUE` par défaut. En outre, `use_large_pages` a

la valeur `ONLY`. Vous pouvez désactiver HugePages manuellement en définissant `use_large_pages` sur `FALSE`.

- Pour les classes d'instance de base de données non mentionnées dans le tableau suivant, si la classe d'instance possède au moins 100 Gio de mémoire, `DBInstanceClassHugePagesDefault` a toujours la valeur `TRUE`. En outre, `use_large_pages` a la valeur `ONLY` et HugePages ne peut pas être désactivé.

HugePages n'est pas activé par défaut pour les classes d'instance de base de données suivantes.

Famille de classes d'instance de base de données	Classes d'instance de base de données avec HugePages non activé par défaut
db.m5	db.m5.large
db.m4	db.m4.large, db.m4.xlarge, db.m4.2xlarge, db.m4.4xlarge, db.m4.10xlarge
db.m3	db.m3.medium, db.m3.large, db.m3.xlarge, db.m3.2xlarge
db.r3	db.r3.large, db.r3.xlarge, db.r3.2xlarge, db.r3.4xlarge, db.r3.8xlarge
db.t3	db.t3.micro, db.t3.small, db.t3.medium, db.t3.large
db.t2	db.t2.micro, db.t2.small, db.t2.medium, db.t2.large

Pour plus d'informations sur les classes d'instance DB, consultez Spécifications matérielles pour les classes d'instance de base de données (p. 25).

Pour activer manuellement HugePages pour des instances de bases de données nouvelles ou existantes, définissez le paramètre `use_large_pages` sur `ONLY`. Vous ne pouvez pas utiliser HugePages avec Oracle Automatic Memory Management (AMM). Si vous définissez le paramètre `use_large_pages` sur `ONLY`, vous devez aussi définir `memory_target` et `memory_max_target` sur `0`. Pour plus d'informations sur la définition des paramètres de votre instance de base de données, consultez Utilisation de groupes de paramètres de base de données (p. 225).

Vous pouvez aussi définir les paramètres `sga_target`, `sga_max_size` et `pga_aggregate_target`. Lorsque vous définissez les paramètres de mémoire des zones SGA (System Global Area) et PGA (Program Global Area), ajoutez les valeurs ensemble. Soustrayez ce total de votre mémoire d'instance disponible (`DBInstanceClassMemory`) pour déterminer l'espace mémoire libre restant au-delà de l'attribution par HugePages. Vous devez conserver une mémoire libre d'au moins 2 Gio ou égale à 10 pourcent de la mémoire totale disponible de l'instance, la plus petite des deux valeurs étant retenue.

Après avoir configuré vos paramètres, vous devez redémarrer votre instance de base de données pour que les modifications soient effectives. Pour plus d'informations, consultez Redémarrage d'une instance de base de données (p. 272).

> **Note**
>
> L'instance de base de données Oracle diffère les modifications apportées aux paramètres d'initialisation liés à la SGA jusqu'à ce que vous redémarriez l'instance sans basculement. Dans la console Amazon RDS, choisissez Redémarrer, mais ne choisissez pas Redémarrer avec basculement. Dans l'AWS CLI, appelez la commande `reboot-db-instance` avec le paramètre `--no-force-failover`. L'instance de base de données ne traite pas les paramètres liés à la SGA pendant le basculement ou lors d'autres opérations de maintenance qui provoquent le redémarrage de l'instance.

Voici un exemple de configuration de paramètres pour HugePages activant manuellement HugePages. Vous devez définir les valeurs qui répondent à vos besoins.

```
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
```

Supposons que les valeurs des paramètres suivantes sont définies dans un groupe de paramètres.

```
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}
```

Le groupe de paramètres est utilisé par une classe d'instance db.r4 avec 100 Gio de mémoire au maximum et une instance db.r3 avec plus de 100 Gio de mémoire. Avec ces valeurs de paramètres et le paramètre `use_large_pages` défini sur `{DBInstanceClassHugePagesDefault}`, HugePages est activé sur l'instance db.r4 mais désactivé sur l'instance db.r3.

Supposons que les valeurs des paramètres suivantes sont définies dans un groupe de paramètres.

```
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
```

Le groupe de paramètres est utilisé par une classe d'instance de base de données db.r4 et une classe d'instance de base de données db.r5, toutes deux avec plus de 100 Gio de mémoire. Le groupe de paramètres est également utilisé par une instance db.r3 avec plus de 100 Gio de mémoire. Avec ces valeurs de paramètres, HugePages est désactivé sur les instances db.r4, db.r5 et db.r3.

> **Note**
>
> Si ce groupe de paramètres est utilisé par une classe d'instance de base de données db.r4 ou db.r5 avec au moins 100 Gio de mémoire, la valeur de `FALSE` pour `use_large_pages` est remplacée et définie sur `ONLY`. Dans ce cas, une notification concernant le remplacement est envoyée au client.

Lorsque HugePages est activé sur votre instance de base de données, vous pouvez afficher les informations sur HugePages en activant la surveillance améliorée. Pour plus d'informations, consultez Surveillance améliorée (p. 394).

Utilisation de utl_http, utl_tcp et utl_smtp avec une instance de base de données Oracle

Amazon RDS prend en charge l'accès réseau sortant sur vos instances de bases de données exécutant Oracle. Vous pouvez utiliser `utl_http`, `utl_tcp` et `utl_smtp` pour vous connecter au réseau à partir de votre instance de base de données.

Notez les éléments suivants sur l'utilisation de l'accès réseau sortant :

- Pour utiliser `utl_http` sur des instances de bases de données exécutant Oracle 11g, vous devez installer l'option XMLDB. Pour plus d'informations, consultez Oracle XML DB (p. 1096).
- L'accès réseau sortant avec `utl_http`, `utl_tcp` et `utl_smtp` est pris en charge uniquement pour les instances de bases de données Oracle dans un VPC. Pour déterminer si votre instance de base de données est dans un VPC ou non, consultez Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611). Pour placer dans un VPC une instance de base de données qui ne se trouve pas dans un VPC, consultez Déplacement vers un VPC d'une instance de base de données n'appartenant pas à un VPC (p. 1627).
- Pour utiliser SMTP avec l'option UTL_MAIL, consultez Oracle UTL_MAIL (p. 1093).
- Le nom DNS (Domain Name Server) de l'hôte distant doit avoir l'une des caractéristiques suivantes :
  - être publiquement résolu ;
  - être le point de terminaison d'une instance de base de données Amazon RDS ;
  - pouvant être résolu via un serveur DNS personnalisé. Pour plus d'informations, consultez Configuration d'un serveur DNS personnalisé (p. 1114).
  - être le nom DNS privé d'une instance Amazon EC2 dans le même VPC ou un VPC appairé. Dans ce cas, assurez-vous que le nom peut être résolu via un serveur DNS personnalisé. De même, pour utiliser le DNS fourni par Amazon, vous pouvez activer l'attribut `enableDnsSupport` dans les paramètres VPC et activer la prise en charge de la résolution DNS pour la connexion d'appairage de VPC. Pour plus d'informations, consultez Prise en charge du DNS dans votre VPC et Modification de votre connexion d'appairage de VPC.

Pour vous connecter en toute sécurité à des ressources SSL/TLS distantes, vous pouvez créer et charger des portefeuilles Oracle personnalisés. En utilisant l'intégration de Amazon S3 à la fonction Amazon RDS pour Oracle, vous pouvez télécharger un portefeuille depuis Amazon S3 vers des instances de base de données Oracle. Pour plus d'informations sur l'intégration de Amazon S3 pour Oracle, consultez Intégration Amazon S3 (p. 1014).

L'exemple suivant crée un portefeuille pour l'accès à https://status.aws.amazon.com/robots.txt via `utl_http`.

1. Obtenez le certificat pour `Amazon Root CA 1` depuis le Référentiel des services d'approbation Amazon.
2. Créez un nouveau portefeuille et ajoutez le certificat suivant :

```
orapki wallet create -wallet . -auto_login_only
orapki wallet add -wallet . -trusted_cert -cert AmazonRootCA1.pem -auto_login_only
orapki wallet display -wallet .
```

3. Chargez le portefeuille dans votre compartiment Amazon S3.
4. Respectez les conditions préalables de l'intégration de Amazon S3 à Oracle et ajoutez l'option `S3_INTEGRATION` à votre instance de base de données Oracle. Assurez-vous que le rôle IAM pour l'option a accès au compartiment Amazon S3 que vous utilisez.

   Pour plus d'informations, consultez Intégration Amazon S3 (p. 1014).

5. Connectez-vous à l'instance de base de données et créez un répertoire dans la base de données pour stocker le portefeuille. L'exemple suivant crée un répertoire nommé `SSL_WALLET`.

```
exec rdsadmin.rdsadmin_util.create_directory('SSL_WALLET');
```

6. Téléchargez le portefeuille depuis votre compartiment Amazon S3 vers l'instance de base de données Oracle.

   L'exemple suivant télécharge un portefeuille vers le répertoire de l'instance de base de données `SSL_WALLET` :

```
SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3(
      p_bucket_name    =>  'bucket_name',
      p_s3_prefix      =>  'wallet_name',
      p_directory_name =>  'SSL_WALLET')
   AS TASK_ID FROM DUAL;
```

   Remplacez *`bucket_name`* par le nom du compartiment que vous utilisez et *`wallet_name`* par le nom du portefeuille.

7. Définissez ce portefeuille pour les transactions `utl_http` en exécutant la procédure suivante :

```
DECLARE
 l_wallet_path all_directories.directory_path%type;
BEGIN
 select directory_path into l_wallet_path from all_directories
 where upper(directory_name)='SSL_WALLET';

  utl_http.set_wallet('file:/' || l_wallet_path);
END;
```

8. Accédez à l'URL ci-dessus via SSL/TLS.

```
SELECT utl_http.request('https://status.aws.amazon.com/robots.txt') AS ROBOTS_TXT FROM
 DUAL;

ROBOTS_TXT
--------------------------------------------------------------------------------
User-agent: *
Allow: /
```

   Note

   Les certificats spécifiques requis pour votre portefeuille varient par service. Pour les services AWS, vous trouverez généralement les certificats dans le Référentiel des services d'approbation Amazon.

Vous pouvez utiliser une configuration similaire pour envoyer des e-mails via UTL_SMTP sur SSL/TLS (notamment Amazon Simple Email Service).

Vous pouvez établir des liens de base de données entre des instances de base de données Oracle via un point de terminaison SSL/TLS si l'option Oracle SSL est configurée pour chaque instance. Aucune autre configuration n'est requise. Pour plus d'informations, consultez Oracle Secure Sockets Layer (SSL) (p. 1068).

Utilisation d'OEM, d'APEX, de TDE et d'autres options

La plupart des moteurs de base de données Amazon RDS prennent en charge des groupes d'options qui vous permettent de sélectionner des fonctions supplémentaires pour votre instance de base de données. Les instances de bases de données Oracle prennent en charge plusieurs options, notamment Oracle Enterprise Manager (OEM), Transparent Data Encryption (TDE), Application Express (APEX) et Native Network Encryption. Pour obtenir une liste complète des options Oracle prises en charge, consultez Options propres aux instances de bases de données Oracle (p. 1013). Pour plus d'informations sur l'utilisation de groupes d'options, consultez Utilisation de groupes d'options (p. 209).

Utilisation des types de données étendus

La version Amazon RDS Oracle 12c prend en charge les types de données étendus. Avec les types de données étendus, la taille maximum est de 32 767 octets pour les types de données VARCHAR2, NVARCHAR2 et RAW. Pour utiliser les types de données étendus, définissez le paramètre `MAX_STRING_SIZE` sur `EXTENDED`. Pour plus d'informations, consultez Extended Data Types dans la documentation Oracle.

Si vous ne souhaitez pas utiliser les types de données étendus, gardez le paramètre `MAX_STRING_SIZE` défini sur `STANDARD` (par défaut). Lorsque ce paramètre est défini sur `STANDARD`, les limites de taille sont 4 000 octets pour les types de données VARCHAR2 et NVARCHAR2, et 2 000 octets pour le type de données RAW.

Vous pouvez activer les types de données étendus sur une nouvelle instance de base de données ou sur une instance de base de données existante. Pour les nouvelles instances de base de données, la durée nécessaire pour créer une instance de base de données est généralement plus longue lorsque vous activez les types de données étendus. Pour les instances de base de données existantes, l'instance de base de données n'est pas disponible pendant le processus de conversion.

Voici les considérations relatives à une instance de base de données pour laquelle les types de données étendus sont activés :

- Lorsque vous activez les types de données étendus pour une instance de base de données, vous ne pouvez pas à nouveau modifier l'instance de base de données afin qu'elle utilise la taille standard pour les types de données. Après la conversion d'une instance afin qu'elle utilise les types de données étendus, si vous redéfinissez le paramètre `MAX_STRING_SIZE` sur `STANDARD` le statut devient `incompatible-parameters`.
- Lorsque vous restaurez une instance de base de données qui utilise des types de données étendus, vous devez spécifier un groupe de paramètres avec le paramètre `MAX_STRING_SIZE` défini sur `EXTENDED`. Pendant la restauration, si vous spécifiez le groupe de paramètres par défaut ou tout autre groupe de paramètres avec le paramètre `MAX_STRING_SIZE` défini sur `STANDARD` le statut devient `incompatible-parameters`.
- Nous vous conseillons de ne pas activer les types de données étendus pour les instances de base de données Oracle qui s'exécutent sur la classe d'instance de base de données t2.micro.

Lorsque l'état de l'instance de base de données est `incompatible-parameters` à cause du paramètre `MAX_STRING_SIZE`, l'instance de base de données reste indisponible jusqu'à ce que le paramètre `MAX_STRING_SIZE` soit défini sur `EXTENDED` et que l'instance de base de données soit redémarrée.

Activation des types de données étendus pour une nouvelle instance de base de données

Pour activer les types de données étendus pour une nouvelle instance de base de données

1. Définissez le paramètre `MAX_STRING_SIZE` sur `EXTENDED` dans un groupe de paramètres.

   Pour définir le paramètre, vous pouvez créer un groupe de paramètres de base de données ou modifier un groupe de paramètres existant.

   Pour plus d'informations, consultez Utilisation de groupes de paramètres de base de données (p. 225).
2. Créez une nouvelle instance de base de données Amazon RDS Oracle et associez le groupe de paramètres avec le paramètre `MAX_STRING_SIZE` défini sur `EXTENDED` avec l'instance de base de données.

   Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).

Activation des types de données étendus pour une instance de base de données existante

Lorsque vous modifiez une instance de base de données afin d'activer les types de données étendus, les données de la base de données sont converties afin d'utiliser les tailles étendues. L'instance de base de données n'est pas disponible pendant la conversion. La durée nécessaire pour convertir les données dépend de la classe d'instance de base de données utilisée par l'instance de base de données et de la taille de la base de données.

> Note
>
> Une fois que vous avez activé les types de données étendus, vous pouvez effectuer une opération de restauration à un moment donné pendant la conversion. Vous pouvez restaurer au moment précédant immédiatement la conversion ou au moment suivant immédiatement la conversion.

Pour activer les types de données étendus pour une instance de base de données existante

1. Créez un instantané de la base de données.

   S'il existe des objets no valides dans la base de données, Amazon RDS tente de les recompiler. La conversion en vue d'activer les types de données étendus peut échouer si Amazon RDS ne peut pas recompiler un objet non valide. L'instantané vous permet de restaurer la base de données en cas de problème avec la conversion. Vérifiez toujours la présence d'objets non valides avant la conversion afin d'y apporter une solution ou de les supprimer. Pour les bases de données de production, nous vous conseillons d'abord de tester le processus de conversion sur une copie de votre instance de base de données.

   Pour plus d'informations, consultez Création d'un instantané de base de données (p. 327).
2. Définissez le paramètre `MAX_STRING_SIZE` sur `EXTENDED` dans un groupe de paramètres.

   Pour définir le paramètre, vous pouvez créer un groupe de paramètres de base de données ou modifier un groupe de paramètres existant.

   Pour plus d'informations, consultez Utilisation de groupes de paramètres de base de données (p. 225).
3. Modifiez l'instance de base de données afin de l'associer au groupe de paramètres avec le paramètre `MAX_STRING_SIZE` défini sur `EXTENDED`.

Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

4. Redémarrez l'instance de base de données pour que la modification des paramètres prenne effet.

   Pour plus d'informations, consultez Redémarrage d'une instance de base de données (p. 272).

Synonymes publics

Vous pouvez créer des synonymes publics référençant des objets dans vos propres schémas. Ne créez ou ne modifiez pas des synonymes publics pour les schémas gérés par Oracle, notamment `SYS`, `SYSTEM` et `RDSADMIN`. Cela peut entraîner l'invalidation de composants de base de données de base et affecter la disponibilité de votre instance de base de données.

Connexion à une instance de base de données Oracle

Une fois qu'Amazon RDS a provisionné votre instance de base de données Oracle, vous pouvez utiliser n'importe quelle application cliente SQL standard pour vous connecter à l'instance de base de données. Dans cette rubrique, vous vous connectez à une instance de base de données exécutant le moteur de base de données Oracle avec Oracle SQL Developer ou SQL*Plus.

Pour obtenir un exemple qui vous explique le processus de création et de connexion à un exemple d'instance de base de données, consultez Création d'une instance de base de données Oracle et connexion à une base de données sur une instance de base de données Oracle (p. 93).

Recherche du point de terminaison de votre instance de base de données

Chaque instance de base de données Amazon RDS possède un point de terminaison. Chaque point de terminaison possède le nom DNS et le numéro de port de l'instance de base de données. Pour connecter votre instance de base de données à l'aide d'une application cliente SQL, vous avez besoin du nom DNS et du numéro de port de votre instance de base de données.

Vous pouvez trouver le point de terminaison d'une instance de base de données à l'aide de la console Amazon RDS ou de l'AWS CLI.

> Note
>
> Si vous utilisez l'authentification Kerberos, veuillez consulter Connexion à Oracle avec l'authentification Kerberos (p. 1181).

Console

Pour rechercher le point de terminaison à l'aide de la console

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le coin supérieur droit de la console, choisissez la région AWS de votre instance de base de données.

3. Trouvez le numéro de port et le nom DNS pour votre instance de base de données.
   a. Choisissez Bases de données pour afficher une liste de vos instances de bases de données.
   b. Choisissez le nom de l'instance de base de données Oracle pour afficher les détails de l'instance.
   c. Dans l'onglet Connectivity & security (Connectivité et sécurité), copiez le point de terminaison. Notez également le numéro du port. Vous avez besoin du point de terminaison et du numéro de port pour vous connecter à l'instance de base de données.

AWS CLI

Pour trouver le point de terminaison d'une instance de base de données Oracle à l'aide de l'AWS CLI, appelez la commande describe-db-instances.

Example Pour rechercher le point de terminaison à l'aide de l'AWS CLI

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

Recherchez `Endpoint` dans la sortie pour trouver le nom DNS et le numéro de port de votre instance de base de données. La ligne `Address` de la sortie contient le nom DNS. Voici un exemple de sortie de point de terminaison JSON.

```
"Endpoint": {
    "HostedZoneId": "Z1PVIF0B656C1W",
    "Port": 3306,
    "Address": "myinstance.123456789012.us-west-2.rds.amazonaws.com"
},
```

> **Note**
>
> La sortie peut contenir des informations pour plusieurs instances de bases de données.

Connexion à votre instance de base de données à l'aide d'Oracle SQL Developer

Dans cette procédure, vous vous connectez à votre instance de base de données à l'aide d'Oracle SQL Developer. Pour télécharger une version autonome de cet utilitaire, consultez la page Oracle SQL Developer Downloads.

Pour vous connecter à votre instance de base de données, vous avez besoin de son nom DNS et de son numéro de port. Pour plus d'informations sur la recherche du nom DNS et du numéro de port d'une instance de base de données, consultez Recherche du point de terminaison de votre instance de base de données (p. 961).

Pour vous connecter à une instance de base de données à l'aide de SQL Developer

1. Démarrez Oracle SQL Developer.
2. Sous l'onglet Connexions, sélectionnez l'icône ajouter (+).

3. Dans la boîte de dialogue Nouvelle connexion de base de données/Sélectionner une connexion de base de données, entrez les informations relatives à votre instance de base de données :

   - Pour Nom de connexion, saisissez un nom qui décrit la connexion, tel que `Oracle-RDS`.
   - Pour Nom d'utilisateur, saisissez le nom de l'administrateur de base de données pour l'instance de base de données.
   - Pour Mot de passe, saisissez le mot de passe de l'administrateur de base de données.
   - Pour Nom d'hôte, saisissez le nom DNS de l'instance de base de données.
   - Pour Port, saisissez le numéro de port.
   - Pour SID, saisissez le SID de la base de données Oracle.

   La boîte de dialogue dûment remplie doit se présenter comme suit :

4. Choisissez Connexion.
5. Vous pouvez maintenant commencer à créer vos propres bases de données et à exécuter des requêtes sur votre instance de base de données et vos bases de données comme d'habitude. Pour exécuter une requête de test sur votre instance de base de données, procédez comme suit :

   a. Dans l'onglet Feuille de calcul de votre connexion, saisissez la requête SQL suivante.

   ```
   SELECT NAME FROM V$DATABASE;
   ```

   b. Choisissez l'icône exécuter pour exécuter la requête.

   SQL Developer renvoie le nom de la base de données.

Connexion à votre instance de base de données à l'aide de SQL*Plus

Vous pouvez utiliser un utilitaire comme SQL*Plus pour vous connecter à une instance de base de données Amazon RDS exécutant Oracle. Pour télécharger une version autonome de SQL*Plus, consultez SQL*Plus User's Guide and Reference (Guide et référence de l'utilisateur SQL*Plus).

Pour vous connecter à votre instance de base de données, vous avez besoin de son nom DNS et de son numéro de port. Pour plus d'informations sur la recherche du nom DNS et du numéro de port d'une instance de base de données, consultez Recherche du point de terminaison de votre instance de base de données (p. 961).

Example Pour se connecter à une instance de base de données Oracle à l'aide de SQL*Plus

Dans les exemples suivants, remplacez le nom d'utilisateur de l'administrateur de votre instance de base de données. Remplacez également le nom DNS de votre instance de base de données, puis incluez le numéro de port et le SID Oracle. La valeur SID est le nom de la base de données de l'instance de base de données que vous avez spécifié lors de la création de l'instance de base de données, pas le nom de l'instance de base de données.

Pour Linux, macOS ou Unix :

```
sqlplus 'user_name@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=dns_name)(PORT=port))
(CONNECT_DATA=(SID=database_name)))'
```

Pour Windows :

```
sqlplus user_name@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=dns_name)(PORT=port))
(CONNECT_DATA=(SID=database_name)))
```

Vous devez visualiser des résultats similaires à ce qui suit.

```
SQL*Plus: Release 12.1.0.2.0 Production on Mon Aug 21 09:42:20 2017
```

Une fois que vous avez saisi le mot de passe de l'utilisateur, l'invite SQL apparaît.

```
SQL>
```

> **Note**
>
> La chaîne de connexion de format court (Easy connect ou EZCONNECT), comme `sqlplus USER/PASSWORD@LONGER-THAN-63-CHARS-RDS-ENDPOINT-HERE:1521/DATABASE_IDENTIFIER`, peut comporter une limite de caractères maximale et ne doit pas être utilisée pour se connecter.

Considérations relatives aux groupes de sécurité

Pour vous connecter à votre instance de base de données, celle-ci doit être associée à un groupe de sécurité contenant l'adresse IP et la configuration réseau que vous utilisez pour accéder à l'instance de base de données. Vous avez peut-être associé votre instance de base de données à un groupe de sécurité approprié lorsque vous l'avez créée. Si vous assignez un groupe de sécurité non configuré par défaut lors de la création de l'instance de base de données, le pare-feu de l'instance de base de données empêche les connexions.

Si vous avez besoin de créer un nouveau groupe de sécurité pour permettre l'accès, le type de groupe de sécurité que vous créez dépend de la plateforme Amazon EC2 sur laquelle se trouve votre instance de base de données. Pour déterminer votre plateforme, consultez Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611). En général, si votre instance de base de données se situe sur la plateforme EC2-Classic, créez un groupe de sécurité de base de données ; si votre instance de base de données se situe sur la plateforme VPC, vous devez créer un groupe de sécurité VPC. Pour obtenir des informations sur la création d'un groupe de sécurité, consultez Contrôle d'accès par groupe de sécurité (p. 1590).

Une fois le groupe de sécurité créé, vous devez modifier votre instance de base de données pour l'associer au groupe de sécurité. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Vous pouvez améliorer la sécurité en utilisant SSL pour chiffrer les connexions à votre instance de base de données. Pour plus d'informations, consultez Oracle Secure Sockets Layer (SSL) (p. 1068).

Processus serveur dédiés et partagés

Le serveur traite les connexions utilisateur à une instance de base de données Oracle. Par défaut, l'instance de base de données Oracle utilise des processus serveur dédiés. Avec des processus serveur dédiés, chaque processus serveur ne traite qu'un seul processus utilisateur. Le cas échéant, vous pouvez configurer des processus serveur partagés. Avec des processus serveur partagés, chaque processus serveur peut traiter plusieurs processus utilisateur.

Vous pouvez envisager d'utiliser des processus serveur partagés quand un nombre élevé de sessions utilisateur consomment trop de mémoire sur le serveur. Vous pouvez également envisager d'utiliser des processus serveur partagés quand les sessions se connectent et déconnectent très souvent, ce qui entraîne un problème de performance. L'utilisation de processus serveur partagés présente également des inconvénients. Par exemple, elles peuvent peser sur les ressources d'UC et elles sont plus compliquées à configurer et administrer.

Pour plus d'informations sur les processus serveur dédiés et partagés, consultez About Dedicated and Shared Server Processes (Informations relatives aux processus de serveur dédiés et partagés) dans la documentation Oracle. Pour plus d'informations sur la configuration des processus serveur partagés sur une instance de base de données Amazon RDS Oracle, consultez How do I configure Amazon RDS for Oracle Database to work with shared servers ? (Comment configurer Amazon RDS pour Oracle Database afin d'utiliser des serveurs partagés ?) dans le Knowledge Center (Centre de connaissances).

Résolution des problèmes de connexion à votre instance de base de données Oracle

Les problèmes suivants peuvent survenir lors d'une tentative de connexion à votre instance de base de données Oracle.

Problème	Suggestions de dépannage
Impossible de se connecter à votre instance de base de données.	Pour une instance de base de données récemment créée, l'état de l'instance de base de données est creating (création) jusqu'à ce qu'elle soit prête à l'emploi. Lorsque l'état devient available (disponible), vous pouvez vous connecter à l'instance de base de données. En fonction de la classe d'instance de base de données et de la quantité de stockage, la mise à disposition de la nouvelle instance de base de données peut prendre jusqu'à 20 minutes.
Impossible de se connecter à votre instance de base de données.	Si vous ne pouvez pas envoyer ou recevoir de communications sur le port que vous avez spécifié lors de la création de l'instance de base de données, vous ne pourrez pas vous connecter à l'instance de base de données. Vérifiez auprès de votre administrateur réseau si l'utilisation du port que vous avez spécifié pour votre instance de base de données autorise les communications entrantes et sortantes.
Impossible de se connecter à votre instance de base de données.	Les règles d'accès appliquées par votre pare-feu local et les adresses IP que vous avez autorisées à accéder à votre instance de base de données dans le groupe de sécurité de l'instance de base de données peuvent ne pas correspondre. Le problème est probablement lié aux règles de sortie ou d'entrée sur votre pare-feu. Vous pouvez ajouter ou modifier une règle entrante dans le groupe de sécurité. Pour Source, choisissez Mon IP. Cela autorise à accéder à l'instance de base de données à partir de l'adresse IP détectée dans votre navigateur. Pour de plus amples informations, veuillez consulter VPC Amazon Virtual Private Cloud et Amazon RDS (p. 1610). Pour plus d'informations sur les groupes de sécurité, consultez Contrôle d'accès par groupe de sécurité (p. 1590). Pour passer en revue le processus de configuration de règles de votre groupe de sécurité, consultez Didacticiel : créer un Amazon VPC à utiliser avec une instance de base de données (p. 1629).

Problème	Suggestions de dépannage
Connexion échouée, car l'hôte ou l'objet cible n'existe pas – Oracle, Erreur : ORA-12545	Vérifiez que vous avez spécifié le nom du serveur et le numéro de port correctement. Pour Nom du serveur, saisissez le nom DNS de la console. Pour plus d'informations sur la recherche du nom DNS et du numéro de port d'une instance de base de données, consultez Recherche du point de terminaison de votre instance de base de données (p. 961).
Invalid username/password; logon denied – Oracle, Error: ORA-01017	Vous avez pu atteindre l'instance de base de données, mais la connexion a été refusée. Cela est souvent dû au fait que le nom d'utilisateur ou le mot de passe fournis sont incorrects. Vérifiez le nom d'utilisateur et le mot de passe, puis réessayez.

Pour de plus amples informations sur les problèmes de connexion, veuillez consulter Impossible de se connecter à l'instance de base de données Amazon RDS (p. 1639).

Mise à jour des applications pour se connecter aux instances de bases de données Oracle à l'aide des nouveaux certificats SSL/TLS

Le 19 septembre 2019, Amazon RDS a publié de nouveaux certificats de l'autorité de certification (CA) à connecter à vos instances de bases de données RDS à l'aide du protocole Secure Socket Layer ou Transport Layer Security (SSL/TLS). Vous trouverez ci-après des informations sur la mise à jour de vos applications afin d'utiliser les nouveaux certificats.

Cette rubrique peut vous aider à déterminer si des applications clientes utilisent un protocole SSL/TLS pour se connecter à vos instances de bases de données.

> **Important**
>
> Lorsque vous modifiez le certificat d'une instance de base de données Amazon RDS for Oracle, seul le processus d'écoute de base de données est redémarré. L'instance de base de données n'est pas redémarrée. Les connexions de base de données existantes ne sont pas affectées, mais les nouvelles connexions rencontrent des erreurs pendant une brève période au cours du redémarrage du processus d'écoute.

> **Note**
>
> Pour les applications clientes qui utilisent un protocole SSL/TLS pour se connecter à vos instances de bases de données, vous devez mettre à jour les magasins d'approbations de vos applications clientes qui incluent les nouveaux certificats de l'autorité de certification.

Une fois que vous avez mis à jour les certificats de l'autorité de certification dans les magasins d'approbations des applications clientes, vous pouvez soumettre les certificats de vos instances de bases de données à une rotation. Nous vous recommandons vivement de tester ces procédures dans un environnement de développement ou intermédiaire avant de les implémenter dans vos environnements de production.

Pour de plus amples informations sur la rotation de certificats, veuillez consulter Rotation de votre certificat SSL/TLS (p. 1527). Pour en savoir plus sur le téléchargement de certificats, consultez Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525). Pour de plus amples

informations sur l'utilisation des protocoles SSL/TLS avec les instances de bases de données Oracle, veuillez consulter Oracle Secure Sockets Layer (SSL) (p. 1068).

Rubriques

- Déterminer si les applications utilisent SSL pour votre instance de base de données (p. 970)
- Mise à jour du magasin d'approbations de votre application (p. 970)
- Exemple de code Java pour l'établissement de connexions SSL (p. 972)

Déterminer si les applications utilisent SSL pour votre instance de base de données

Si votre instance de base de données Oracle utilise un groupe d'options avec l'option `SSL` ajoutée, vous pouvez utiliser SSL. Procédez à la vérification en suivant les instructions dans Liste des options et des paramètres d'options pour un groupe d'options (p. 219). Pour plus d'informations sur l'option `SSL`, veuillez consulter Oracle Secure Sockets Layer (SSL) (p. 1068).

Vérifiez le journal d'écouteur afin de déterminer s'il existe des connexions SSL. Voici un exemple de sortie dans un journal d'écouteur.

```
date time * (CONNECT_DATA=(CID=(PROGRAM=program)
(HOST=host)(USER=user))(SID=sid)) *
(ADDRESS=(PROTOCOL=tcps)(HOST=host)(PORT=port)) * establish * ORCL * 0
```

Lorsque `PROTOCOL` possède la valeur `tcps` pour une entrée, il affiche une connexion SSL. Cependant, quand `HOST` est `127.0.0.1`, vous pouvez ignorer l'entrée. Les connexions provenant de `127.0.0.1` sont un agent de gestion locale sur l'instance de base de données. Il ne s'agit pas de connexions SSL externes. Par conséquent, vous avez des applications se connectant à l'aide d'un protocole SSL si vous voyez des entrées de journal d'écouteur pour lesquelles `PROTOCOL` est `tcps` et `HOST` n'est pas `127.0.0.1`.

Pour vérifier le journal d'écouteur, vous pouvez publier le journal dans Amazon CloudWatch Logs. Pour de plus amples informations, veuillez consulter Publication des journaux Oracle dans Amazon CloudWatch Logs (p. 518).

Mise à jour du magasin d'approbations de votre application

Vous pouvez mettre à jour le magasin d'approbations pour les applications qui utilisent SQL*Plus ou JDBC dans le cadre de connexions SSL/TLS.

Mise à jour du magasin d'approbations des applications pour SQL*Plus

Vous pouvez mettre à jour le magasin d'approbations pour les applications qui utilisent SQL*Plus dans le cadre de connexions SSL/TLS.

> **Note**
>
> Lors de la mise à jour du magasin d'approbations, vous pouvez conserver les certificats plus anciens en complément de l'ajout des nouveaux certificats.

Pour mettre à jour le magasin d'approbations pour les applications SQL*Plus

1. Téléchargez le certificat racine 2019 qui fonctionne pour toutes les régions AWS et placez le fichier dans le répertoire `ssl_wallet`.

Pour plus d'informations sur le téléchargement du certificat racine, consultez Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).

2. Exécutez la commande suivante afin de mettre à jour le portefeuille Oracle.

```
prompt>orapki wallet add -wallet $ORACLE_HOME/ssl_wallet -trusted_cert -cert
      $ORACLE_HOME/ssl_wallet/rds-ca-2019-root.pem -auto_login_only
```

Remplacez le nom du fichier par celui du fichier téléchargé.

3. Exécutez la commande suivante pour vérifier que le portefeuille a été installé avec succès.

```
prompt>orapki wallet display -wallet $ORACLE_HOME/ssl_wallet
```

La sortie doit contenir les lignes suivantes :

```
Trusted Certificates:
Subject: CN=Amazon RDS Root 2019 CA,OU=Amazon RDS,O=Amazon Web Services\,
 Inc.,L=Seattle,ST=Washington,C=US
```

Mise à jour du magasin d'approbations de votre application pour JDBC

Vous pouvez mettre à jour le magasin d'approbations pour les applications qui utilisent JDBC dans le cadre de connexions SSL/TLS.

Pour mettre à jour le magasin d'approbations pour les applications JDBC

1. Téléchargez le certificat racine 2019 qui fonctionne pour toutes les régions AWS et placez le fichier dans le répertoire ssl_wallet.

   Pour plus d'informations sur le téléchargement du certificat racine, consultez Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).

2. Convertissez le certificat au format .der à l'aide de la commande suivante.

```
openssl x509 -outform der -in rds-ca-2019-root.pem -out rds-ca-2019-root.der
```

Remplacez le nom du fichier par celui du fichier téléchargé.

3. Importez le certificat dans le magasin de clés à l'aide de la commande suivante.

```
keytool -import -alias rds-root -keystore clientkeystore -file rds-ca-2019-root.der
```

4. Vérifiez que le magasin de clés a été mis à jour avec succès.

```
keytool -list -v -keystore clientkeystore.jks
```

Entrez le mot de passe du magasin de clés lorsque vous y êtes invité.

La sortie doit contenir les lignes suivantes :

```
rds-root,date, trustedCertEntry,
```

```
Certificate fingerprint (SHA1):
 D4:0D:DB:29:E3:75:0D:FF:A6:71:C3:14:0B:BF:5F:47:8D:1C:80:96
# This fingerprint should match the output from the below command
openssl x509 -fingerprint -in rds-ca-2019-root.pem -noout
```

Exemple de code Java pour l'établissement de connexions SSL

L'exemple de code suivant montre comment configurer la connexion SSL à l'aide de 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

Une fois que vous avez déterminé que vos connexions de base de données utilisent un protocole SSL/TLS et que vous avez mis à jour le magasin d'approbations de votre application, vous pouvez mettre à jour votre base de données de sorte qu'elle utilise les certificats rds-ca-2019. Pour obtenir des instructions, veuillez consulter l'étape 3 dans Mise à jour de votre certificat CA en modifiant votre instance de base de données (p. 1528).

Modification des paramètres Oracle sqlnet.ora

Le fichier sqlnet.ora inclut des paramètres qui configurent les fonctions Oracle Net sur les serveurs et les clients de bases de données Oracle. L'utilisation de ces paramètres dans le fichier sqlnet.ora vous permet de modifier les propriétés des connexions à l'intérieur et à l'extérieur de la base de données.

Pour plus d'informations sur les raisons pouvant justifier la définition des paramètres sqlnet.ora, consultez Configuring Profile Parameters (Configurations de paramètres de profil) dans la documentation Oracle.

Définition des paramètres sqlnet.ora

Les groupes de paramètres Amazon RDS Oracle incluent un sous-ensemble de paramètres sqlnet.ora. Vous les définissez de la même manière que les autres paramètres Oracle. C'est le préfixe `sqlnetora.` qui identifie les paramètres sqlnet.ora. Par exemple, dans un groupe de paramètres Oracle dans Amazon RDS, le paramètre sqlnet.ora `default_sdu_size` est `sqlnetora.default_sdu_size`.

Pour plus d'informations sur la gestion des groupes de paramètres et la définition des valeurs de paramètres, consultez Utilisation de groupes de paramètres de base de données (p. 225).

Paramètres sqlnet.ora pris en charge

Amazon RDS prend en charge les paramètres sqlnet.ora ci-après. Les modifications apportées aux paramètres sqlnet.ora dynamiques sont appliquées immédiatement.

Paramètre	Valeurs valides	Statique/ Dynamique	Description
`sqlnetora.default_sdu_size`	Oracle 11g – `512` à `65535` Oracle 12c – `512` à `2097152`	Répartition dynamique	Taille, en octets, de l'unité de données de session (SDU). L'unité de données de session (SDU) est la quantité de données placées dans une mémoire tampon et envoyées dans le réseau en une seule fois.
`sqlnetora.diagnostic_enabled`	`ON`, `OFF`	Répartition dynamique	Valeur qui active ou désactive le traçage Automatic Diagnostic Repository (ADR). `ON` indique que le traçage de fichier ADR est utilisé. `OFF` indique que le traçage de fichier non-ADR est utilisé.
`sqlnetora.recv_buf_size`	`8192` – `268435456`	Répartition dynamique	Limite de l'espace tampon pour les opérations de réception de sessions, prise en charge par les protocoles TCP/IP, TCP/IP avec SSL et SDP.
`sqlnetora.send_buf_size`	`8192` – `268435456`	Répartition dynamique	Limite de l'espace tampon pour les opérations d'envoi de sessions, prise en charge par les protocoles TCP/IP, TCP/IP avec SSL et SDP.
`sqlnetora.sqlnet.allowed_logon_version_client`	`8`, `10`, `11`, `12`	Répartition dynamique	Version de protocole d'authentifications minimum autorisée pour les clients, et les serveurs agissant en tant que clients, pour établir une connexion aux instances de bases de données Oracle.
`sqlnetora.sqlnet.allowed_logon_version_server`	`8`, `10`, `11`, `12`, `12a`	Répartition dynamique	Version de protocole d'authentification minimum autorisée pour établir une connexion aux instances de bases de données Oracle.
`sqlnetora.sqlnet.expire_time`	`0` – `4320`	Répartition dynamique	Intervalle, en minutes, pour envoyer une instruction visant à vérifier que les connexions client-serveur sont actives.

Paramètre	Valeurs valides	Statique/ Dynamique	Description
`sqlnetora.sqlnet.inbound_connect_timeout`	0 ou 10 à 7200	Répartition dynamique	Délai, en secondes, imparti à un client pour se connecter au serveur de bases de données et pour fournir les informations d'authentification nécessaires.
`sqlnetora.sqlnet.outbound_connect_timeout`	0 ou 10 à 7200	Répartition dynamique	Délai, en secondes, imparti à un client pour établir une connexion Oracle Net avec une instance de base de données.
`sqlnetora.sqlnet.recv_timeout`	0 ou 10 à 7200	Répartition dynamique	Délai, en secondes, imparti à un serveur de bases de données pour attendre les données client après l'établissement d'une connexion.
`sqlnetora.sqlnet.send_timeout`	0 ou 10 à 7200	Répartition dynamique	Délai, en secondes, imparti à un serveur de bases de données pour terminer une opération d'envoi aux clients après l'établissement d'une connexion.
`sqlnetora.tcp.connect_timeout`	0 ou 10 à 7200	Répartition dynamique	Délai, en secondes, imparti à un client pour établir une connexion TCP avec un serveur de bases de données.
`sqlnetora.trace_level_server`	`0`, `4`, `10`, `16`, `OFF`, `USER`, `ADMIN`, `SUPPORT`	Répartition dynamique	Pour le traçage non-ADR, active le traçage du serveur à un niveau défini ou le désactive.

La valeur par défaut pour chaque paramètre sqlnet.ora pris en charge est la valeur par défaut Oracle correspondant à la version. Pour plus d'informations sur les valeurs par défaut pour Oracle 12c, consultez Parameters for the sqlnet.ora File (Paramètres pour le fichier sqlnet.ora) dans la documentation Oracle 12c. Pour plus d'informations sur les valeurs par défaut pour Oracle 11g, consultez Parameters for the sqlnet.ora File (Paramètres pour le fichier sqlnet.ora) dans la documentation Oracle 11g.

Affichage des paramètres sqlnet.ora

Vous pouvez afficher les paramètres sqlnet.ora et leurs valeurs via la AWS Management Console, l'AWS CLI ou un client SQL.

Affichage des paramètres sqlnet.ora à l'aide de la console

Pour plus d'informations sur l'affichage des paramètres d'un groupe de paramètres, consultez Utilisation de groupes de paramètres de base de données (p. 225).

Dans les groupes de paramètres Oracle, c'est le préfixe `sqlnetora.` qui identifie les paramètres sqlnet.ora.

Affichage des paramètres sqlnet.ora à l'aide de l'AWS CLI

Pour afficher les paramètres sqlnet.ora qui ont été configurés dans un groupe de paramètres Oracle, utilisez la commande describe-db-parameters de l'AWS CLI.

Pour afficher tous les paramètres sqlnet.ora d'une instance de base de données Oracle, appelez la commande download-db-log-file-portion de l'AWS CLI. Spécifiez l'identifiant de l'instance de base de données, le nom du fichier journal et le type de sortie.

Example

Le code suivant répertorie tous les paramètres sqlnet.ora pour `mydbinstance`.

Pour Linux, macOS ou Unix :

```
aws rds download-db-log-file-portion \
--db-instance-identifier mydbinstance \
--log-file-name trace/sqlnet-parameters \
--output text
```

Pour Windows :

```
aws rds download-db-log-file-portion ^
--db-instance-identifier mydbinstance ^
--log-file-name trace/sqlnet-parameters ^
--output text
```

Affichage des paramètres sqlnet.ora à l'aide d'un client SQL

Une fois que vous vous êtes connecté à l'instance de base de données Oracle dans un client SQL, la requête suivante répertorie les paramètres sqlnet.ora.

```
SELECT * FROM TABLE
   (rdsadmin.rds_file_util.read_text_file(
        p_directory => 'BDUMP',
        p_filename  => 'sqlnet-parameters'));
```

Pour plus d'informations sur la connexion à une instance de base de données Oracle dans un client SQL, consultez Connexion à une instance de base de données Oracle (p. 961).

Mise à niveau du moteur de base de données Oracle

Lorsque Amazon RDS prend en charge une nouvelle version d'Oracle, vous pouvez mettre à niveau vos instances de base de données vers cette nouvelle version. Amazon RDS prend en charge les mises à niveau suivantes à une instance de base de données Oracle :

- Mises à niveau de version majeure.

  En général, une mise à niveau de version majeure pour un moteur de base de données peut introduire des modifications non compatibles avec les applications existantes. Pour effectuer une mise à niveau de version majeure, modifiez l'instance de base de données manuellement.

  > **Important**
  >
  > Le 1er novembre 2020, Amazon RDS commence à mettre automatiquement niveau les instances Oracle 11g SE1 License Included (LI) vers Oracle 19c. La mise à niveau automatique

applique la dernière mise à jour Oracle disponible à toutes les instances de base de données 11g. Pour de plus amples informations, veuillez consulter Préparation de la mise à niveau automatique d'Oracle 11g SE1 (p. 982).

- Mises à niveau de version mineure.

  Une mise à niveau de version mineure contient uniquement des modifications rétrocompatibles avec les applications existantes. Les mises à niveau de version mineure sont effectuées automatiquement si vous activez l'option correspondante sur votre instance de base de données. Dans tous les autres cas, vous devez modifier manuellement l'instance de base de données.

La mise à jour du moteur de base de données provoque une panne. La durée de cette dernière dépend de la version de votre moteur et de la taille de l'instance.

Pour plus d'informations sur les versions Oracle disponibles sur Amazon RDS, consultez Notes de mise à jour pour le moteur de base de données Oracle (p. 1208).

Présentation des mises à niveau du moteur de base de données Oracle

Si la période de rétention des sauvegardes de votre instance de base de données est supérieure à 0, Amazon RDS prend les instantanés de base de données suivants au cours de la mise à niveau :

1. Un instantané de l’instance de base de données avant que toute modification de mise à niveau soit apportée. Si la mise à niveau ne fonctionne pas pour vos bases de données, vous pouvez restaurer cet instantané pour créer une instance de base de données exécutant l'ancienne version.
2. Un instantané de l'instance de base de données une fois la mise à niveau terminée.

> **Note**
>
> Pour modifier la période de rétention des sauvegardes, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Une fois une mise à niveau terminée, vous ne pouvez pas rétablir la version précédente du moteur de base de données. Toutefois, vous créez une nouvelle instance de base de données en restaurant l'instantané de base de données pris avant la mise à niveau.

Mises à niveau Oracle dans un déploiement multi-AZ

Si votre instance de base de données se trouve dans un déploiement Multi-AZ, Amazon RDS met à niveau les deux réplicas, principal et de secours. Si aucune mise à jour du système d'exploitation n'est requise, les mises à niveau principale et de secours se produisent simultanément. Les instances ne sont pas disponibles tant que la mise à niveau n'est pas terminée.

Si des mises à jour du système d'exploitation sont requises dans le cadre d'un déploiement Multi-AZ, Amazon RDS applique ces mises à jour lorsque vous demandez la mise à niveau de la base de données. Amazon RDS effectue les opérations suivantes :

1. Mise à jour du système d'exploitation sur l'instance de base de données de secours.
2. Mise à niveau de l'instance de base de données de secours.
3. Basculement de l'instance principale vers l'instance de base de données de secours.
4. Mise à niveau du système d'exploitation sur la nouvelle instance de base de données de secours, qui était auparavant l'instance principale.
5. Mise à niveau de la nouvelle instance de base de données de secours.

Mises à niveau Oracle des réplicas en lecture

La version du moteur de base de données Oracle de l'instance de base de données source et tous ses réplicas en lecture doivent être identiques. Amazon RDS procède à la mise à niveau via les étapes suivantes :

1. Mise à niveau de l'instance de base de données source. Les réplicas en lecture sont disponibles au cours de cette étape.
2. Mise à niveau des réplicas en lecture en parallèle, quelles que soient les fenêtres de maintenance des réplicas. La base de données source est disponible pendant cette étape.

Pour les mises à niveau de versions majeures des réplicas en lecture entre régions, Amazon RDS effectue des actions supplémentaires :

- Génération automatique d’un groupe d'options pour la version cible
- Copie de toutes les options et tous les paramètres d'option du groupe d'options d'origine vers le nouveau groupe d'options
- Association du réplica en lecture entre régions mis à niveau au nouveau groupe d'options

Mises à niveau Oracle des instances de base de données micro

Nous ne recommandons pas la mise à niveau des bases de données s'exécutant sur des instances de base de données micro. En effet, ces instances ont un processeur limité et la mise à niveau peut donc prendre des heures.

Vous pouvez mettre à niveau des micro-instances de base de données dont la capacité de stockage est réduite (entre 10 et 20 Gio) en copiant vos données à l'aide de Data Pump. Avant de migrer vos instances de base de données de production, nous vous recommandons de les tester en copiant des données à l'aide de Data Pump.

Mises à niveau de version majeure.

Amazon RDS prend en charge les mises à niveau des versions majeures suivantes.

Pour effectuer une mise à niveau de version majeure, modifiez l'instance de base de données manuellement. Les mises à niveau de versions majeures ne sont pas effectuées automatiquement.

Versions prises en charge pour les mises à niveau majeures

Amazon RDS prend en charge les mises à niveau des versions majeures suivantes.

Version actuelle	Mise à niveau prise en charge
18.0.0.0	19.0.0.0
12.2.0.1	19.0.0.0 18.0.0.0
12.1.0.2	19.0.0.0 18.0.0.0 12.2.0.1

Version actuelle	Mise à niveau prise en charge
11.2.0.4	19.0.0.0 18.0.0.0 12.2.0.1 12.1.0.2.v5 et versions 12.1 supérieures

Les mises à niveau de versions majeures ne sont pas prises en charge pour les versions obsolètes d'Oracle, comme les versions 11.2.0.3 et 11.2.0.2. Le retour à une ancienne version majeure n'est pas pris en charge pour les versions Oracle.

Une mise à niveau majeure de version de la version 11g vers la version 12c doit effectuer une mise à niveau vers un PSU (Patch Set Update) Oracle publié le même mois ou ultérieurement. Par exemple, une mise à niveau de version majeure de 11.2.0.4.v14 vers 12.1.0.2.v11 est prise en charge. Cependant, une mise à niveau de version majeure de 11.2.0.4.v14 vers 12.1.0.2.v9 n'est pas prise en charge. Cela s'explique par le fait qu'Oracle version 11.2.0.4.v14 a été lancé en octobre 2017 et Oracle version 12.1.0.2.v9 en juillet 2017. Pour plus d'informations sur la date de parution de chaque PSU Oracle, consultez Notes de mise à jour pour le moteur de base de données Oracle (p. 1208).

Classes d'instance prises en charge pour les mises à niveau majeures

Dans certains cas, il est possible que votre instance de base de données Oracle s'exécute sur une classe d'instance qui n'est pas prise en charge pour la version vers laquelle vous effectuez la mise à niveau. Dans ce cas, assurez-vous de migrer l'instance de base de données vers une classe prise en charge avant la mise à niveau. Pour plus d'informations sur les classes d'instances de base de données prises en charge pour chaque version et édition de Amazon RDS Oracle, consultez la section Classes d'instances de base de données (p. 6).

Collecte de statistiques avant les mises à niveau majeures

Avant d'effectuer une mise à niveau de version majeure, Oracle vous recommande de recueillir des statistiques de l'optimiseur sur l'instance de base de données que vous mettez à jour. La collecte de statistiques de l'optimiseur peut réduire les temps d'arrêt de l'instance de base de données lors de la mise à niveau.

Pour recueillir des statistiques de l'optimiseur, connectez-vous à l'instance de base de données en tant qu'utilisateur principal et exécutez la procédure `DBMS_STATS.GATHER_DICTIONARY_STATS`, comme dans l'exemple suivant.

```
EXEC DBMS_STATS.GATHER_DICTIONARY_STATS;
```

Pour plus d'informations, consultez la section Gathering Optimizer Statistics to Decrease Oracle Database Downtime de la documentation Oracle.

Autorisation d'installation des mises à niveau majeures

Une mise à niveau majeure de la version du moteur peut être incompatible avec votre application. La mise à niveau est irréversible. Si vous spécifiez une version majeure différente de la version principale actuelle pour le paramètre EngineVersion, vous devez autoriser les mises à niveau de version majeure.

Si vous mettez à niveau une version majeure à l'aide de la commande CLI modify-db-instance, vous devez spécifier `--allow-major-version-upgrade`. Cette autorisation n'est pas un paramètre permanent,

vous devez donc spécifier `--allow-major-version-upgrade` chaque fois que vous effectuez une mise à niveau majeure. Ce paramètre n'a aucun impact sur les mises à niveau des versions mineures du moteur. Pour de plus amples informations, veuillez consulter Mise à niveau d'une version du moteur d'une instance de base de données (p. 267).

Si vous mettez à niveau une version majeure à l'aide de la console, vous n'avez pas besoin de choisir une option pour autoriser la mise à niveau. Au lieu de cela, la console affiche un avertissement indiquant que les mises à niveau majeures sont irréversibles.

Mises à niveau des versions mineures d'Oracle

Une mise à niveau des versions mineures s'applique à un PSU (Patch Set Update) ou à un RU (Release Update) de base de données Oracle dans une version majeure.

Un Amazon RDS pour instance de base de données Oracle est planifié pour être mis à niveau automatiquement pendant le créneau de maintenance suivant lorsqu'il répond aux conditions suivantes :

- L'option Mise à niveau automatique de versions mineures est activée pour l'instance de base de données.
- L'instance de base de données n'exécute pas la dernière version mineure de moteur de base de données.

L'instance de base de données est mise à niveau vers le PSU ou le RU du dernier trimestre dans les quatre à six semaines suivant sa mise à disposition par Amazon RDS pour Oracle. Pour plus d'informations sur les PSU et les RU, consultez Notes de mise à jour pour le moteur de base de données Oracle (p. 1208).

Les mises à niveau des versions mineures suivantes ne sont pas prises en charge.

Version actuelle	Mise à niveau non prise en charge
12.1.0.2.v6	12.1.0.2.v7
12.1.0.2.v5	12.1.0.2.v7
12.1.0.2.v5	12.1.0.2.v6

> **Note**
>
> Les retours à des versions antérieures de versions mineures ne sont pas pris en charge.

Chemins de mise à niveau Oracle SE2

Le tableau suivant montre les chemins de mise à niveau pris en charge vers la version Standard Edition Two (SE2). Pour plus d'informations sur les modèles Licence incluse et Bring Your Own License, consultez Options de licence Oracle (p. 930).

Votre configuration existante	Configuration SE2 prise en charge
12.2.0.1 SE2, BYOL	12.2.0.1 SE2, BYOL ou licence incluse
12.1.0.2 SE2, BYOL	12.2.0.1 SE2, BYOL ou licence incluse

Votre configuration existante	Configuration SE2 prise en charge
	12.1.0.2 SE2, BYOL ou licence incluse
11.2.0.4 SE1, BYOL ou licence incluse 11.2.0.4 SE, BYOL	12.2.0.1 SE2, BYOL ou licence incluse 12.1.0.2 SE2, BYOL ou licence incluse

Pour mettre à niveau votre configuration existante vers une configuration SE2 prise en charge, utilisez un chemin de mise à niveau pris en charge. Pour plus d'informations, consultez Mises à niveau de version majeure. (p. 977).

Considérations relatives aux mises à niveau d'une base de données Oracle

Avant la mise à niveau, vérifiez les implications relatives aux groupes d'options, groupes de paramètres et fuseaux horaires.

Considérations relatives au groupe d'options

Si votre instance de base de données utilise un groupe d'options personnalisé, Amazon RDS ne peut pas toujours attribuer automatiquement un nouveau groupe d'options à votre instance de base de données. Par exemple, ceci se produit lorsque vous procédez à une mise à niveau vers une nouvelle version majeure. Dans ce cas, vous devez spécifier un nouveau groupe d'options pendant la mise à niveau. Nous vous recommandons de créer un nouveau groupe d'options et d'y ajouter les mêmes options qu'à votre groupe d'options personnalisé existant.

Pour plus d'informations, consultez Création d'un groupe d'options (p. 212) ou Copie d'un groupe d'options (p. 213).

Si votre instance de base de données utilise un groupe d'options personnalisé contenant l'option APEX, vous pouvez dans certains cas réduire le temps nécessaire à la mise à niveau de votre instance de base de données. Pour ce faire, mettez à niveau votre version d'APEX en même temps que votre instance de base de données. Pour plus d'informations, consultez Mise à niveau de la version d'APEX (p. 1036).

Considérations relatives au groupe de paramètres

Si votre instance de base de données utilise un groupe de paramètres personnalisé, Amazon RDS n'est pas toujours en mesure d'attribuer automatiquement un nouveau groupe de paramètres à votre instance de base de données. C'est le cas, par exemple, lorsque vous procédez à une mise à niveau vers une nouvelle version majeure. Dans ce cas, assurez-vous de spécifier un nouveau groupe de paramètres lors de la mise à niveau. Nous vous recommandons de créer un nouveau groupe de paramètres et de configurer les mêmes paramètres que ceux de votre groupe de paramètres personnalisé existant.

Pour de plus amples informations, veuillez consulter Création d'un groupe de paramètres de bases de données (p. 227) ou Copie d'un groupe de paramètres de bases de données (p. 231).

Considérations relatives au fuseau horaire

L'option de fuseau horaire vous permet de modifier le fuseau horaire système utilisé par votre instance de base de données Oracle. Par exemple, vous devrez peut-être modifier le fuseau horaire d'une instance de base de données afin qu'elle soit compatible avec un environnement sur site ou une application héritée.

L'option de fuseau horaire modifie le fuseau horaire au niveau de l'hôte. Amazon RDS for Oracle met à jour automatiquement le fuseau horaire système tout au long de l'année. Pour de plus amples informations sur le fuseau horaire système, veuillez consulter Fuseau horaire Oracle (p. 1088).

Lorsque vous créez une instance de base de données Oracle, la base de données définit automatiquement le fuseau horaire de la base de données. Le fuseau horaire de la base de données est également connu sous le nom de fuseau horaire pour l'heure d'été (DST). Le fuseau horaire de la base de données est distinct du fuseau horaire système.

Entre les versions de base de données Oracle, les jeux de correctifs ou les correctifs individuels peuvent inclure de nouvelles versions d'heure d'été. Ces correctifs reflètent les modifications apportées aux règles de transition pour diverses régions de fuseau horaire. Par exemple, un gouvernement peut modifier l'entrée en vigueur de l'heure d'été. Les modifications apportées aux règles d'heure d'été peuvent affecter les données existantes du type de données `TIMESTAMP WITH TIME ZONE`.

Si vous mettez à niveau une instance RDS for Oracle, Amazon RDS ne met pas à niveau le fuseau horaire de la base de données automatiquement. Pour mettre à niveau manuellement le fuseau horaire de la base de données, créez une nouvelle instance de base de données Oracle dotée du correctif d'heure d'été souhaité. Ensuite, migrez les données depuis votre instance actuelle vers la nouvelle instance. Vous pouvez migrer des données à l'aide de plusieurs techniques, dont les suivantes :

- Oracle GoldenGate
- AWS Database Migration Service
- Oracle Data Pump
- Exportation/importation d'origine (annulation de la prise en charge d'utilisation générale à partir d'Oracle Database 11g)

> **Note**
>
> Lorsque vous migrez des données à l'aide d'Oracle Data Pump, l'utilitaire déclenche l'erreur ORA-39405 lorsque la version du fuseau horaire cible est inférieure à la version du fuseau horaire source.

Pour de plus amples informations, veuillez consulter TIMESTAMP WITH TIMEZONE Restrictions dans la documentation Oracle.

Test d'une mise à niveau

Avant d'effectuer une mise à niveau de version majeure sur votre instance de base de données, testez soigneusement la compatibilité de votre base de données et de toutes les applications qui y accèdent avec la nouvelle version. Nous vous recommandons d'utiliser la procédure suivante.

Pour tester une mise à niveau de version majeure

1. Passez en revue la documentation de la mise à niveau Oracle pour la nouvelle version du moteur de base de données pour voir si des problèmes de compatibilité peuvent affecter votre base de données ou vos applications. Pour plus d'informations, consultez le document Database Upgrade Guide (Guide de mise à niveau de base de données) dans la documentation d'Oracle.
2. Si votre instance de base de données utilise un groupe d'options personnalisé, créez un nouveau groupe d'options compatible avec la version vers laquelle vous procédez à la mise à niveau. Pour plus d'informations, consultez Considérations relatives au groupe d'options (p. 980).
3. Si votre instance de base de données utilise un groupe de paramètres personnalisé, créez un nouveau groupe de paramètres compatible avec la version vers laquelle vous procédez à la mise à niveau. Pour plus d'informations, consultez Considérations relatives au groupe de paramètres (p. 980).
4. Créez un instantané de base de données de l'instance de base de données à mettre à niveau. Pour de plus amples informations, veuillez consulter Création d'un instantané de base de données (p. 327).

5. Restaurez l'instantané de base de données pour créer une nouvelle instance de base de données de test. Pour de plus amples informations, veuillez consulter Restauration à partir d'un instantané de base de données (p. 329).
6. Modifiez cette nouvelle instance de base de données de test pour la mettre à niveau vers la nouvelle version, en utilisant l'une des méthodes suivantes :
   - Console (p. 268)
   - AWS CLI (p. 268)
   - API RDS (p. 269)
7. Effectuez des tests :
   - Exécutez sur l'instance de base de données mise à niveau autant de tests d'assurance qualité que nécessaire pour garantir que votre base de données et votre application fonctionnent correctement avec la nouvelle version.
   - Implémentez tous les nouveaux tests requis pour évaluer l'impact des éventuels problèmes de compatibilité que vous avez identifiés à l'étape 1.
   - Testez l'ensemble des procédures stockées, fonctions et déclencheurs.
   - Dirigez les versions de test de vos applications vers l'instance de base de données mise à niveau. Vérifiez que les applications fonctionnent correctement avec la nouvelle version.
   - Evaluez le stockage utilisé par l'instance mise à niveau pour déterminer si la mise à niveau requiert un stockage supplémentaire. Vous devrez peut-être choisir une plus grande classe d'instance pour la prise en charge de la nouvelle version en production. Pour plus d'informations, consultez Classes d'instances de base de données (p. 6).
8. Si tous les tests réussissent, mettez à niveau votre instance de base de données de production. Nous vous recommandons de confirmer que l'instance de base de données fonctionne correctement avant d'autoriser les opérations d'écriture sur l'instance de base de données.

Préparation de la mise à niveau automatique d'Oracle 11g SE1

Le 1er novembre 2020, nous prévoyons de commencer à mettre à niveau automatiquement les instances Oracle 11g SE1 License Included (LI) vers Oracle 19c pour Amazon RDS for Oracle. La dernière mise à jour (RU) Oracle sera installée sur toutes les instances 11g, y compris les instances réservées.

> **Important**
>
> Si votre instance de base de données se trouve dans la classe d'instance db.t2.micro ou db.t3.micro, votre bail sera annulé. Vous pouvez acheter de nouvelles instances réservées pour la nouvelle classe d'instance exécutée sur Oracle 19c SE2. Pour plus d'informations, contactez AWS Support.

Rubriques

- Choix d'une stratégie de mise à niveau (p. 982)
- Migration de SE2 vers EE à l'aide d'instantanés (p. 983)
- Modification du modèle de licence en Bring Your Own License (BYOL) (p. 984)
- Fonctionnement de la mise à niveau automatique de 11g SE1 (p. 985)

Choix d'une stratégie de mise à niveau

Avant le 1er novembre 2020, si votre instance de base de données exécute 11.2.0.4 SE LI et que vous ne souhaitez pas qu'elle soit automatiquement mise à niveau par Amazon RDS, utilisez l'une des stratégies suivantes :

- Mettez à niveau votre instance de base de données vers Oracle versions 12.1, 12.2, 18c ou 19c sur le modèle LI.
- Mettez à niveau vos instantanés 11.2, puis restaurez-les. Pour plus d'informations, consultez Migration de SE2 vers EE à l'aide d'instantanés (p. 983).
- Modifiez votre instance vers le modèle Bring Your Own License (BYOL), si vous disposez de la licence SE1 appropriée. Pour plus d'informations, consultez Modification du modèle de licence en Bring Your Own License (BYOL) (p. 984).

Si votre instance de base de données exécute 11.2.0.4 SE LI et que vous souhaitez qu'elle soit automatiquement mise à niveau par Amazon RDS à partir du 1er novembre 2020, assurez-vous de bien comprendre les implications décrites dans Fonctionnement de la mise à niveau automatique de 11g SE1 (p. 985).

Migration de SE2 vers EE à l'aide d'instantanés

Pour éviter la mise à niveau automatique, vous pouvez migrer le logiciel Oracle des éditions SE vers Enterprise Edition. Pour utiliser cette technique, vous avez besoin d'une licence Oracle non utilisée appropriée pour l'édition et la classe de l'instance de base de données que vous prévoyez d'exécuter. En revanche, il n'est pas possible de migrer d'une édition Entreprise Edition vers d'autres éditions.

Lors de la mise à niveau ou de la restauration d'instantanés, fournissez de nouveaux groupes de paramètres conformes à la version 19c SE2. Nous vous recommandons de faire correspondre étroitement vos groupes d'options 11g SE1 et 19c SE2. Vous disposez des options de mise à niveau suivantes :

- Si vous avez des instantanés SE1 LI 11.2.0.4, mettez-les à niveau vers 12.1, 12.2, 18c ou 19c SE2 sur le modèle LI.
- Si vous avez des instantanés 11.2.0.2 ou 11.2.0.3 SE1 LI, effectuez les opérations suivantes :
  1. Mettez à niveau les instantanés de 11.2.0.2 ou 11.2.0.3 vers 11.2.0.4.
  2. Mettez à niveau les instantanés de 11.2.0.4 vers 12.1, 12.2, 18c ou 19c SE2 LI.

Pour modifier l'édition Oracle et conserver vos données, prenez un instantané de votre instance de base de données en cours d'exécution. Créez ensuite une nouvelle instance de base de données de l'édition souhaitée à partir de l'instantané. À moins que vous ne souhaitiez conserver votre ancienne instance de base de données et que vous disposiez des licences Oracle Database appropriées, nous vous recommandons de supprimer votre ancienne instance de base de données.

Pour migrer de 12.2 SE2 vers 12.2 EE à l'aide d'instantanés

1. Arrêtez votre application.
2. Prenez un instantané de votre instance 12.2 SE2 en suivant les instructions de la section Création d'un instantané de base de données (p. 327).
3. Restaurez l'instantané que vous venez de créer en suivant les instructions de la section Restaurer à partir d'un instantané (p. 331). Pour Moteur, choisissez Oracle Enterprise Edition.

   Pour restaurer l'instantané, Oracle crée une nouvelle instance de base de données.
4. Renommez l'instance de base de données SE2 d'origine en suivant les instructions de la section Affectation d'un nouveau nom à une instance DB (p. 270). Par exemple, si l'instance de base de données d'origine est `orcl1`, vous pouvez la renommer en `orcl1-se2`.
5. Renommez la nouvelle instance EE de sorte qu'elle corresponde au nom d'origine de l'instance SE2. Par exemple, si l'instance SE2 d'origine est nommée `orcl1`, renommez l'instance EE en `orcl1`. La nouvelle instance portant le même nom que l'instance d'origine, elle peut réutiliser le point de terminaison de l'écouteur.
6. Démarrez votre application et connectez-vous à la nouvelle instance EE.

7. Assurez-vous que l'application fonctionne comme prévu, puis supprimez l'instance SE2.

Pour de plus amples informations sur la mise à niveau des instantanés, veuillez consulter Mise à niveau d'un instantané de base de données Oracle (p. 988).

Modification du modèle de licence en Bring Your Own License (BYOL)

Lorsque vous passez de LI à « Apportez votre propre licence », votre instance de base de données subit quelques minutes de temps d'arrêt. Pendant cette période, RDS for Oracle déplace votre instance de base de données vers un hôte différent. Si les temps d'arrêt vous inquiètent, nous vous recommandons de tester la modification de licence sur un instantané de production restauré.

Console

Une façon de changer le modèle de licence en Bring Your Own License (BYOL) consiste à utiliser AWS Management Console.

Pour changer le modèle de licence en Bring Your Own License (BYOL) à l'aide de la console

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Pour Identifiant de base de données, choisissez l'ID de la base de données dont vous souhaitez modifier le modèle de licence.
4. Sélectionnez Modify.
5. Pour Modèle de licence, choisissez bring-your-own-license.
6. Choisissez Continue.
7. Dans la section Planification des modifications, choisissez Appliquer immédiatement.
8. Choisissez Modifier l'instance de base de données.

AWS CLI

Pour créer un groupe d'options, utilisez la commande AWS CLI `modify-db-instance` avec le paramètre `--license-model`.

Example

L'exemple suivant bascule la base de données nommée `orcl1` vers le modèle de licence Bring Your Own License (BYOL).

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier orcl1 \
    --license_model bring-your-own-license
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier orcl1 ^
    --license_model bring-your-own-license
```

À ce stade, ouvrez une demande d'annulation d'instance réservée. Demandez à votre responsable des comptes techniques de travailler avec l'équipe des opérations relatives aux instances réservées.

API RDS

Pour créer un groupe d'options, appelez l'opération d'API Amazon RDS `CreateOptionGroup` avec le paramètre `LicenseModel`.

Fonctionnement de la mise à niveau automatique de 11g SE1

Nous prévoyons de commencer à mettre à niveau automatiquement votre instance RDS for Oracle 11.2 le 1er novembre 2020, uniquement si vous n'avez mis en œuvre aucune stratégie de la section précédente. La mise à niveau automatique se produit pendant les fenêtres de maintenance. Toutefois, si les fenêtres de maintenance ne sont pas disponibles lorsque la mise à niveau doit avoir lieu, Amazon RDS for Oracle met immédiatement à niveau le moteur.

La mise à niveau comprend les étapes suivantes :

1. Mise à l'échelle de votre classe d'instance (p. 985)
2. Mise à niveau de 11.2.0.4 SE1 vers 19c SE2 (p. 986)

> **Important**
>
> Les mises à niveau automatiques peuvent avoir des conséquences inattendues pour les piles AWS CloudFormation. Si vous comptez sur Amazon RDS pour mettre automatiquement à niveau vos instances de base de données, vous risquez de rencontrer des problèmes avec AWS CloudFormation.

Mise à l'échelle de votre classe d'instance

Certains types d'instance de base de données ne sont pas pris en charge pour 19c. Avant de commencer la mise à niveau automatique, Amazon RDS met à l'échelle la classe non prise en charge vers une classe prise en charge correspondante. Le tableau suivant répertorie la classe prise en charge correspondant à chaque classe non prise en charge.

Classe d'instance non prise en charge	vCPU dans une classe non prise en charge	Mémoire dans une classe non prise en charge	Classe d'instance prise en charge	vCPU dans une classe prise en charge	Mémoire dans une classe non prise en charge	HugePages est-il activé par défaut ?
t3.micro	2	1 Go	t3.small	2	2 Go	Non
t2.micro	1	1 Go	t3.small	2	2 Go	Non
t2.small	1	2 Go	t3.small	2	2 Go	Non
t2.medium	2	4 Go	t3.medium	2	4 Go	Non
t2.large	2	8 Go	t3.large	2	8 Go	Non
t2.xlarge	4	16 Go	t3.xlarge	4	16 Go	Non

Classe d'instance non prise en charge	vCPU dans une classe non prise en charge	Mémoire dans une classe non prise en charge	Classe d'instance prise en charge	vCPU dans une classe prise en charge	Mémoire dans une classe non prise en charge	HugePages est-il activé par défaut ?
t2.2xlarge	8	32 GO	t3.2xlarge	8	32 GO	Non
m3.large	2	7,5 Go	m5.large	2	8 Go	Non
m3.xlarge	4	15 Go	m5.xlarge	4	16 Go	Oui
m3.2xlarge	8	30 Go	m5.2xlarge	8	32 GO	Oui
r3.large	2	15,25 Go	r5.large	2	16 Go	Oui
r3.xlarge	4	30,5 Go	r5.xlarge	4	32 GO	Oui
r3.2xlarge	8	61 Go	r5.2xlarge	8	64 Go	Oui
r3.4xlarge	16	122 Go	r5.4xlarge	16	128 Go	Oui
r3.8xlarge	32	244 Go	r5.8xlarge	32	256 Go	Oui

Si votre nouvelle classe d'instance utilise HugePages par défaut, la mise à niveau effectue les étapes suivantes :

1. Clone le groupe de paramètres. Amazon RDS définit explicitement le paramètre d'initialisation `USE_LARGE_PAGES` sur `FALSE`.
2. Applique le groupe de paramètres cloné à l'instance de base de données.
3. Redémarre l'instance de base de données.
4. Met à l'échelle l'instance de base de données à la nouvelle classe d'instance.

Mise à niveau de 11.2.0.4 SE1 vers 19c SE2

Au cours de la mise à niveau automatique, Amazon RDS effectue les opérations suivantes :

1. Clone tous les groupes de paramètres personnalisé en groupes de paramètres 19c. Pour plus d'informations, consultez Clonage de groupes de paramètres (p. 986).
2. Clone tous les groupes d'options personnalisés en groupes d'options 19c. Pour plus d'informations, consultez Clonage de groupes d'options (p. 987).
3. Applique le correctif à l'instance de base de données vers 19c. Pour plus d'informations, consultez Application des correctifs 19c (p. 987).

Clonage de groupes de paramètres

Lors de la mise à niveau automatique, RDS crée de nouveaux groupes de paramètres 19c pour les instances 11g. L'instance mise à niveau utilise les nouveaux groupes de paramètres.

RDS copie tous les paramètres et les valeurs de paramètres de 11g vers 19c. Les paramètres suivants, que RDS filtre avant de créer le groupe de paramètres, font exception :

- `_sqlexec_progression_cost`
- `exafusion_enabled`
- `global_context_pool_size`

- `max_connections`
- `max_enabled_roles`
- `o7_dictionary_access`
- `optimizer_adaptive_features`
- `parallel_automatic_tuning`
- `parallel_degree_level`
- `sec_case_sensitive_logon`
- `standby_archive_dest`
- `use_indirect_data_buffers`
- `utl_file_dir`

Clonage de groupes d'options

Lors de la mise à niveau automatique, RDS crée de nouveaux groupes d'options 19c pour les instances 11g. L'instance mise à niveau utilise les nouveaux groupes d'options.

Le tableau suivant décrit les options qui nécessitent une gestion particulière.

Option	Remarques de gestion particulière
OEM_AGENT	Si vous utilisez une version de l'agent antérieure à 13.1.0.0.v1, Amazon RDS n'intègre pas cette option dans le groupe d'options clonées. Les versions de l'agent 19c commencent à partir d'une version ultérieure à celle disponible sur 11g.
XMLDB	Amazon RDS n'intègre pas cette option dans les groupes d'options clonés car cette option n'est pas prise en charge pour les versions ultérieures à 11g.
APEX	Si vous exécutez APEX ou APEX-DEV version 4.1.1.v1, 4.2.6.v1, 5.0.4.v1, 5.1.2.v1, 5.1.4.v1, 18.1.v1 ou 18.2.v1, Amazon RDS procède à la mise à jour en version 19.2.v1. Si vous exécutez APEX 19.1.v1, Amazon RDS copie l'option telle qu'elle est.
SQLT	Si vous exécutez SQLT 12.1.160429 ou 12.2.180331, Amazon RDS le désinstalle puis le met à niveau en version 12.2.180725. Important La mise à niveau automatique supprime les données SQLT préexistantes sur 12.1.160429 ou 12.2.180331.

Application des correctifs 19c

Au cours de la dernière étape de la mise à niveau, Amazon RDS applique les correctifs nécessaires pour mettre à niveau le moteur de base de données vers 19c. Assurez-vous de spécifier les nouveaux groupes de paramètres et d'options 19c que l'instance de base de données devra utiliser après la mise à niveau.

Mise à niveau d'une instance de base de données Oracle

Pour plus d'informations sur la mise à niveau manuelle ou automatique d'une instance de base de données Oracle, consultez la section Mise à niveau d'une version du moteur d'une instance de base de données (p. 267).

Mise à niveau d'un instantané de base de données Oracle

Si vous avez des instantanés de base de données manuels existants, vous pouvez les mettre à niveau vers une version ultérieure du moteur de base de données Oracle.

Quand Oracle cesse de fournir des correctifs pour une version, et que Amazon RDS rend la version obsolète, vous pouvez mettre à niveau vos instantanés qui correspondent à la version obsolète. Pour de plus amples informations, veuillez consulter Gestion des versions du moteur Oracle (p. 953). Pour en savoir plus sur la mise à niveau des instantanés en prévision de la mise à niveau automatique de la version 11.2, veuillez consulter Migration de SE2 vers EE à l'aide d'instantanés (p. 983).

Les mises à niveau d'instantané suivantes sont actuellement prises en charge.

Version d'instantané actuelle	Mise à niveau d'instantané prise en charge
12.1.0.1	12.1.0.2.v8
11.2.0.4	12.1.0.2, 12.2.0.1, 18c et 19c lorsque les conditions suivantes sont remplies : • La version mineure n'est pas une version antérieure. • Vous mettez à niveau l'instantané vers le RU, le RUR ou le PSU pour juillet 2020 ou après. Pour des numéros de version spécifiques, veuillez consulter Notes de mise à jour pour le moteur de base de données Oracle (p. 1208).
11.2.0.3	11.2.0.4.v11
11.2.0.2	11.2.0.4.v12

Amazon RDS prend en charge la mise à niveau des instantanés dans toutes les régions AWS.

Console

Pour mettre à niveau un instantané de base de données Oracle

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Instantanés, puis sélectionnez l'instantané de base de données que vous souhaitez mettre à niveau.
3. Pour Actions, choisissez Upgrade Snapshot (Mettre à niveau l'instantané). La page Upgrade Snapshot (Mettre à niveau l'instantané) s'affiche.
4. Choisissez la nouvelle version du moteur vers laquelle mettre à niveau l'instantané.
5. (Facultatif) Pour Groupe d'options, choisissez le groupe d'options pour l'instantané de base de données mis à niveau. Les mêmes considérations relatives au groupe d'options s'appliquent pour la mise à niveau d'un instantané de base de données et la mise à niveau d'une instance de base de données. Pour de plus amples informations, veuillez consulter Considérations relatives au groupe d'options (p. 980).
6. Choisissez Enregistrer les modifications pour enregistrer vos modifications.

Pendant le processus de mise à niveau, toutes les actions d'instantané sont désactivées pour l'instantané de base de données. De même, le statut de l'instantané de base de données passe de disponible à upgrading (mise à niveau), puis passe à active, une fois la mise à niveau terminée. Si l'instantané de base de données ne peut pas être mis à jour en raison d'un problème d'instantané endommagé, le statut devient indisponible. Vous ne pouvez pas récupérer l'instantané lorsqu'il a ce statut.

Note

Si la mise à niveau de l'instantané de base de données échoue, l'instantané revient à l'état d'origine avec la version originale.

AWS CLI

Pour mettre à niveau un instantané de base de données Oracle à l'aide de l'AWS CLI, appelez la commande modify-db-snapshot avec les paramètres suivants :

- `--db-snapshot-identifier` – Nom de l'instantané de base de données.
- `--engine-version` – Version vers laquelle mettre à niveau l'instantané.

Vous pouvez également devoir fournir le paramètre suivant. Les mêmes considérations relatives au groupe d'options s'appliquent pour la mise à niveau d'un instantané de base de données et la mise à niveau d'une instance de base de données. Pour de plus amples informations, veuillez consulter Considérations relatives au groupe d'options (p. 980).

- `--option-group-name` – Groupe d'options pour l'instantané de base de données mis à niveau.

Example

L'exemple suivant met à niveau un instantané de base de données.

Pour Linux, macOS ou Unix :

```
aws rds modify-db-snapshot \
    --db-snapshot-identifier <mydbsnapshot> \
    --engine-version <11.2.0.4.v12> \
    --option-group-name <default:oracle-se1-11-2>
```

Pour Windows :

```
aws rds modify-db-snapshot ^
    --db-snapshot-identifier <mydbsnapshot> ^
    --engine-version <11.2.0.4.v12> ^
    --option-group-name <default:oracle-se1-11-2>
```

API RDS

Pour mettre à niveau un instantané de base de données Oracle à l'aide de l'API Amazon RDS, appelez l'opératon ModifyDBSnapshot avec les paramètres suivants :

- `DBSnapshotIdentifier` – Nom de l'instantané de base de données.
- `EngineVersion` – Version vers laquelle mettre à niveau l'instantané.

Vous pouvez également devoir fournir le paramètre suivant. Les mêmes considérations relatives au groupe d'options s'appliquent pour la mise à niveau d'un instantané de base de données et la mise à niveau d'une instance de base de données. Pour de plus amples informations, veuillez consulter Considérations relatives au groupe d'options (p. 980).

- `OptionGroupName` – Groupe d'options pour l'instantané de base de données mis à niveau.

Example

L'exemple suivant met à niveau un instantané de base de données.

```
https://rds.amazonaws.com/
    ?Action=ModifyDBSnapshot
    &DBSnapshotIdentifier=mydbsnapshot
    &EngineVersion=11.2.0.4.v12
    &OptionGroupName=default:oracle-se1-11-2
    &SignatureMethod=HmacSHA256
    &SignatureVersion=4
    &Version=2014-10-31
    &X-Amz-Algorithm=AWS4-HMAC-SHA256
    &X-Amz-Credential=AKIADQKE4SARGYLE/20131016/us-west-1/rds/aws4_request
    &X-Amz-Date=20131016T233051Z
    &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
    &X-Amz-Signature=087a8eb41cb1ab5f99e81575f23e73757ffc6a1e42d7d2b30b9cc0be988cff97
```

Importation de données dans Oracle sur Amazon RDS

La façon dont vous importez des données dans une instance de base de données Amazon RDS dépend du volume de données dont vous disposez ainsi que du nombre et de la variété des objets de base de données dans votre base de données. Par exemple, vous pouvez utiliser Oracle SQL Developer pour importer une base de données simple de 20 Mo. Vous pouvez utiliser Oracle Data Pump pour importer des bases de données complexes ou des bases de données de centaines de mégaoctets ou de plusieurs téraoctets.

Vous pouvez également utiliser AWS Database Migration Service (AWS DMS) pour importer des données vers une instance de base de données Amazon RDS. AWS DMS peut migrer les bases de données sans interruption et, pour de nombreux moteurs de bases de données, poursuivre la réplication en cours jusqu'à ce que vous soyez prêt à basculer sur la base de données cible. Vous pouvez migrer Oracle vers le même moteur de base de données ou vers un moteur de base de données différent avec AWS DMS. Si vous migrez à partir d'un moteur de base de données différent, vous pouvez utiliser l'AWS Schema Conversion Tool pour migrer des objets de schéma qui ne sont pas migrés par AWS DMS. Pour plus d'informations sur AWS DMS, consultez Qu'est-ce qu'un AWS Database Migration Service.

Avant d'utiliser ces techniques de migration, nous vous recommandons la bonne pratique de réaliser une sauvegarde de votre base de données. Après avoir importé les données, vous pouvez sauvegarder vos instances de base de données Amazon RDS en créant des instantanés. Vous pouvez restaurer ultérieurement la base de données à partir des instantanés. Pour de plus amples informations, veuillez consulter Sauvegarde et restauration d'une instance de base de données Amazon RDS (p. 317).

> **Note**
>
> Vous pouvez également importer des données dans Oracle à l'aide de fichiers issus de Amazon S3. Par exemple, vous pouvez télécharger des fichiers Data Pump de Amazon S3 vers l'hôte d'instance de base de données. Pour de plus amples informations, veuillez consulter Intégration Amazon S3 (p. 1014).

Importation à l'aide d'Oracle SQL Developer

Pour les petites bases de données, vous pouvez utiliser Oracle SQL Developer, un outil Java graphique distribué gratuitement par Oracle. Vous pouvez installer cet outil sur votre ordinateur de bureau (Windows, Linux ou Mac) ou l'un de vos serveurs. Oracle SQL Developer fournit des options pour la migration des données entre deux bases de données Oracle, ou pour la migration des données depuis d'autres bases de données, comme MySQL, vers Oracle. Oracle SQL Developer convient parfaitement à la migration de bases de données peu volumineuses. Nous vous recommandons de lire la documentation de produit Oracle SQL Developer avant de commencer à migrer vos données.

Après avoir installé SQL Developer, vous pouvez l'utiliser pour vous connecter à vos bases de données source et cible. Utilisez la commande Database Copy (Copie de la base de données) dans le menu Tools pour copier vos données vers votre instance Amazon RDS.

Pour télécharger Oracle SQL Developer, consultez http://www.oracle.com/technetwork/developer-tools/sql-developer.

Oracle possède également une documentation sur la façon de migrer depuis d'autres bases de données dont MySQL et SQL Server. Pour plus d'informations, consultez http://www.oracle.com/technetwork/database/migration dans la documentation Oracle.

Importation à l'aide d'Oracle Data Pump

Oracle Data Pump remplace à long terme les utilitaires d'exportation/importation d'Oracle Oracle Data Pump est la solution à privilégier pour transférer d'importants volumes de données d'une installation Oracle vers une instance de base de données Amazon RDS. Vous pouvez utiliser Oracle Data Pump pour plusieurs scénarios :

- Importez des données depuis une base de données Oracle (locale ou une instance Amazon EC2) vers une Amazon RDS pour une instance de base de données Oracle.
- Importation de données depuis une instance de base de données RDS Oracle (locale ou sur une instance Amazon EC2)
- Importation de données entre des instances de bases de données RDS Oracle (par exemple, pour migrer des données d'EC2-Classic vers le VPC)

Pour télécharger les utilitaires Oracle Data Pump, veuillez consulter Oracle Database Software Downloads sur le site web Oracle Technology Network.

Pour en savoir plus sur la compatibilité lors de la migration entre les versions d'Oracle Database, veuillez consulter la documentation Oracle.

Lorsque vous importez des données avec Oracle Data Pump, vous devez transférer le fichier de vidage qui contient les données de la base de données source vers la base de données cible. Vous pouvez transférer le fichier de vidage à l'aide d'un compartiment Amazon S3 ou en utilisant un lien de base de données entre les deux bases de données.

Voici les pratiques recommandées pour utiliser Oracle Data Pump afin d'importer des données dans un Amazon RDS pour l'instance de base de données Oracle :

- Effectuez les importations en mode `schema` ou `table` pour importer des schémas et des objets spécifiques.
- Limitez les schémas que vous importez à ceux requis par votre application.
- N'importez pas en mode `full`.

  Dans la mesure où Amazon RDS pour Oracle n'autorise pas l'accès aux utilisateurs administratifs `SYS` ou `SYSDBA`, l'importation en mode `full`, ou l'importation de schémas pour des composants gérés par

Oracle, risque d'endommager le dictionnaire de données Oracle et d'affecter la stabilité de votre base de données.

- Lors du chargement de volumes de données importants, transférez le fichier de vidage vers le Amazon RDS cible pour l'instance de base de données Oracle, prenez un instantané de base de données de votre instance, puis testez l'importation afin de vérifier sa réussite. Si les composants de la base de données sont invalidés, vous pouvez supprimer l'instance de base de données et la recréer à partir de l'instantané de base de données. L'instance de base de données restaurée inclut les fichiers de vidage intermédiaires sur l'instance de base de données lorsque vous avez pris l'instantané de base de données.
- N'importez pas de fichiers de vidage qui ont été créés à l'aide des paramètres d'exportation Oracle Data Pump `TRANSPORT_TABLESPACES`, `TRANSPORTABLE` ou `TRANSPORT_FULL_CHECK`. Amazon RDS pour les instances de base de données Oracle ne prennent pas en charge l'importation de ces fichiers de vidage.

Les exemples de cette section montrent une façon d'importer des données dans une base de données Oracle, mais il existe de nombreuses façons de le faire avec Oracle Data Pump. Pour obtenir des informations complètes sur l'utilisation d'Oracle Data Pump, veuillez consulter la documentation Oracle.

Les exemples de cette section utilisent le package `DBMS_DATAPUMP`. Les mêmes tâches peuvent être accomplies à l'aide des utilitaires de ligne de commande Oracle Data Pump `impdp` et `expdp`. Vous pouvez installer ces utilitaires sur un hôte distant dans le cadre d'une installation de client Oracle, y compris Oracle Instant Client.

Rubriques

- Importation de données avec Oracle Data Pump et un compartiment Amazon S3 (p. 992)
- Importation de données avec Oracle Data Pump et un lien de base de données (p. 996)

Importation de données avec Oracle Data Pump et un compartiment Amazon S3

Le processus d'importation suivant utilise Oracle Data Pump et un compartiment Amazon S3. Ce processus exporte les données sur la base de données source à l'aide du package Oracle DBMS_DATAPUMP et place le fichier de vidage dans un compartiment Amazon S3. Il télécharge ensuite le fichier de vidage du compartiment Amazon S3 vers le répertoire `DATA_PUMP_DIR` sur l'instance de base de données Oracle Amazon RDS cible. L'étape finale importe les données du fichier de vidage copié dans l'instance de base de données Oracle Amazon RDS à l'aide du package `DBMS_DATAPUMP`.

Le processus est soumis aux exigences suivantes :

- Vous devez disposer d'un compartiment Amazon S3 disponible pour les transferts de fichiers et le compartiment Amazon S3 doit être dans la même région AWS que l'instance de base de données. Pour de plus amples informations, veuillez consulter Créer un compartiment dans le Guide de démarrage d'Amazon Simple Storage Service.
- L'objet que vous téléchargez dans le compartiment Amazon S3 doit être d'une taille inférieure ou égale à 5 To. Pour de plus amples informations sur l'utilisation des objets dans Amazon S3, veuillez consulter Amazon Simple Storage Service Manuel du développeur.

  Note

  Si le fichier de vidage dépasse 5 To, vous pouvez exécuter l'exportation Oracle Data Pump avec l'option parallèle. Cette opération répartit les données dans plusieurs fichiers de vidage de sorte que la taille de chaque fichier ne dépasse pas la limite de 5 To.
- Vous devez préparer le compartiment Amazon S3 pour l'intégration Amazon RDS en suivant les instructions de Conditions préalables à l'intégration de Amazon RDS Oracle avec Amazon S3 (p. 1014).

- Vous devez veiller à disposer de suffisamment d'espace de stockage pour stocker le fichier de vidage sur l'instance source et l'instance de base de données cible.

  Note

  Ce processus importe un fichier de vidage dans le répertoire `DATA_PUMP_DIR`, qui est préconfiguré sur toutes les instances de bases de données Oracle. Ce répertoire est situé sur le même volume de stockage que vos fichiers de données. Lorsque vous importez le fichier de vidage, les fichiers de données Oracle existants utilisent davantage d'espace. Vous devez donc veiller à ce que votre instance de base de données puisse répondre aux besoins de cette utilisation d'espace supplémentaire. Le fichier de vidage importé n'est pas automatiquement supprimé ou purgé du répertoire `DATA_PUMP_DIR`. Pour supprimer le fichier de vidage importé, utilisez UTL_FILE.FREMOVE, disponible sur le site web d'Oracle.

Le processus d'importation qui utilise Oracle Data Pump et un compartiment Amazon S3 comporte les étapes suivantes :

Rubriques

- Étape 1 : Accorder des privilèges à l'utilisateur sur l'instance de base de données cible Amazon RDS (p. 993)
- Étape 2 : utiliser DBMS_DATAPUMP pour créer un fichier de vidage (p. 994)
- Étape 3 : Charger le fichier de vidage dans votre compartiment Amazon S3 (p. 994)
- Étape 4 : Copier le fichier de vidage exporté du compartiment Amazon S3 vers l'instance de base de données cible (p. 995)
- Étape 5 : Utiliser DBMS_DATAPUMP pour importer le fichier de données sur l'instance de base de données cible (p. 995)
- Étape 6 : nettoyer (p. 996)

Étape 1 : Accorder des privilèges à l'utilisateur sur l'instance de base de données cible Amazon RDS

Pour accorder des privilèges à l'utilisateur sur l'instance cible RDS, procédez comme suit :

1. Utilisez SQL Plus ou Oracle SQL Developer pour vous connecter à l'instance de base de données Oracle cible Amazon RDS vers laquelle les données seront importées. Connectez-vous à l'utilisateur principal Amazon RDS. Pour plus d'informations sur la connexion à votre instance de base de données, consultez Connexion à une instance de base de données Oracle (p. 961).
2. Créez les espaces de table requis avant d'importer les données. Pour de plus amples informations, veuillez consulter Création et dimensionnement des espaces de table (p. 1116).
3. Si le compte d'utilisateur dans lequel les données seront importées n'existe pas, créez-en un et accordez-lui les autorisations et rôles nécessaires. Si vous importez des données avec plusieurs schémas d'utilisateur, créez chaque compte d'utilisateur et accordez-lui les privilèges et rôles nécessaires.

   Par exemple, les commandes suivantes créent un utilisateur et lui accordent les autorisations et rôles nécessaires pour importer les données dans le schéma de celui-ci :

   ```
   CREATE USER schema_1 IDENTIFIED BY <password>;
   GRANT CREATE SESSION, RESOURCE TO schema_1;
   ALTER USER schema_1 QUOTA 100M ON users;
   ```

   Cet exemple montre comment accorder au nouvel utilisateur le privilège `CREATE SESSION` et le rôle `RESOURCE`. Des privilèges et rôles supplémentaires peuvent être requis en fonction des objets de la base de données que vous allez importer.

Note

Remplacez *schema_1* par le nom de votre schéma dans cette étape et dans les étapes suivantes.

Étape 2 : utiliser DBMS_DATAPUMP pour créer un fichier de vidage

Utilisez SQL Plus ou Oracle SQL Developer pour vous connecter à l'instance Oracle source avec un utilisateur administrateur. Si la base de données source est une instance de base de données Amazon RDS, connectez-vous avec l'utilisateur principal Amazon RDS. Ensuite, employez l'utilitaire Oracle Data Pump pour créer un fichier de vidage.

Le script suivant crée un fichier de vidage nommé sample.dmp dans le répertoire `DATA_PUMP_DIR` qui contient le schéma *SCHEMA_1*. Remplacez *SCHEMA_1* par le nom du schéma que vous souhaitez exporter.

```
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.START_JOB(v_hdnl);
END;
/
```

Note

Les tâches de vidage de données sont démarrées de façon asynchrone. Pour obtenir des informations sur la surveillance d'une tâche Data Pump, veuillez consulter Monitoring Job Status dans la documentation Oracle. Vous pouvez afficher le contenu du journal d'exportation à l'aide de la procédure `rdsadmin.rds_file_util.read_text_file`. Pour de plus amples informations, consultez Lecture de fichiers dans un répertoire d'instance de base de données (p. 1166).

Étape 3 : Charger le fichier de vidage dans votre compartiment Amazon S3

Chargez le fichier de vidage dans le compartiment Amazon S3.

Utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_s3_tasks.upload_to_s3` pour copier le fichier de vidage dans le compartiment Amazon S3. L'exemple suivant charge tous les fichiers du répertoire *DATA_PUMP_DIR* dans le compartiment Amazon S3 nommé *mys3bucket*.

```
SELECT rdsadmin.rdsadmin_s3_tasks.upload_to_s3(
  p_bucket_name    =>  'mys3bucket',
  p_directory_name =>  'DATA_PUMP_DIR')
AS TASK_ID FROM DUAL;
```

L'instruction `SELECT` renvoie l'ID de la tâche dans un type de données `VARCHAR2`.

Pour plus d'informations, consultez Chargement de fichiers d'une instance de base de données Oracle vers un compartiment Amazon S3 (p. 1021).

Étape 4 : Copier le fichier de vidage exporté du compartiment Amazon S3 vers l'instance de base de données cible

Utilisez SQL Plus ou Oracle SQL Developer pour vous connecter à l'instance de base de données Oracle cible Amazon RDS. Utilisez ensuite la procédure Amazon RDS `rdsadmin.rdsadmin_s3_tasks.download_from_s3` pour copier le fichier de vidage du compartiment Amazon S3 vers l'instance de base de données cible. L'exemple suivant télécharge tous les fichiers d'un compartiment Amazon S3 nommé *mys3bucket* vers le répertoire *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;
```

L'instruction `SELECT` renvoie l'ID de la tâche dans un type de données `VARCHAR2`.

Pour plus d'informations, consultez Téléchargement des fichiers d'un compartiment Amazon S3 vers une instance de base de données Oracle (p. 1023).

Étape 5 : Utiliser DBMS_DATAPUMP pour importer le fichier de données sur l'instance de base de données cible

Utilisez Oracle Data Pump pour importer le schéma dans l'instance de base de données. Notez que des options supplémentaires comme METADATA_REMAP pourraient être obligatoires.

Connectez-vous à l'instance de base de données avec le compte d'utilisateur principal Amazon RDS pour effectuer l'importation.

```
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**
>
> Les tâches de vidage de données sont démarrées de façon asynchrone. Pour obtenir des informations sur la surveillance d'une tâche Data Pump, veuillez consulter Monitoring Job Status dans la documentation Oracle. Vous pouvez afficher le contenu du journal d'importation à l'aide de la procédure `rdsadmin.rds_file_util.read_text_file`. Pour de plus amples informations, consultez Lecture de fichiers dans un répertoire d'instance de base de données (p. 1166).

Vous pouvez vérifier l'importation des données en consultant les table de l'utilisateur sur l'instance de base de données. Par exemple, la requête suivante renvoie le nombre de tables de *SCHEMA_1*.

```
SELECT COUNT(*) FROM DBA_TABLES WHERE OWNER='SCHEMA_1';
```

Étape 6 : nettoyer

Après l'importation des données, vous pouvez supprimer les fichiers que vous ne souhaitez plus conserver. Vous pouvez lister les fichiers dans le répertoire DATA_PUMP_DIR en utilisant la commande suivante :

```
SELECT * FROM TABLE(rdsadmin.rds_file_util.listdir('DATA_PUMP_DIR')) ORDER BY MTIME;
```

La commande suivante peut être utilisée pour supprimer des fichiers dont vous n'avez plus besoin dans le répertoire DATA_PUMP_DIR :

```
EXEC UTL_FILE.FREMOVE('DATA_PUMP_DIR','<file name>');
```

Par exemple, la commande suivante supprime le fichier appelé `"sample_copied.dmp"`.

```
EXEC UTL_FILE.FREMOVE('DATA_PUMP_DIR','sample_copied.dmp');
```

Importation de données avec Oracle Data Pump et un lien de base de données

Le processus d'importation suivant utilise Oracle Data Pump et le package DBMS_FILE_TRANSFER. Le processus se connecte à une instance Oracle source, qui peut être sur site ou une instance Amazon EC2, ou une instance de base de données Amazon RDS Oracle. Le processus exporte ensuite les données à l'aide du package DBMS_DATAPUMP. Il utilise ensuite la méthode `DBMS_FILE_TRANSFER.PUT_FILE` pour copier le fichier de vidage depuis l'instance Oracle vers le répertoire `DATA_PUMP_DIR` sur l'instance de base de données Oracle Amazon RDS cible qui est connectée à l'aide d'un lien de base de données. L'étape finale importe les données du fichier de vidage copié dans l'instance de base de données Oracle Amazon RDS à l'aide du package `DBMS_DATAPUMP`.

Le processus est soumis aux exigences suivantes :

- Vous devez disposer des privilèges d'exécution sur les packages `DBMS_DATAPUMP` et `DBMS_FILE_TRANSFER`.
- Vous devez disposer de privilèges d'écriture sur le répertoire `DATA_PUMP_DIR` de l'instance de base de données source.
- Vous devez veiller à disposer de suffisamment d'espace de stockage pour stocker le fichier de vidage sur l'instance source et l'instance de base de données cible.

> **Note**
>
> Ce processus importe un fichier de vidage dans le répertoire `DATA_PUMP_DIR`, qui est préconfiguré sur toutes les instances de bases de données Oracle. Ce répertoire est situé sur le même volume de stockage que vos fichiers de données. Lorsque vous importez le fichier de vidage, les fichiers de données Oracle existants utilisent davantage d'espace. Vous devez donc veiller à ce que votre instance de base de données puisse répondre aux besoins de cette utilisation d'espace supplémentaire. Le fichier de vidage importé n'est pas automatiquement supprimé ou purgé du répertoire `DATA_PUMP_DIR`. Pour supprimer le fichier de vidage importé, utilisez UTL_FILE.FREMOVE, disponible sur le site web d'Oracle.

Le processus d'importation utilisant Oracle Data Pump et le package `DBMS_FILE_TRANSFER` comporte les étapes suivantes :

Rubriques

- Étape 1 : Accorder des privilèges à l'utilisateur sur l'instance de base de données cible Amazon RDS (p. 997)
- Étape 2 : Accorder des privilèges à l'utilisateur sur la base de données source (p. 997)
- Étape 3 : utiliser DBMS_DATAPUMP pour créer un fichier de vidage (p. 998)
- Étape 4 : créer un lien de base de données vers l'instance de base de données cible (p. 998)
- Étape 5 : utiliser DBMS_FILE_TRANSFER pour copier le fichier de vidage exporté vers l'instance de base de données cible (p. 999)
- Étape 6 : Utiliser DBMS_DATAPUMP pour importer le fichier de données sur l'instance de base de données cible (p. 999)
- Étape 7 : nettoyer (p. 1000)

Étape 1 : Accorder des privilèges à l'utilisateur sur l'instance de base de données cible Amazon RDS

Pour accorder des privilèges à l'utilisateur sur l'instance cible RDS, procédez comme suit :

1. Utilisez SQL Plus ou Oracle SQL Developer pour vous connecter à l'instance de base de données Oracle cible Amazon RDS vers laquelle les données seront importées. Connectez-vous à l'utilisateur principal Amazon RDS. Pour plus d'informations sur la connexion à votre instance de base de données, consultez Connexion à une instance de base de données Oracle (p. 961).
2. Créez les espaces de table requis avant d'importer les données. Pour de plus amples informations, veuillez consulter Création et dimensionnement des espaces de table (p. 1116).
3. Si le compte d'utilisateur dans lequel les données seront importées n'existe pas, créez-en un et accordez-lui les autorisations et rôles nécessaires. Si vous importez des données avec plusieurs schémas d'utilisateur, créez chaque compte d'utilisateur et accordez-lui les privilèges et rôles nécessaires.

   Par exemple, les commandes suivantes créent un utilisateur et lui accordent les autorisations et rôles nécessaires pour importer les données dans le schéma de celui-ci :

   ```
   CREATE USER schema_1 IDENTIFIED BY <password>;
   GRANT CREATE SESSION, RESOURCE TO schema_1;
   ALTER USER schema_1 QUOTA 100M ON users;
   ```

   Cet exemple montre comment accorder au nouvel utilisateur le privilège `CREATE SESSION` et le rôle `RESOURCE`. Des privilèges et rôles supplémentaires peuvent être requis en fonction des objets de la base de données que vous allez importer.

   > **Note**
   >
   > Remplacez *`schema_1`* par le nom de votre schéma dans cette étape et dans les étapes suivantes.

Étape 2 : Accorder des privilèges à l'utilisateur sur la base de données source

Utilisez SQL*Plus ou Oracle SQL Developer pour vous connecter à l'instance Oracle qui contient les données à importer. Le cas échéant, créez un compte utilisateur et accordez les autorisations nécessaires.

> **Note**
>
> Si la base de données source est une instance Amazon RDS, vous pouvez ignorer cette étape. Vous allez utiliser votre compte d'utilisateur principal Amazon RDS pour effectuer l'exportation.

Les commandes suivantes créent un nouvel utilisateur et accordent les autorisations nécessaires.

```
CREATE USER export_user IDENTIFIED BY <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;
```

Étape 3 : utiliser DBMS_DATAPUMP pour créer un fichier de vidage

Utilisez SQL Plus ou Oracle SQL Developer pour vous connecter à l'instance Oracle source avec un utilisateur administrateur ou avec l'utilisateur créé à l'étape 2. Si la base de données source est une instance de base de données Amazon RDS, connectez-vous avec l'utilisateur principal Amazon RDS. Ensuite, employez l'utilitaire Oracle Data Pump pour créer un fichier de vidage.

Le script suivant crée un fichier de vidage appelé sample.dmp dans le répertoire `DATA_PUMP_DIR`.

```
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.START_JOB(v_hdnl);
END;
/
```

Note

Les tâches de vidage de données sont démarrées de façon asynchrone. Pour obtenir des informations sur la surveillance d'une tâche Data Pump, veuillez consulter Monitoring Job Status dans la documentation Oracle. Vous pouvez afficher le contenu du journal d'exportation à l'aide de la procédure `rdsadmin.rds_file_util.read_text_file`. Pour de plus amples informations, consultez Lecture de fichiers dans un répertoire d'instance de base de données (p. 1166).

Étape 4 : créer un lien de base de données vers l'instance de base de données cible

Créez un lien de base de données entre votre instance source et votre instance de base de données cible. Notez que votre instance Oracle locale doit avoir une connectivité réseau à l'instance de base de données pour créer un lien de base de données et transférer votre fichier de vidage.

Exécutez cette étape en étant connecté au même compte d'utilisateur qu'à l'étape précédente.

Si vous créez un lien de base de données entre deux instances de bases de données dans un même VPC ou dans des VPC appairés, un itinéraire valide doit exister entre les deux instances de bases de données. Le groupe de sécurité de chaque instance de base de données doit autoriser le trafic entrant dans l'autre instance de base de données et le trafic sortant de cette instance. Les règles entrantes et sortantes des

groupes de sécurité peuvent faire référence à des groupes de sécurité à partir du même VPC ou d'un VPC appairé. Pour plus d'informations, consultez Réglage des liens de base de données pour une utilisation avec les instances de base de données dans un VPC (p. 1123).

La commande suivante crée un lien de base de données appelé `to_rds` qui se connecte à l'utilisateur principal Amazon RDS au niveau de l'instance de base de données cible :

```
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>)))';
```

Étape 5 : utiliser DBMS_FILE_TRANSFER pour copier le fichier de vidage exporté vers l'instance de base de données cible

Utilisez `DBMS_FILE_TRANSFER` pour copier le fichier de vidage depuis l'instance de base de données source vers l'instance de base de données cible. Le script suivant copie un fichier de vidage appelé sample.dmp depuis l'instance source vers un lien de base de données cible appelé to_rds (créé dans l'étape précédente) :

```
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;
/
```

Étape 6 : Utiliser DBMS_DATAPUMP pour importer le fichier de données sur l'instance de base de données cible

Utilisez Oracle Data Pump pour importer le schéma dans l'instance de base de données. Notez que des options supplémentaires comme METADATA_REMAP pourraient être obligatoires.

Connectez-vous à l'instance de base de données avec le compte d'utilisateur principal Amazon RDS pour effectuer l'importation.

```
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**
>
> Les tâches de vidage de données sont démarrées de façon asynchrone. Pour obtenir des informations sur la surveillance d'une tâche Data Pump, veuillez consulter Monitoring Job Status dans la documentation Oracle. Vous pouvez afficher le contenu du journal d'importation à l'aide de la procédure `rdsadmin.rds_file_util.read_text_file`. Pour de plus amples informations, consultez Lecture de fichiers dans un répertoire d'instance de base de données (p. 1166).

Vous pouvez vérifier l'importation des données en consultant les table de l'utilisateur sur l'instance de base de données. Par exemple, la requête suivante renvoie le nombre de tables de *`schema_1`*.

```
SELECT COUNT(*) FROM DBA_TABLES WHERE OWNER='SCHEMA_1';
```

Étape 7 : nettoyer

Après l'importation des données, vous pouvez supprimer les fichiers que vous ne souhaitez plus conserver. Vous pouvez répertorier les fichiers de `DATA_PUMP_DIR` à l'aide de la commande suivante.

```
SELECT * FROM TABLE(rdsadmin.rds_file_util.listdir('DATA_PUMP_DIR')) ORDER BY MTIME;
```

Pour supprimer des fichiers dont vous n'avez plus besoin dans `DATA_PUMP_DIR`, utilisez la commande suivante :

```
EXEC UTL_FILE.FREMOVE('DATA_PUMP_DIR','<file name>');
```

Par exemple, la commande suivante supprime le fichier appelé `"sample_copied.dmp"`.

```
EXEC UTL_FILE.FREMOVE('DATA_PUMP_DIR','sample_copied.dmp');
```

Utilitaires Oracle Export/Import

Les utilitaires Oracle Export/Import sont parfaitement adaptés aux migrations lorsque le volume de données est faible et que les types de données comme les nombres flottants et les doubles ne sont pas obligatoires. Le processus d'importation crée les objets du schéma pour que vous n'ayez pas à exécuter un script pour les créer au préalable, ce qui rend ce processus parfaitement adapté aux bases de données à petites tables. L'exemple suivant montre comment ces utilitaires peuvent être utilisés pour exporter et importer des tables spécifiques.

Pour télécharger les utilitaires d'exportation et d'importation d'Oracle, accédez à http://www.oracle.com/technetwork/database/enterprise-edition/downloads/index.html.

Exportez les tables depuis la base de données source en utilisant la commande ci-dessous. Remplacez le nom d'utilisateur/mot de passe, le cas échéant.

```
exp cust_dba@ORCL FILE=exp_file.dmp TABLES=(tab1,tab2,tab3) LOG=exp_file.log
```

Le processus d'exportation crée un fichier de vidage binaire qui contient le schéma et les données pour les tables spécifiées. À présent, ce schéma et ces données peuvent être importés dans une base de données cible en utilisant la commande suivante :

```
imp cust_dba@targetdb FROMUSER=cust_schema TOUSER=cust_schema \
TABLES=(tab1,tab2,tab3) FILE=exp_file.dmp LOG=imp_file.log
```

Il existe d'autres variations des commandes Export et Import qui pourraient être parfaitement adaptées à vos besoins. Pour plus d'informations, consultez la documentation d'Oracle.

Oracle SQL*Loader

Oracle SQL*Loader est parfaitement adapté aux bases de données volumineuses qui contiennent un nombre limité d'objets. Étant donné que le processus d'importation depuis une base de données source et de chargement vers une base de données cible est propre au schéma, l'exemple suivant crée des exemples d'objets de schéma, les exporte depuis une source et les charge ensuite dans une base de données cible.

Pour télécharger Oracle SQL*Loader, accédez à http://www.oracle.com/technetwork/database/enterprise-edition/downloads/index.html.

1. Créez un exemple de table source en utilisant la commande ci-dessous.

```
CREATE TABLE customer_0 TABLESPACE users
   AS (SELECT ROWNUM id, o.*
       FROM   ALL_OBJECTS o, ALL_OBJECTS x
       WHERE  ROWNUM <= 1000000);
```

2. Sur l'instance Amazon RDS cible, créez une table de destination qui est utilisée pour charger les données. La clause `WHERE 1=2` permet de copier la structure de `ALL_OBJECTS` sans copier aucune ligne.

```
CREATE TABLE customer_1 TABLESPACE users
  AS (SELECT 0 AS ID, OWNER, OBJECT_NAME, CREATED
      FROM   ALL_OBJECTS
      WHERE  1=2);
```

3. Les données sont exportées depuis la base de données source vers un fichier plat avec des délimiteurs. Cet exemple utilise SQL*Plus à cette fin. Pour vos données, vous pourrez avoir besoin de générer un script qui exporte tous les objets dans la base de données.

```
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. Vous devez créer un fichier de contrôle pour décrire les données. Encore une fois, en fonction de vos donnés, vous devez créer un script qui réalise cette étape.

```
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"
```

```
)
```

Le cas échéant, copiez les fichiers générés par le code précédent vers une zone tampon comme une instance Amazon EC2.

5. Enfin, importez les données en utilisant SQL*Loader avec le nom d'utilisateur et le mot de passe adaptés pour la base de données cible.

```
sqlldr cust_dba@targetdb CONTROL=sqlldr_1.ctl BINDSIZE=10485760 READSIZE=10485760
 ROWS=1000
```

Vues matérialisées Oracle

Vous pouvez également utiliser la réplication des vues matérialisées Oracle pour migrer efficacement des ensembles de données volumineux. La réplication vous permet de garantir la synchronisation permanente entre les tables cible et source, afin que le transfert réel vers Amazon RDS puisse être réalisé ultérieurement, le cas échéant. La réplication est configurée à l'aide d'un lien de base de données depuis l'instance Amazon RDS vers la base de données source.

Une exigence pour les vues matérialisées est d'autoriser l'accès depuis la base de données cible vers la base de données source. Dans l'exemple suivant, l'accès aux règles était activé sur la base de données source pour autoriser la base de données cible Amazon RDS à se connecter à la source via SQLNet.

1. Créez un compte utilisateur sur les instances Amazon RDS source et cible que vous pouvez authentifier avec le même mot de passe.

```
CREATE USER dblink_user IDENTIFIED BY <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. Créez un lien de base de données depuis l'instance Amazon RDS cible vers l'instance source en utilisant le nouveau dblink_user créé.

```
CREATE DATABASE LINK remote_site
  CONNECT TO dblink_user IDENTIFIED BY <password>
  USING '(description=(address=(protocol=tcp) (host=<myhost>)
    (port=<listener port>)) (connect_data=(sid=<sourcedb sid>)))';
```

3. Testez le lien :

```
SELECT * FROM V$INSTANCE@remote_site;
```

4. Créez un exemple de table avec une clé primaire et un journal des vues matérialisées sur l'instance source.

```
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. Sur l'instance Amazon RDS cible, créez une vue matérialisée.

```
CREATE MATERIALIZED VIEW customer_0
  BUILD IMMEDIATE REFRESH FAST
  AS (SELECT *
      FROM   cust_dba.customer_0@remote_site);
```

6. Sur l'instance Amazon RDS cible, actualisez la vue matérialisée.

```
EXEC DBMS_MV.REFRESH('CUSTOMER_0', 'f');
```

7. Supprimez la vue matérialisée et incluez la clause PRESERVE TABLE pour conserver la table de conteneur de vue matérialisée et son contenu.

```
DROP MATERIALIZED VIEW customer_0 PRESERVE TABLE;
```

   La table conservée a le même nom que la vue matérialisée supprimée.

Utilisation des réplicas Oracle pour Amazon RDS

Pour configurer la réplication entre les instances de base de données Oracle, vous pouvez créer des bases de données de réplicas.

Rubriques

- Présentation des réplicas Oracle (p. 1003)
- Exigences de réplica pour Oracle (p. 1004)
- Préparation de la création d'un réplica Oracle (p. 1005)
- Création d'un réplica Oracle en mode monté (p. 1007)
- Modification du mode réplica Oracle (p. 1008)
- Dépannage des réplicas Oracle (p. 1009)

Présentation des réplicas Oracle

Une base de données de réplicas Oracle est montée ou en lecture seule. Un réplica Oracle en lecture seule est appelé réplica en lecture. Un réplica Oracle en mode monté est appelé réplica monté.

Réplicas en lecture seule et montés

Lorsque vous créez ou modifiez un réplica Oracle, vous pouvez le placer dans l'un des modes suivants :

- Lecture seule Il s'agit de l'option par défaut. Active Data Guard transmet et applique les modifications de la base de données source à toutes les bases de données de réplicas en lecture.

  Vous pouvez créer jusqu'à cinq réplicas en lecture à partir d'une seule instance de base de données source. Pour de plus amples informations sur les réplicas en lecture qui s'appliquent à tous les moteurs de base de données, veuillez consulter Utilisation des réplicas en lecture (p. 275). Pour de plus amples informations sur Oracle Data Guard, veuillez consulter Oracle Data Guard Concepts and Administration dans la documentation Oracle.
- Monté. Dans ce cas, la réplication utilise Oracle Data Guard, mais la base de données du réplica n'accepte pas les connexions utilisateur. L'utilisation principale des réplicas montés est la reprise après sinistre inter-région.

Un réplica monté ne peut pas servir de charge de travail en lecture seule. Le réplica monté supprime les fichiers de journalisation archivés après leur application, quelle que soit la stratégie de conservation des journaux archivés.

Vous pouvez créer une combinaison de réplicas de base de données montés et en lecture seule pour la même instance de base de données source. Vous pouvez changer un réplica en lecture seule en mode monté ou changer un réplica monté en mode lecture seule. Dans les deux cas, la base de données Oracle conserve le paramètre de conservation des journaux archivés.

Pannes pendant la réplication

Lorsque vous créez un réplica Oracle, aucune panne ne se produit pour l'instance de base de données source. Amazon RDS prend un instantané de l'instance de base de données source. Cet instantané devient le réplica. Amazon RDS définit les paramètres et autorisations nécessaires pour la base de données source et le réplica sans interruption de service. De même, si vous supprimez un réplica, aucune panne ne se produit.

Exigences de réplica pour Oracle

Avant de créer un réplica Oracle, vérifiez les conditions requises suivantes.

Exigences de version et de licence pour les réplicas Oracle

Avant de créer un réplica Oracle, vérifiez la version et les conditions de licence requises :

- Si le réplica est en mode lecture seule, assurez-vous que vous disposez d'une licence Active Data Guard. Si vous placez le réplica en mode monté, vous n'avez pas besoin d'une licence Active Data Guard. Seul le moteur Oracle DB prend en charge les réplicas montés.
- Les réplicas en lecture Oracle sont uniquement disponibles sur le moteur Oracle Enterprise Edition (EE).
- Les réplicas en lecture Oracle sont uniquement disponibles pour la version Oracle 12.1.0.2.v10 et les versions 12.1 supérieures, pour toutes les versions 12.2, toutes les versions 18 et toutes les versions 19.
- Les réplicas Oracle sont disponibles pour les instances de base de données uniquement sur la plateforme EC2-VPC.
- Les réplicas Oracle sont disponibles pour les instances de base de données exécutées uniquement sur des classes d'instance de base de données avec deux vCPU ou plus. Une instance de base de données source ne peut pas utiliser la classe de micro-instance db.t3.
- La version du moteur Oracle DB de l'instance de base de données source et tous ses réplicas doivent être identiques. Amazon RDS met à niveau les réplicas immédiatement après la mise à niveau de l'instance de base de données source, quelle que soit la fenêtre de maintenance d'un réplica. Pour les mises à niveau majeures de versions de réplicas inter-régions, Amazon RDS effectue automatiquement les opérations suivantes :
  - Génère un groupe d'options pour la version cible
  - Copie toutes les options et tous les paramètres d'option du groupe d'options d'origine vers le nouveau groupe d'options
  - Associe le réplica en lecture inter-région mis à niveau au nouveau groupe d'options

  Pour de plus amples informations sur la mise à niveau de la version du moteur de base de données, veuillez consulter la section Mise à niveau du moteur de base de données Oracle (p. 975).

Exigences d'option pour les réplicas Oracle

Avant de créer un réplica pour Oracle, vérifiez les conditions requises pour les groupes d'options :

- Si votre réplica Oracle se trouve dans la même région AWS que son instance de base de données source, assurez-vous qu'il appartient au même groupe d'options que l'instance de base de données source. Les modifications apportées au groupe d'options source ou à l'appartenance au groupe d'options source sont propagées aux réplicas. Ces modifications sont appliquées aux réplicas immédiatement après leur application à l'instance de base de données source, quelle que soit la fenêtre de maintenance du réplica.

  Pour de plus amples informations sur les groupes d'options, veuillez consulter Utilisation de groupes d'options (p. 209).
- Lorsque vous créez un réplica Oracle inter-région, Amazon RDS crée un groupe d'options qui lui est dédié.

  Vous ne pouvez pas supprimer un réplica Oracle inter-région du groupe d'options qui lui est dédié. Aucune autre instance de base de données ne peut utiliser le groupe d'options dédié à un réplica Oracle inter-région.

  Vous pouvez uniquement ajouter ou supprimer les options non répliquées suivantes d'un groupe d'options dédié :
  - `NATIVE_NETWORK_ENCRYPTION`
  - `OEM`
  - `OEM_AGENT`
  - `SSL`

  Pour ajouter d'autres options à un réplica Oracle inter-région, ajoutez-les au groupe d'options de l'instance de base de données source. L'option est également installée sur tous les réplicas de l'instance de base de données source. Pour les options sous licence, assurez-vous qu'il existe suffisamment de licences pour les réplicas.

  Lorsque vous promouvez un réplica Oracle inter-région, le réplica promu se comporte de la même façon que d'autres instances de bases de données Oracle, y compris pour la gestion de ses options. Vous pouvez promouvoir un réplica explicitement ou implicitement en supprimant son instance de base de données source.

  Pour de plus amples informations sur les groupes d'options, veuillez consulter Utilisation de groupes d'options (p. 209).

Exigences diverses pour les réplicas Oracle

Avant de créer un réplica Oracle, vérifiez les conditions diverses suivantes :

- Si une instance de base de données est une source pour un ou plusieurs réplicas inter-région, la base de données source conserve ses journaux redo archivés jusqu'à ce qu'ils soient appliqués dans tous les réplicas inter-régions. Les journaux redo archivés peuvent entraîner une augmentation de la consommation de stockage.
- Un déclencheur de connexion sur une instance principale doit permettre l'accès à l'utilisateur `RDS_DATAGUARD` et à tout utilisateur dont la valeur `AUTHENTICATED_ENTITY` est `RDS_DATAGUARD` ou `rdsdb`. En outre, le déclencheur ne doit pas définir le schéma actuel pour l'utilisateur `RDS_DATAGUARD`.
- Pour éviter de bloquer les connexions du processus de l’agent Data Guard, n'activez pas les sessions restreintes. Pour plus d'informations sur les sessions restreintes, consultez Activation et désactivation de sessions restreintes (p. 1105).

Préparation de la création d'un réplica Oracle

Avant de commencer à utiliser votre réplica, effectuez les tâches suivantes.

Rubriques

- Planification des sauvegardes automatiques (p. 1006)
- Activation du mode de journalisation (p. 1006)
- Modification de votre configuration de journalisation (p. 1006)
- Définition du paramètre MAX_STRING_SIZE (p. 1006)
- Planification des ressources de calcul et de stockage (p. 1007)

Planification des sauvegardes automatiques

Avant qu'une instance de base de données puisse être utilisée comme instance de bases de données source, vous devez activer les sauvegardes automatiques sur l'instance de base de données source. Pour savoir comment effectuer cette procédure, veuillez consulter Activation des sauvegardes automatiques (p. 321).

Activation du mode de journalisation

Nous vous recommandons d'activer le mode de journalisation forcée. En mode de journalisation forcée, la base de données Oracle écrit des enregistrements de journalisation même lorsque `NOLOGGING` est utilisée avec des instructions DDL (Data Definition Language).

Pour activer le mode de journalisation forcée

1. Connectez-vous à votre base de données Oracle à l'aide d'un outil client tel que SQL Developer.
2. Activez le mode de journalisation forcée en exécutant la procédure suivante.

```
exec rdsadmin.rdsadmin_util.force_logging(p_enable => true);
```

Pour de plus amples informations sur cette procédure, veuillez consulter Configuration du mode FORCE LOGGING (p. 1129).

Modification de votre configuration de journalisation

Si vous souhaitez modifier votre configuration de journalisation, nous vous recommandons de terminer les modifications avant de faire d'une instance de base de données la source des réplicas. En outre, nous vous recommandons de ne pas modifier la configuration de journalisation après avoir créé les réplicas. En raison des modifications, la configuration de la journalisation redo en ligne peut être désynchronisée par rapport à la configuration de la journalisation en attente.

Modifiez la configuration de journalisation d'une instance DB à l'aide des procédures Amazon RDS `rdsadmin.rdsadmin_util.add_logfile` et `rdsadmin.rdsadmin_util.drop_logfile`. Pour de plus amples informations, veuillez consulter Ajout de journaux redo en ligne (p. 1131) et Suppression de journaux redo en ligne (p. 1132).

Définition du paramètre MAX_STRING_SIZE

Avant de créer un réplica Oracle, assurez-vous que le paramètre `MAX_STRING_SIZE` est le même sur l'instance de base de données source et sur le réplica. Pour cela, vous devez les associer au même groupe de paramètres. Si vous avez différents groupes de paramètres pour la source et le réplica, vous pouvez définir `MAX_STRING_SIZE` sur la même valeur. Pour de plus amples informations sur ce paramètre, veuillez consulter Activation des types de données étendus pour une nouvelle instance de base de données (p. 960).

Planification des ressources de calcul et de stockage

Assurez-vous que l'instance de base de données source et ses réplicas sont dimensionnés correctement, en termes de calcul et de stockage, en fonction de leur charge opérationnelle. Si un réplica atteint la capacité de calcul, de réseau ou de ressources de stockage, le réplica cesse de recevoir ou d'appliquer des modifications à partir de sa source. Amazon RDS pour Oracle n'intervient pas pour atténuer le décalage de réplica élevé entre une instance de base de données source et ses réplicas. Vous pouvez modifier les ressources de stockage et d'UC d'un réplica indépendamment de sa source et d'autres réplicas.

Création d'un réplica Oracle en mode monté

Par défaut, les réplicas Oracle sont en lecture seule. Pour créer un réplica en mode monté, utilisez la console, l'AWS CLI ou l'API RDS.

Console

Pour créer un réplica monté à partir d'une instance de base de données Oracle source

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez l'instance de base de données Oracle que vous souhaitez utiliser comme source pour un réplica monté.
4. Sous Actions, choisissez Créer un réplica.
5. Pour le Mode réplica, choisissez Monté.
6. Choisissez les paramètres que vous souhaitez utiliser. Sous Identifiant de l'instance DB, saisissez un nom pour le réplica en lecture. Ajustez les autres paramètres selon les besoins.
7. Pour Régions, choisissez la région dans laquelle le réplica monté sera lancé.
8. Choisissez la taille de votre instance et le type de stockage. Nous vous recommandons d'utiliser le même type de stockage et la même classe d'instance de base de données que l'instance de base de données source pour le réplica en lecture.
9. Pour Déploiement Multi-AZ, choisissez Créer une instance de secours pour créer une instance de secours de votre réplica dans une autre zone de disponibilité pour la prise en charge du basculement pour le réplica monté. La création de votre réplica monté en tant qu'instance de base de données multi-AZ est indépendante du fait que la base de données source soit ou non une instance de base de données multi-AZ.
10. Choisissez les autres paramètres que vous voulez utiliser.
11. Choisissez Créer un réplica.

Dans la page Bases de données, le réplica monté a le rôle Réplica.

AWS CLI

Pour créer un réplica Oracle en mode monté, définissez `--replica-mode` sur `mounted` dans la commande AWS CLI create-db-instance-read-replica.

Example

Pour Linux, macOS ou Unix :

```
aws rds create-db-instance-read-replica \
```

```
    --db-instance-identifier myreadreplica \
    --source-db-instance-identifier mydbinstance \
    --replica-mode mounted
```

Pour Windows :

```
aws rds create-db-instance-read-replica ^
    --db-instance-identifier myreadreplica ^
    --source-db-instance-identifier mydbinstance ^
    --replica-mode mounted
```

Pour modifier un réplica en lecture seule en état monté, définissez `--replica-mode` sur `mounted` dans la commande AWS CLI modify-db-instance. Pour placer un réplica monté en mode lecture seule, définissez `--replica-mode` sur `read-only`.

API RDS

Pour créer un réplica Oracle en mode monté, spécifiez `ReplicaMode=mounted` dans l'opération API RDS CreateDBInstanceReadReplica.

```
https://rds.amazonaws.com/
 ?Action=CreateDBInstanceReadReplica
 &DBInstanceIdentifier=myreadreplica
 &SourceDBInstanceIdentifier=mydbinstance
 &Version=2012-01-15
 &SignatureVersion=2
 &SignatureMethod=HmacSHA256
 &Timestamp=2012-01-20T22%3A06%3A23.624Z
 &AWSAccessKeyId=<AWS Access Key ID>
 &Signature=<Signature>
 &ReplicaMode=mounted
```

Modification du mode réplica Oracle

Pour modifier le mode de réplica d'un réplica existant, utilisez la console, AWS CLI ou l'API RDS. Lorsque vous passez en mode monté, le réplica déconnecte toutes les connexions actives. Lorsque vous passez en mode lecture seule, Amazon RDS initialise Active Data Guard.

L'opération de modification peut prendre quelques minutes. Au cours de l'opération, l'état de l'instance de base de données passe à en cours de modification. Pour de plus amples informations sur les modifications d'état, veuillez consulter Statut d'instance de bases de données (p. 386).

Console

Pour changer le mode réplica d'un réplica Oracle de monté en lecture seule

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez la base de données de réplica montée.
4. Sélectionnez Modify.
5. Pour le mode Réplica, choisissez Lecture seule.
6. Choisissez les autres paramètres que vous souhaitez modifier.
7. Choisissez Continue.

8. Pour Scheduling of Modifications (Planification des modifications), choisissez Appliquer immédiatement.
9. Choisissez Modifier l'instance DB.

AWS CLI

Pour changer un réplica en lecture en mode monté, définissez `--replica-mode` sur `mounted` dans la AWS CLI commande modify-db-instance. Pour changer un réplica monté en mode lecture seule, définissez `--replica-mode` sur `read-only`.

Example

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier myreadreplica \
    --replica-mode mode
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier myreadreplica ^
    --replica-mode mode
```

API RDS

Pour changer un réplica en lecture seule en mode monté, définissez `ReplicaMode=mounted` dans ModifyDBInstance. Pour changer un réplica monté en mode lecture seule, définissez `ReplicaMode=read-only`.

```
https://rds.amazonaws.com/
 ?Action=ModifyDBInstance
 &DBInstanceIdentifier=myreadreplica
 &SourceDBInstanceIdentifier=mysourcedb
 &Version=2012-01-15
 &SignatureVersion=2
 &SignatureMethod=HmacSHA256
 &Timestamp=2012-01-20T22%3A06%3A23.624Z
 &AWSAccessKeyId=<AWS Access Key ID>
 &Signature=<Signature>
 &ReplicaMode=mode
```

Dépannage des réplicas Oracle

Pour surveiller le décalage de réplication dans Amazon CloudWatch, affichez la métrique Amazon RDS `ReplicaLag`. Pour de plus amples informations sur la durée du retard de réplication, veuillez consulter Supervision de la réplication en lecture (p. 291).

Si le retard de réplication est trop long, vous pouvez interroger les vues suivantes afin d'obtenir des informations sur le retard :

- `V$ARCHIVED_LOG` – Indique quelles validations ont été appliquées au réplica en lecture.
- `V$DATAGUARD_STATS` – Indique la répartition détaillée des composants qui font partie de la métrique `replicaLag`.
- `V$DATAGUARD_STATUS` – Indique la sortie de journal des processus de réplication internes d'Oracle.

Jeux de caractères Oracle pris en charge dans Amazon RDS

Amazon RDS pour Oracle prend en charge deux types de jeux de caractères : le jeu de caractères de base de données et le jeu de caractères national.

Jeu de caractères de base de données

Le jeu de caractères de base de données Oracle est utilisé dans les types de données `CHAR`, `VARCHAR2` et `CLOB`. La base de données utilise également ce jeu de caractères pour les métadonnées telles que les noms de table, les noms de colonne et les instructions SQL. Le jeu de caractères de base de données Oracle est généralement appelé jeu de caractères de base de données.

Vous définissez le jeu de caractères lorsque vous créez une instance de base de données. Vous ne pouvez pas modifier le jeu de caractères de base de données après avoir créé la base de données.

Jeux de caractères de base de données pris en charge

La table suivante répertorie les jeux de caractères de base de données Oracle qui sont pris en charge dans Amazon RDS. Vous pouvez utiliser une valeur depuis ce tableau avec le paramètre `--character-set-name` de l'AWS CLI create-db-instance ou avec le paramètre `CharacterSetName` de l'opération d'API Amazon RDS CreateDBInstance.

Valeur	Description
AL32UTF8	Jeu de caractères universel UTF-8 Unicode 5.0 (par défaut)
AR8ISO8859P6	ISO 8859-6 Latis.o.rabe
AR8MSWIN1256	Page de codes Microsoft Windows 1256 8 bits Latis.o.rabe
BLT8ISO8859P13	ISO 8859-13 Baltique
BLT8MSWIN1257	Page de codes Microsoft Windows 1257 8 bits Baltique
CL8ISO8859P5	ISO 88559-5 Latin/Cyrillique
CL8MSWIN1251	Page de codes Microsoft Windows 1251 8 bits Latin/Cyrillique
EE8ISO8859P2	ISO 8859-2 Europe de l'Est
EL8ISO8859P7	ISO 8859-7 Latin/Grec
EE8MSWIN1250	Page de codes Microsoft Windows 1250 8 bits Europe de l'Est
EL8MSWIN1253	Page de codes Microsoft Windows 1253 8 bits Latin/Grec
IW8ISO8859P8	ISO 8859-8 Latin/Hébreu
IW8MSWIN1255	Page de codes Microsoft Windows 1255 8 bits Latin/Hébreu

Valeur	Description
JA16EUC	EUC 24 bits Japonais
JA16EUCTILDE	Même chose que JA16EUC, sauf pour le mapping du trait d'union en esse et du tilde vers et depuis Unicode
JA16SJIS	Shift-JIS 16 bits Japonais
JA16SJISTILDE	Même chose que JA16SJIS sauf pour le mapping du trait d'union en esse et du tilde vers et depuis Unicode
KO16MSWIN949	Page de codes Microsoft Windows 949 Coréen
NE8ISO8859P10	ISO 8859-10 Europe du Nord
NEE8ISO8859P4	ISO 8859-4 Europe du Nord et du Nord-Est
TH8TISASCII	Thai Industrial Standard 620-2533-ASCII 8 bits
TR8MSWIN1254	Page de codes Microsoft Windows 1254 8 bits Turc
US7ASCII	ASCII 7 bits Américain
UTF8	Jeu de caractères universel UTF-8 Unicode 3.0, compatible CESU-8
VN8MSWIN1258	Page de codes Microsoft Windows 1258 8 bits Vietnamien
WE8ISO8859P1	ISO 8859 Partie 1 Europe de l'Ouest 8 bits
WE8ISO8859P15	ISO 8859-15 Europe de l'Ouest
WE8ISO8859P9	ISO 8859-9 Europe de l'Ouest et Turc
WE8MSWIN1252	Page de codes Microsoft Windows 1252 8 bits Europe de l'Ouest
ZHS16GBK	GBK 16 bits Chinois simplifié
ZHT16HKSCS	Page de codes Microsoft Windows 950 avec jeu de caractères supplémentaire Hong Kong HKSCS-2001. La conversion de jeu de caractères est basée sur Unicode 3.0.
ZHT16MSWIN950	Page de codes Microsoft Windows 950 Chinois traditionnel
ZHT32EUC	EUC 32 bits Chinois traditionnel

Variable d'environnement NLS_LANG

Un paramètre régional est un ensemble d'informations répondant aux exigences linguistiques et culturelles qui correspondent à une langue et à un pays donnés. La définition de la variable d'environnement NLS_LANG dans l'environnement de votre client est la manière la plus simple de spécifier le comportement local du logiciel Oracle. Cette variable définit la langue et le territoire utilisés par l'application cliente et le serveur de base de données. Ils indiquent également le jeu de caractères client qui

correspond au jeu de caractères pour les données entrées ou affichées par une application cliente. Pour de plus amples informations sur NLS_LANG et les jeux de caractères, veuillez consulter What is a Character set or Code Page? (Qu'est-ce qu'un jeu de caractères ou une page de code ?) dans la documentation Oracle.

Paramètres d'initialisation NLS

Vous pouvez également définir les paramètres d'initialisation NLS (National Language Support) suivants au niveau de l'instance pour une instance de base de données Oracle dans 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

Pour plus d'informations sur la modification des paramètres d'instance, consultez Utilisation de groupes de paramètres de base de données (p. 225).

Vous pouvez définir d'autres paramètres d'initialisation NLS dans votre client SQL. Par exemple, l'instruction suivante définit le paramètre d'initialisation NLS LANGUAGE à GERMAN dans un client SQL connecté à une instance de base de données Oracle :

```
ALTER SESSION SET NLS_LANGUAGE=GERMAN;
```

Pour plus d'informations sur la connexion à une instance de base de données Oracle avec un client SQL, consultez Connexion à une instance de base de données Oracle (p. 961).

Jeu de caractères national

Le jeu de caractères national est utilisé dans les types de données `NCHAR`, `NVARCHAR2` et `NCLOB`. Le jeu de caractères national est généralement appelé jeu de caractères NCHAR. Contrairement au jeu de caractères de base de données, le jeu de caractères NCHAR n'affecte pas les métadonnées de base de données.

Le jeu de caractères NCHAR prend en charge les jeux de caractères suivants :

- AL16UTF16 (par défaut)
- UTF8

Vous pouvez spécifier l'une de ces valeurs avec le paramètre `--nchar-character-set-name` de la commande AWS CLI create-db-instance ou avec le paramètre `NcharCharacterSetName` de l'opération d'API Amazon RDS CreateDBInstance. Vous ne pouvez pas modifier le jeu de caractères national après avoir créé la base de données.

Pour de plus amples informations sur Unicode dans les bases de données Oracle, veuillez consulter Prise en charge des bases de données multilingues avec unicode dans la documentation Oracle.

Options propres aux instances de bases de données Oracle

La section suivante décrit les options ou fonctions supplémentaires, disponibles pour les instances Amazon RDS exécutant le moteur de base de données Oracle. Pour activer ces options, vous les ajoutez à un groupe d'options, puis associer celui-ci à votre instance de base de données. Pour plus d'informations, consultez Utilisation de groupes d'options (p. 209).

Certaines options nécessitent que de la mémoire supplémentaire s'exécute sur votre instance de base de données. Par exemple, Oracle Enterprise Manager Database Control utilise environ 300 Mo de RAM. Si vous activez cette option pour une petite instance de base de données, vous pourrez rencontrer des problèmes de performance liés aux contraintes de mémoire. Vous pouvez ajuster les paramètres Oracle afin que la base de données nécessite moins de RAM. Sinon, vous pouvez augmenter la taille de l'instance de base de données.

Amazon RDS prend en charge les options suivantes pour les instances de bases de données Oracle.

Option	ID d'option
Intégration Amazon S3 (p. 1014)	`S3_INTEGRATION`
Oracle Application Express (APEX) (p. 1026)	`APEX` `APEX-DEV`
Oracle Enterprise Manager (p. 1037)	`OEM` `OEM_AGENT`
Oracle Java Virtual Machine (p. 1052)	`JVM`
Oracle Label Security (p. 1054)	`OLS`
Oracle Locator (p. 1057)	`LOCATOR`
Oracle Multimedia (p. 1060)	`MULTIMEDIA`
Oracle NNE (Native Network Encryption) (p. 1062)	`NATIVE_NETWORK_ENCRYPTION`
Oracle OLAP (p. 1066)	`OLAP`
Oracle Secure Sockets Layer (SSL) (p. 1068)	`SSL`
Oracle Spatial (p. 1077)	`SPATIAL`
Oracle SQLT (p. 1080)	`SQLT`
Oracle Statspack (p. 1085)	`STATSPACK`
Fuseau horaire Oracle (p. 1088)	`Timezone`
Oracle Transparent Data Encryption (p. 1091)	`TDE`
Oracle UTL_MAIL (p. 1093)	`UTL_MAIL`
Oracle XML DB (p. 1096)	`XMLDB`

Intégration Amazon S3

Vous pouvez transférer des fichiers entre un Amazon RDS pour une instance de base de données Oracle et un compartiment Amazon S3. Vous pouvez utiliser l'intégration Amazon S3 avec les fonctionnalités Oracle telles que Data Pump. Par exemple, vous pouvez télécharger des fichiers Data Pump de Amazon S3 vers l'hôte d'instance de base de données.

> **Note**
>
> L'instance de base de données et le compartiment Amazon S3 doivent se situer dans la même région AWS.

Rubriques

- Conditions préalables à l'intégration de Amazon RDS Oracle avec Amazon S3 (p. 1014)
- Ajout de l'option d'intégration Amazon S3 (p. 1019)
- Transfert de fichiers entre Amazon RDS pour Oracle et un compartiment Amazon S3 (p. 1020)
- Suppression de l'option d'intégration Amazon S3 (p. 1026)

Conditions préalables à l'intégration de Amazon RDS Oracle avec Amazon S3

Pour utiliser l'intégration de Amazon RDS pour Oracle avec Amazon S3, l'instance de base de données Amazon RDS doit avoir accès à un compartiment Amazon S3. Pour cela, créez une stratégie AWS Identity and Access Management (IAM) et un rôle IAM. Le Amazon VPC utilisé par votre instance de base de données n'a pas besoin de fournir d'accès aux points de terminaison Amazon S3.

> **Note**
>
> Pour ajouter un rôle à une instance de base de données, le statut de l'instance de base de données doit être `available`.

Console

Pour créer une stratégie IAM afin d'autoriser l'accès Amazon RDS à un compartiment Amazon S3

1. Ouvrez IAM Management Console.
2. Dans le panneau de navigation, choisissez Stratégies.
3. Choisissez Créer une stratégie.
4. Sous l'onglet Visual editor (Éditeur visuel), choisissez Choose a service (Choisir un service), puis S3.
5. Choisissez Expand all (Développer tout) sous Actions, puis choisissez les autorisations de compartiment et d'objet nécessaires à la stratégie IAM.

   Incluez les actions appropriées dans la stratégie en fonction du type d'accès requis :

   - `GetObject` – Obligatoire pour transférer les fichiers d'un compartiment Amazon S3 vers Amazon RDS.
   - `ListBucket` – Obligatoire pour transférer les fichiers d'un compartiment Amazon S3 vers Amazon RDS.
   - `PutObject` – Obligatoire pour transférer les fichiers de Amazon RDS vers un compartiment Amazon S3.

   Les autorisations d'objet sont des autorisations pour les opérations d'objet dans Amazon S3. Elles doivent être accordées pour les objets d'un compartiment et non pour le compartiment lui-même.

Pour plus d'informations sur les autorisations liées aux opérations d'objet dans Amazon S3, consultez Autorisations pour des opérations d'objet.

6. Choisissez Resources (Ressources), puis Add ARN (Ajouter un ARN) pour bucket (compartiment).
7. Dans la boîte de dialogue Add ARN(s) (Ajouter un ou des ARN), fournissez les détails sur votre ressource, puis choisissez Add (Ajouter).

   Spécifiez le compartiment Amazon S3 auquel autoriser l'accès. Par exemple, si vous voulez autoriser Amazon RDS à accéder au compartiment Amazon S3 nommé `example-bucket`, définissez la valeur d'ARN sur `arn:aws:s3:::example-bucket`.
8. Si la ressource object (objet) est répertoriée, choisissez Add ARN (Ajouter un ARN) pour object (objet).
9. Dans la boîte de dialogue Add ARN(s) (Ajouter un ou des ARN), fournissez les détails sur votre ressource.

   Pour le compartiment Amazon S3, spécifiez le compartiment Amazon S3 auquel autoriser l'accès. Pour l'objet, vous pouvez choisir Any (Tous) pour accorder des autorisations à tous les objets du compartiment.

   > **Note**
   >
   > Vous pouvez affecter à Amazon Resource Name (ARN) une valeur d'ARN plus spécifique afin d'autoriser Amazon RDS à accéder uniquement à des fichiers ou des dossiers spécifiques dans un compartiment Amazon S3. Pour plus d'informations sur la définition d'une stratégie d'accès pour Amazon S3, consultez Gestion des autorisations d'accès de vos ressources Amazon S3.
10. Choisissez éventuellement Add additional permissions (Ajouter des autorisations supplémentaires) pour ajouter un autre compartiment Amazon S3 à la stratégie, puis répétez les étapes précédentes pour le compartiment.

    > **Note**
    >
    > Vous pouvez répéter ces étapes pour ajouter les instructions d'autorisation de compartiment correspondantes à votre stratégie pour chaque compartiment Amazon S3 auquel Amazon RDS doit accéder. Si vous le souhaitez, vous pouvez également accorder l'accès à tous les compartiments et à tous les objets dans Amazon S3.
11. Choisissez Examiner une stratégie.
12. Dans Name (Name), attribuez un nom à votre stratégie IAM, par exemple `rds-s3-integration-policy`. Vous utilisez ce nom lorsque vous créez un rôle IAM à associer à votre cluster de base de données. Vous pouvez également ajouter une valeur Description facultative.
13. Choisissez Créer une stratégie.

Pour créer un rôle IAM afin d'autoriser Amazon RDS à accéder à un compartiment Amazon S3

1. Dans le volet de navigation, choisissez Rôles.
2. Sélectionnez Créer un rôle.
3. Pour Service AWS, choisissez RDS.
4. Pour Sélectionner votre cas d'utilisation, choisissez RDS – Ajouter un rôle à la base de données.
5. Choisissez Suivant : Autorisations.
6. Pour Rechercher, sous Attacher les stratégies d'autorisations, entrez le nom de la stratégie IAM que vous avez créée et choisissez la stratégie lorsqu'elle apparaît dans la liste.
7. Choisissez Suivant : Balises, puis Suivant : Vérification.
8. DansNom du rôle, attribuez un nom à votre rôle IAM, par exemple, `rds-s3-integration-role`. De même, vous pouvez éventuellement compléter le champ Description du rôle.
9. Choisissez Créer le rôle.

Pour associer le rôle IAM à votre instance de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Choisissez le nom de l'instance de base de données Oracle pour afficher ses détails.
3. Dans l'onglet Connectivité & sécurité de la section Gérer les rôles IAM, choisissez le rôle à ajouter sous Ajouter des rôles IAM à cette instance.
4. Pour Fonction, choisissez S3_INTEGRATION.

5. Choisissez Ajouter un rôle.

AWS CLI

Pour accorder à Amazon RDS l'accès à un compartiment Amazon S3

1. Créez une stratégie AWS Identity and Access Management (IAM) qui accorde à Amazon RDS un accès à un compartiment Amazon S3.

   Incluez les actions appropriées dans la stratégie en fonction du type d'accès requis :

   - `GetObject` – Obligatoire pour transférer les fichiers d'un compartiment Amazon S3 vers Amazon RDS.
   - `ListBucket` – Obligatoire pour transférer les fichiers d'un compartiment Amazon S3 vers Amazon RDS.
   - `PutObject` – Obligatoire pour transférer les fichiers de Amazon RDS vers un compartiment Amazon S3.

   La commande AWS CLI suivante permet de créer une stratégie IAM nommée *`rds-s3-integration-policy`* avec ces options. Elle accorde un accès à un compartiment nommé *`your-s3-bucket-arn`*.

   #### Example

   Pour Linux, macOS ou 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/*"
        ]
      }
    ]
  }'
```

Pour 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/*"
         ]
       }
     ]
   }'
```

2. Après avoir créé la stratégie, notez son ARN (Amazon Resource Name). Vous en aurez besoin lors d'une étape ultérieure.
3. Créez un rôle IAM qu'Amazon RDS peut endosser en votre nom pour accéder à vos compartiments Amazon S3.

   La commande AWS CLI suivante crée le paramètre `rds-s3-integration-role` à cet effet.

   Example

   Pour Linux, macOS ou 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"
      }
    ]
  }'
```

Pour 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"
       }
     ]
   }'
```

Pour de plus amples informations, veuillez consulter Création d'un rôle pour déléguer des autorisations à un utilisateur IAM dans le Guide de l'utilisateur IAM.

4. Une fois le rôle créé, notez son ARN. Vous en aurez besoin lors d'une étape ultérieure.
5. Attachez la stratégie que vous avez créée au rôle que vous avez créé.

   La commande AWS CLI suivante attache la stratégie au rôle nommé *rds-s3-integration-role*.

   Example

   Pour Linux, macOS ou Unix :

```
aws iam attach-role-policy \
   --policy-arn your-policy-arn \
   --role-name rds-s3-integration-role
```

   Pour Windows :

```
aws iam attach-role-policy ^
   --policy-arn your-policy-arn ^
   --role-name rds-s3-integration-role
```

   Remplacez *your-policy-arn* par l'ARN de stratégie que vous avez noté lors d'une étape précédente.
6. Ajoutez le rôle à l'instance de base de données Oracle.

   La commande AWS CLI suivante ajoute le rôle à une instance de base de données Oracle nommée *mydbinstance*.

Example

Pour Linux, macOS ou Unix :

```
aws rds add-role-to-db-instance \
   --db-instance-identifier mydbinstance \
   --feature-name S3_INTEGRATION \
   --role-arn your-role-arn
```

Pour Windows :

```
aws rds add-role-to-db-instance ^
   --db-instance-identifier mydbinstance ^
   --feature-name S3_INTEGRATION ^
   --role-arn your-role-arn
```

Remplacez *your-role-arn* par l'ARN du rôle que vous avez noté lors d'une étape précédente. `S3_INTEGRATION` doit être spécifié pour l'option `--feature-name`.

Ajout de l'option d'intégration Amazon S3

Pour que vous puissiez ajouter l'intégration Amazon RDS pour Oracle avec Amazon S3, votre instance de base de données Amazon RDS Oracle doit être associée à un groupe d'options qui inclut l'option `S3_INTEGRATION`.

Console

Pour configurer un groupe d'options pour l'intégration Amazon S3

1. Créez un groupe d'options ou identifiez un groupe d'options existant auquel vous pouvez ajouter l'option `S3_INTEGRATION`.

   Pour de plus amples informations sur la création d'un groupe d'options, veuillez consulter Création d'un groupe d'options (p. 212).
2. Ajoutez l'option `S3_INTEGRATION` au groupe d'options.

   Pour de plus amples informations sur l'ajout d'une option à un groupe d'options, veuillez consulter Ajout d'une option à un groupe d'options (p. 214).
3. Créez une instance de base de données Oracle et associez le groupe d'options à cette instance ou modifiez une instance de base de données Oracle pour lui associer le groupe d'options.

   Pour de plus amples informations sur la création d'une instance de base de données, veuillez consulter Création d'une instance de base de données Amazon RDS (p. 146).

   Pour de plus amples informations sur la modification d'une instance de base de données Oracle, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

AWS CLI

Pour configurer un groupe d'options pour l'intégration Amazon S3

1. Créez un groupe d'options ou identifiez un groupe d'options existant auquel vous pouvez ajouter l'option `S3_INTEGRATION`.

   Pour de plus amples informations sur la création d'un groupe d'options, veuillez consulter Création d'un groupe d'options (p. 212).
2. Ajoutez l'option `S3_INTEGRATION` au groupe d'options.

   Par exemple, la commande AWS CLI suivante ajoute l'option `S3_INTEGRATION` à un groupe d'options nommé **`myoptiongroup`**.

   Example

   Pour Linux, macOS ou Unix :

```
aws rds add-option-to-option-group \
   --option-group-name myoptiongroup \
   --options OptionName=S3_INTEGRATION,OptionVersion=1.0
```

   Pour Windows :

```
aws rds add-option-to-option-group ^
   --option-group-name myoptiongroup ^
   --options OptionName=S3_INTEGRATION,OptionVersion=1.0
```

3. Créez une instance de base de données Oracle et associez le groupe d'options à cette instance ou modifiez une instance de base de données Oracle pour lui associer le groupe d'options.

   Pour de plus amples informations sur la création d'une instance de base de données, veuillez consulter Création d'une instance de base de données Amazon RDS (p. 146).

   Pour de plus amples informations sur la modification d'une instance de base de données Oracle, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

Transfert de fichiers entre Amazon RDS pour Oracle et un compartiment Amazon S3

Vous pouvez utiliser les procédures Amazon RDS pour charger les fichiers d'une instance de base de données Oracle vers un compartiment Amazon S3. Vous pouvez également utiliser les procédures Amazon RDS pour télécharger les fichiers d'un compartiment Amazon S3 vers une instance de base de données Oracle.

> **Note**
>
> Ces procédures chargent ou téléchargent les fichiers dans un répertoire unique. Vous ne pouvez pas inclure de sous-répertoires dans ces opérations.

Rubriques

- Chargement de fichiers d'une instance de base de données Oracle vers un compartiment Amazon S3 (p. 1021)

- Téléchargement des fichiers d'un compartiment Amazon S3 vers une instance de base de données Oracle (p. 1023)
- Surveillance du statut d'un transfert de fichiers (p. 1025)

Chargement de fichiers d'une instance de base de données Oracle vers un compartiment Amazon S3

Vous pouvez charger des fichiers depuis une instance de base de données Oracle vers un compartiment Amazon S3 Par exemple, vous pouvez charger les fichiers de sauvegarde Oracle Recovery Manager (RMAN). La taille maximale d'un objet dans un compartiment Amazon S3 est de 5 To. Pour de plus amples informations sur l'utilisation des objets, veuillez consulter Amazon Simple Storage Service Manuel du développeur. Pour de plus amples informations sur les sauvegardes RMAN, veuillez consulter Tâches Recovery Manager (RMAN) DBA courantes pour les instances base de données Oracle (p. 1136).

Vous téléchargez des fichiers à l'aide de la procédure `rdsadmin.rdsadmin_s3_tasks.upload_to_s3`. Cette procédure comporte les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`p_bucket_name`	VARCHAR2	–	obligatoire	Nom du compartiment Amazon S3 dans lequel charger les fichiers.
`p_directory_name`	VARCHAR2	–	obligatoire	Nom de l'objet de répertoire Oracle à partir duquel les fichiers doivent être chargés. Le répertoire peut être n'importe quel objet de répertoire créé par l'utilisateur ou répertoire Data Pump, par exemple `DATA_PUMP_DIR`. Note Vous pouvez uniquement charger les fichiers à partir du répertoire spécifié. Vous ne pouvez pas charger les fichiers des sous-répertoires dans le répertoire spécifié.
`p_s3_prefix`	VARCHAR2	–	obligatoire	Préfixe de nom de fichier Amazon S3 en fonction duquel les fichiers sont chargés. Un préfixe vide charge tous les fichiers au niveau supérieur dans le compartiment Amazon S3 spécifié et n'ajoute pas de préfixe aux noms de fichier.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
				Par exemple, si le préfixe est `folder_1/oradb`, les fichiers sont chargés dans `folder_1`. Dans ce cas, le préfixe `oradb` est ajouté à chaque fichier.
`p_prefix`	VARCHAR2	–	obligatoire	Préfixe de nom de fichier que les noms de fichier doivent contenir pour être chargés. Un préfixe vide charge tous les fichiers du répertoire spécifié.

La valeur renvoyée pour la procédure `rdsadmin.rdsadmin_s3_tasks.upload_to_s3` est un ID de tâche.

L'exemple suivant télécharge tous les fichiers d'un répertoire *`DATA_PUMP_DIR`* dans le compartiment Amazon S3 nommé *`mys3bucket`*.

```
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;
```

L'exemple suivant télécharge tous les fichiers ayant le préfixe *`db`* dans le répertoire*`DATA_PUMP_DIR`* du compartiment Amazon S3 nommé *`mys3bucket`*.

```
SELECT rdsadmin.rdsadmin_s3_tasks.upload_to_s3(
      p_bucket_name    =>  'mys3bucket',
      p_prefix         =>  'db',
      p_s3_prefix      =>  '',
      p_directory_name =>  'DATA_PUMP_DIR')
   AS TASK_ID FROM DUAL;
```

L'exemple suivant télécharge tous les fichiers d'un répertoire *`DATA_PUMP_DIR`* dans le compartiment Amazon S3 nommé *`mys3bucket`*. Les fichiers sont chargés dans un dossier `dbfiles`.

```
SELECT rdsadmin.rdsadmin_s3_tasks.upload_to_s3(
      p_bucket_name    =>  'mys3bucket',
      p_prefix         =>  '',
      p_s3_prefix      =>  'dbfiles/',
      p_directory_name =>  'DATA_PUMP_DIR')
   AS TASK_ID FROM DUAL;
```

L'exemple suivant télécharge tous les fichiers d'un répertoire *DATA_PUMP_DIR* dans le compartiment Amazon S3 nommé *mys3bucket*. Les fichiers sont chargés dans un dossier `dbfiles` et `ora` est ajouté au début de chaque nom de fichier.

```
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;
```

Dans chaque exemple, l'instruction `SELECT` renvoie l'ID de la tâche dans un type de données `VARCHAR2`.

Vous pouvez afficher le résultat en affichant le fichier de sortie de la tâche.

```
SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP','dbtask-task-
id.log'));
```

Remplacez *task-id* par l'ID de tâche renvoyé par la procédure.

> **Note**
>
> Les tâches sont exécutées de manière asynchrone.

Téléchargement des fichiers d'un compartiment Amazon S3 vers une instance de base de données Oracle

Pour télécharger les fichiers d'un compartiment Amazon S3 vers une instance de base de données Oracle, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_s3_tasks.download_from_s3`. La procédure `rdsadmin.rdsadmin_s3_tasks.download_from_s3` possède les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`p_bucket_name`	VARCHAR2	–	obligatoire	Nom du compartiment Amazon S3 à partir duquel télécharger les fichiers.
`p_directory_name`	VARCHAR2	–	obligatoire	Nom de l'objet de répertoire Oracle vers lequel les fichiers doivent être téléchargés. Le répertoire peut être n'importe quel objet de répertoire créé par l'utilisateur ou répertoire Data Pump, par exemple `DATA_PUMP_DIR`.
`p_s3_prefix`	VARCHAR2	''	facultatif	Préfixe de nom de fichier que les noms de fichier doivent contenir pour être téléchargés. Un préfixe vide télécharge tous les fichiers au niveau le plus

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
				haut dans le compartiment Amazon S3 spécifié, mais pas les dossiers dans le compartiment. La procédure télécharge les objets Amazon S3 du dossier de premier niveau correspondant au préfixe. Les structures de répertoire imbriquées correspondant au préfixe spécifié ne sont pas téléchargées. Par exemple, supposons qu'un compartiment Amazon S3 ait la structure de dossiers `folder_1/folder_2/folder_3`. Supposons également que vous ayez spécifié le préfixe `'folder_1/folder_2/'`. Dans ce cas, seuls les fichiers de `folder_2` sont téléchargés, et non ceux de `folder_1` ou `folder_3`. Si à la place vous spécifiez le préfixe `'folder_1/folder_2'`, tous les fichiers dans `folder_1` qui correspondent au préfixe `'folder_2'` sont téléchargés et aucun fichier dans `folder_2` n'est téléchargé.

La valeur renvoyée pour la procédure `rdsadmin.rdsadmin_s3_tasks.download_from_s3` est un ID de tâche.

L'exemple suivant télécharge tous les fichiers du compartiment Amazon S3 nommé *`mys3bucket`* vers le répertoire *`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;
```

L'exemple suivant télécharge tous les fichiers ayant le préfixe *`db`* dans le compartiment Amazon S3 nommé *`mys3bucket`* du répertoire *`DATA_PUMP_DIR`*.

```
SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3(
      p_bucket_name    =>  'mys3bucket',
      p_s3_prefix      =>  'db',
      p_directory_name =>  'DATA_PUMP_DIR')
   AS TASK_ID FROM DUAL;
```

L'exemple suivant télécharge tous les fichiers du dossier *myfolder/* du compartiment Amazon S3 nommé *mys3bucket* vers le répertoire *DATA_PUMP_DIR*. Utilisez la définition du paramètre de préfixe pour spécifier le dossier Amazon S3.

```
SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3(
      p_bucket_name    =>  'mys3bucket',
      p_s3_prefix      =>  'myfolder/',
      p_directory_name =>  'DATA_PUMP_DIR')
   AS TASK_ID FROM DUAL;
```

Dans chaque exemple, l'instruction `SELECT` renvoie l'ID de la tâche dans un type de données `VARCHAR2`.

Vous pouvez afficher le résultat en affichant le fichier de sortie de la tâche.

```
SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP','dbtask-task-
id.log'));
```

Remplacez *task-id* par l'ID de tâche renvoyé par la procédure.

> **Note**
>
> Les tâches sont exécutées de manière asynchrone.
> Vous pouvez utiliser la procédure Oracle `UTL_FILE.FREMOVE` pour supprimer les fichiers d'un répertoire. Pour de plus amples informations, veuillez consulter FREMOVE Procedure dans la documentation Oracle.

Surveillance du statut d'un transfert de fichiers

Les tâches de transfert de fichiers publient des événements Amazon RDS lorsqu'elles démarrent et lorsqu'elles se terminent. Pour de plus amples informations sur l'affichage des événements, veuillez consulter Affichage d'événements Amazon RDS (p. 486).

Vous pouvez consulter le statut d'une tâche en cours dans un fichier bdump. Les fichiers bdump se trouvent dans le répertoire `/rdsdbdata/log/trace`. Chaque nom de fichier bdump a le format suivant.

```
dbtask-task-id.log
```

Remplacez *task-id* par l'ID de la tâche que vous souhaitez surveiller.

> **Note**
>
> Les tâches sont exécutées de manière asynchrone.

Vous pouvez utiliser la procédure stockée `rdsadmin.rds_file_util.read_text_file` pour afficher le contenu des fichiers bdump. Par exemple, la requête suivante renvoie le contenu du fichier bdump *dbtask-1546988886389-2444.log*.

```
SELECT text FROM
 table(rdsadmin.rds_file_util.read_text_file('BDUMP','dbtask-1546988886389-2444.log'));
```

Suppression de l'option d'intégration Amazon S3

Vous pouvez supprimer l'option d'intégration Amazon S3 d'une instance de base de données.

Pour supprimer l'option d'intégration Amazon S3 d'une instance de base de données, effectuez l'une des actions suivantes :

- Pour supprimer l'option d'intégration Amazon S3 de plusieurs instances de base de données, supprimez l'option `S3_INTEGRATION` du groupe d'options auquel celles-ci appartiennent. Ce changement affecte toutes les instances de bases de données qui utilisent le groupe d'options. Pour de plus amples informations, veuillez consulter Suppression d'une option d'un groupe d'options (p. 222).
- Pour supprimer l'option d'intégration Amazon S3 d'une instance de base de données particulière, modifiez l'instance de base de données et spécifiez un autre groupe d'options qui n'inclut pas l'option `S3_INTEGRATION`. Vous pouvez spécifier le groupe d'options (vide) par défaut, ou un groupe d'options personnalisées différent. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Oracle Application Express (APEX)

Amazon RDS prend en charge Oracle Application Express (APEX) à l'aide des options `APEX` et `APEX-DEV`. Oracle APEX peut être déployé en tant qu'environnement d'exécution ou de développement pour les applications web. A l'aide d'Oracle APEX, les développeurs peuvent créer des applications entièrement dans le navigateur web. Pour plus d'informations, consultez Oracle Application Express dans la documentation d'Oracle.

Oracle APEX comprend les principaux composants suivants :

- Un référentiel qui stocke les métadonnées pour les composants et les applications APEX. Le référentiel se compose de tables, d'index et d'autres objets installés dans votre instance de base de données Amazon RDS.
- Un écouteur qui gère les communications HTTP avec les clients Oracle APEX. L'écouteur accepte les connexions entrantes des navigateurs web, les transmet à l'instance de base de données Amazon RDS pour traitement, puis renvoie les résultats du référentiel aux navigateurs. Amazon RDS pour Oracle prend en charge les types d'écouteurs suivants :
  - Pour APEX version 5.0 et ultérieure, utilisez Oracle Rest Data Services (ORDS) version 19.1 et supérieure. Nous vous recommandons d'utiliser la dernière version prise en charge d'Oracle APEX et ORDS. La documentation décrit les anciennes versions à des fins de compatibilité descendante uniquement.
  - Pour APEX version 4.1.1, vous pouvez utiliser Oracle APEX Listener version 1.1.4.
  - Oracle HTTP Server et `mod_plsql`

    > **Note**
    >
    > Amazon RDS ne prend pas en charge le serveur HTTP Oracle XML DB avec la passerelle PL/SQL incorporée ; vous ne pouvez pas l'utiliser en tant qu'écouteur pour APEX. En général, Oracle recommande de ne pas utiliser la passerelle PL/SQL incorporée pour les applications qui s'exécutent sur Internet.

  Pour plus d'informations sur ces types d'écouteur, consultez About Choosing a Web Listener dans la documentation Oracle.

Lorsque vous ajoutez les options APEX Amazon RDS à votre instance de base de données, Amazon RDS installe uniquement le référentiel Oracle APEX. Installez votre écouteur sur un hôte distinct, tel qu'une instance Amazon EC2, un serveur sur site de votre entreprise ou votre ordinateur de bureau.

L'option APEX utilise le stockage dans la classe d'instance de base de données pour votre instance de base de données. Voici les versions prises en charge et les besoins approximatifs en stockage pour Oracle APEX.

Version APEX	Besoins de stockage	Versions de base de données Oracle prises en charge	Remarques
Oracle APEX version 20.1.v1	173 Mio	Tous les comptes	APEX version 20.1.v1 comprend le correctif 30990551. Vous pouvez voir le numéro et la date du correctif en exécutant la requête suivante : `SELECT PATCH_VERSION, PATCH_NUMBER FROM APEX_PATCHES;`
Oracle APEX version 19.2.v1	149 Mio	Tous les comptes	
Oracle APEX version 19.1.v1	148 Mio	Tous les comptes	
Oracle APEX version 18.2.v1	146 MIO	Tous sauf 19c	
Oracle APEX version 18.1.v1	145 Mio	Tous sauf 19c	
Oracle APEX version 5.1.4.v1	220 Mio	Tous sauf 19c (voir les remarques)	Oracle APEX 5.1.4 pour Oracle 11g n'est pas pris en charge lorsque la classe d'instance de base de données utilisée pour l'instance de base de données dispose uniquement d'un vCPU. Pour plus d'informations sur les classes d'instances de base de données, consultez Classes d'instances de base de données (p. 6).
Oracle APEX version 5.1.2.v1	150 Mio	12.1 et 11g seulement (voir les remarques)	Oracle APEX 5.1.2 pour Oracle 11g n'est pas pris en charge lorsque la classe d'instance de base de données utilisée pour l'instance de base de données dispose uniquement d'un vCPU. Pour plus d'informations sur les classes d'instances de base de données, consultez Classes d'instances de base de données (p. 6).
Oracle APEX version 5.0.4.v1	140 Mio	12.1 et 11g seulement (voir les remarques)	Oracle APEX 5.0.4 pour Oracle 11g n'est pas pris en charge lorsque la classe d'instance de base de données utilisée pour l'instance de base de données dispose uniquement d'un vCPU. Pour plus

Version APEX	Besoins de stockage	Versions de base de données Oracle prises en charge	Remarques
			d'informations sur les classes d'instances de base de données, consultez Classes d'instances de base de données (p. 6).
Oracle APEX version 4.2.6.v1	160 Mio	12.1 et 11g seulement	
Oracle APEX version 4.1.1.v1	130 Mio	11g seulement	

Conditions préalables pour Oracle APEX et ORDS

Pour utiliser Oracle APEX et ORDS, assurez-vous de disposer des éléments suivants :

- Java Runtime Environment (JRE)
- Installation client Oracle comprenant les éléments suivants :
  - SQL*Plus ou SQL Developer pour les tâches d'administration
  - Oracle Net Services pour configurer les connexions à votre instance Oracle

Ajout des options APEX Amazon RDS

La procédure générale pour ajouter des options APEX Amazon RDS à une instance de base de données est la suivante :

1. Créer un groupe d'options ou copier ou modifier un groupe existant.
2. Ajouter les options au groupe d'options.
3. Associer un groupe d'options à une instance de base de données.

Lorsque vous ajoutez les options APEX Amazon RDS, une brève panne se produit pendant le redémarrage automatique de votre instance de base de données.

Pour ajouter les options APEX à une instance de base de données

1. Déterminez le groupe d'options que vous voulez utiliser. Vous pouvez créer un groupe d'options ou utiliser un groupe d'options existant. Si vous souhaitez utiliser un groupe d'options existant, passez à l'étape suivante. Sinon, créez un groupe d'options DB personnalisé avec les paramètres suivants :

   a. Pour Moteur, sélectionnez l'édition d'Oracle que vous voulez utiliser. Les options APEX sont prises en charge sur toutes les éditions.

   b. Pour Version majeure du moteur, choisissez la version de votre instance de base de données.

   Pour de plus amples informations, veuillez consulter Création d'un groupe d'options (p. 212).
2. Ajouter les options au groupe d'options. Si vous souhaitez déployer uniquement l'environnement d'exécution Oracle APEX, ajoutez seulement l'option `APEX`. Si vous souhaitez déployer l'environnement de développement complet, ajoutez les options `APEX` et `APEX-DEV`.

   - Pour Oracle 12c, ajoutez les options APEX et APEX-DEV.

- Pour Oracle 11g, ajoutez d'abord l'option prérequise XMLDB, puis ajoutez les options APEX et APEX-DEV.

Pour Version, choisissez la version d'`APEX` que vous souhaitez utiliser. Si vous ne choisissez pas de version, la version 4.1.1.v1 est utilisée par défaut pour 11g, et la version 4.2.6.v1 est utilisée par défaut pour 12c.

> **Important**
>
> Si vous ajoutez les options APEX à un groupe d'options existant qui est déjà attaché à une ou plusieurs instances de base de données, une brève interruption de service a lieu. Pendant cette interruption, toutes les instances de base de données sont automatiquement redémarrées.

Pour plus d'informations sur l'ajout d'options, consultez Ajout d'une option à un groupe d'options (p. 214).

3. Appliquez le groupe d'options à une instance de base de données nouvelle ou existante:

   - Pour une nouvelle instance de base de données, vous appliquez le groupe d'options lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).
   - Pour une instance de base de données existante, vous appliquez le groupe d'options en modifiant l'instance et en attachant le nouveau groupe d'options. Lorsque vous ajoutez les options APEX à une instance de base de données existante, une brève interruption de service se produit pendant le redémarrage automatique de votre instance de base de données. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Déverrouillage du compte utilisateur public

Lorsque les options APEX Amazon RDS sont installées, vous devez modifier le mot de passe du compte utilisateur public APEX, puis déverrouiller le compte. Pour cela, vous pouvez utiliser l'utilitaire de ligne de commande SQL*Plus Oracle. Connectez-vous à votre instance de base de données en tant qu'utilisateur principal et exécutez les commandes suivantes. Remplacez `new_password` par un mot de passe de votre choix.

```
alter user APEX_PUBLIC_USER identified by new_password;
alter user APEX_PUBLIC_USER account unlock;
```

Configuration des services RESTful pour Oracle APEX

Pour configurer les services RESTful dans APEX (non nécessaire pour APEX 4.1.1.V1), utilisez SQL*Plus pour vous connecter à votre instance de base de données en tant qu'utilisateur principal. Ensuite, exécutez la procédure stockée `rdsadmin.rdsadmin_run_apex_rest_config`. Lorsque vous exécutez la procédure stockée, vous fournissez les mots de passe des utilisateurs suivants :

- `APEX_LISTENER`
- `APEX_REST_PUBLIC_USER`

La procédure stockée exécute le script `apex_rest_config.sql`, qui crée de nouveaux comptes de base de données pour ces utilisateurs.

> **Note**
>
> Aucune configuration n'est requise pour Oracle APEX version 4.1.1.v1. Pour cette version d'Oracle APEX uniquement, vous n'avez pas besoin d'exécuter la procédure stockée.

La commande suivante exécute la procédure stockée.

```
exec rdsadmin.rdsadmin_run_apex_rest_config('apex_listener_password',
 'apex_rest_public_user_password');
```

Configuration d'ORDS pour Oracle APEX

Vous êtes maintenant prêt à installer et à configurer Oracle Rest Data Services (ORDS) pour une utilisation avec Oracle APEX. Pour APEX version 5.0 et ultérieure, utilisez Oracle Rest Data Services (ORDS) version 19.1 et supérieure.

Installez l'écouteur sur un hôte distinct : une instance Amazon EC2, un serveur sur site de votre entreprise ou votre ordinateur de bureau. Pour les exemples de cette section, nous supposons que le nom de votre hôte est `myapexhost.example.com`, et que votre hôte exécute Linux.

Préparation de l'installation d'ORDS

Avant de pouvoir installer ORDS, vous devez créer un utilisateur du système d'exploitation non privilégié, puis télécharger et décompresser le fichier d'installation APEX.

Pour préparer l'installation d'ORDS

1. Connectez-vous à `myapexhost.example.com` en tant que `root`.
2. Créez un utilisateur du système d'exploitation non privilégié qui sera propriétaire de l'installation de l'écouteur. La commande suivante crée un utilisateur nommé apexuser.

   ```
   useradd -d /home/apexuser apexuser
   ```

   La commande suivante affecte un mot de passe au nouvel utilisateur.

   ```
   passwd apexuser;
   ```

3. Connectez-vous à `myapexhost.example.com` en tant qu'`apexuser` et téléchargez le fichier d'installation d'APEX à partir d'Oracle dans le répertoire `/home/apexuser` :
   - http://www.oracle.com/technetwork/developer-tools/apex/downloads/index.html
   - Archives de versions antérieures d'Oracle Application Express
4. Décompressez le fichier dans le répertoire `/home/apexuser`.

   ```
   unzip apex_<version>.zip
   ```

   Une fois le fichier décompressé, un répertoire `apex` se trouve dans le répertoire `/home/apexuser`.
5. Pendant que vous êtes toujours connecté à `myapexhost.example.com` en tant que `apexuser`, téléchargez le fichier Oracle REST Data Services depuis Oracle vers votre le répertoire `/home/apexuser` : http://www.oracle.com/technetwork/developer-tools/apex-listener/downloads/index.html.

Installation et configuration d'ORDS

Avant de pouvoir utiliser APEX, vous devez télécharger le fichier ords.war, utiliser Java pour installer ORDS, puis démarrer l'écouteur.

Pour installer et configurer ORDS en vue d'une utilisation avec Oracle APEX

1. Créez un nouveau répertoire basé sur ORDS, puis décompressez le fichier du processus d'écoute.

```
mkdir /home/apexuser/ORDS
cd /home/apexuser/ORDS
```

2. Téléchargez le fichier ords.*version.number*.zip à partir de la page Oracle REST Data Services.
3. Décompressez le fichier dans le répertoire `/home/apexuser/ORDS`.
4. Accordez à l'utilisateur principal les privilèges nécessaires à l'installation d'ORDS.

   Une fois l'option Amazon RDS APEX installée, octroyez à l'utilisateur principal les privilèges nécessaires à l'installation du schéma ORDS. Pour ce faire, connectez-vous à la base de données et exécutez les commandes suivantes. Remplacez *master_user* par le nom de votre utilisateur principal.

```
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

   Ces commandes s'appliquent à ORDS versions 19.1 et ultérieures.

5. Installez le schéma ORDS à l'aide du fichier téléchargé ords.war.

```
java -jar ords.war install advanced
```

   Le programme vous demande les informations suivantes. Les valeurs par défaut sont placées entre crochets. Pour de plus amples informations, veuillez consulter Introduction to Oracle REST Data Services dans la documentation Oracle.

   - Entrez l'emplacement de stockage des données de configuration :

     Entrez `/home/apexuser/ORDS`. Il s'agit de l'emplacement des fichiers de configuration ORDS.
   - Spécifiez le type de connexion à la base de données à utiliser. Entrez le numéro pour [1] Basic [2] TNS [3] Custom URL [1] :

     Choisissez le type de connexion souhaité.
   - Entrez le nom du serveur de base de données [localhost] :*DB_instance_endpoint*

Choisissez la valeur par défaut ou entrez la valeur correcte.

- Entrez le port de l'écouteur de base de données [1521] : *DB_instance_port*

  Choisissez la valeur par défaut ou entrez la valeur correcte.

- Entrez 1 pour spécifier le nom du service de base de données ou 2 pour spécifier le SID de base de données [1] :

  Choisissez `2` pour spécifier le SID de la base de données.

- SID de base de données [xe]

  Choisissez la valeur par défaut ou entrez la valeur correcte.

- Entrez 1 si vous souhaitez vérifier/installer le schéma Oracle REST Data Services ou 2 pour ignorer cette étape [1] :

  Choisissez `1`. Cette étape crée l'utilisateur proxy Oracle REST Data Services nommé ORDS_PUBLIC_USER.

- Entrez le mot de passe de base de données pour ORDS_PUBLIC_USER :

  Entrez le mot de passe, puis confirmez-le.

- Nécessite une connexion avec des privilèges d'administrateur pour vérifier le schéma Oracle REST Data Services.

  Entrez le nom d'utilisateur de l'administrateur : *master_user*

  Entrez le mot de passe de la base de données pour *master_user* : *master_user_password*

  Confirmez le mot de passe : *master_user_password*

- Entrez l'espace de table par défaut pour ORDS_METADATA [SYSAUX].

  Entrez l'espace de table temporaire pour ORDS_METADATA [TEMP].

  Entrez l'espace de table par défaut pour ORDS_PUBLIC_USER [USERS].

  Entrez l'espace de table temporaire pour ORDS_PUBLIC_USER [TEMP].

- Entrez 1 si vous voulez utiliser PL/SQL Gateway ou 2 pour passer cette étape. Si vous utilisez Oracle Application Express ou migrez à partir de mod_plsql, vous devez entrer 1 [1].

  Choisissez la valeur par défaut.

- Entrez le nom d'utilisateur de base de données de la passerelle PL/SQL [APEX_PUBLIC_USER]

  Choisissez la valeur par défaut.

- Entrez le mot de passe de base de données pour APEX_PUBLIC_USER :

  Entrez le mot de passe, puis confirmez-le.

- Entrez 1 pour spécifier les mots de passe des utilisateurs de base de données des services Application Express RESTful (APEX_LISTENER, APEX_REST_PUBLIC_USER) ou 2 pour ignorer cette étape [1] :

  Choisissez `2` pour APEX 4.1.1.V1 ou `1` pour toutes les autres versions d'APEX.

- [Non nécessaire pour APEX 4.1.1.v1] Mot de passe de base de données pour APEX_LISTENER

  Entrez le mot de passe (si nécessaire), puis confirmez-le.

- [Non nécessaire pour APEX 4.1.1.v1] Mot de passe de base de données pour APEX_REST_PUBLIC_USER

Entrez le mot de passe (si nécessaire), puis confirmez-le.

- Entrez un nombre pour sélectionner une fonction à activer :

  Entrez `1` pour activer toutes les fonctions : SQL Developer Web, REST Enabled SQL et Database API.
- Entrez 1 si vous souhaitez démarrer en mode autonome ou 2 pour quitter [1] :

  Saisissez `1`.
- Entrez l'emplacement des ressources statiques APEX :

  Si vous avez décompressé les fichiers d'installation APEX dans `/home/apexuser`, entrez `/home/apexuser/apex/images`. Sinon, entrez *`unzip_path`*`/apex/images`, où *`unzip_path`* est le répertoire dans lequel vous avez décompressé le fichier.
- Entrez 1 si vous utilisez HTTP ou 2 si vous utilisez HTTPS [1] :

  Si vous entrez `1`, spécifiez le port HTTP. Si vous entrez `2`, spécifiez le port HTTPS et le nom d'hôte SSL. L'option HTTPS vous invite à spécifier comment vous fournirez le certificat :
  - Entrez `1` pour utiliser le certificat auto-signé.
  - Entrez `2` pour fournir votre propre certificat. Si vous entrez `2`, spécifiez le chemin d'accès du certificat SSL et le chemin d'accès de la clé privée du certificat SSL.

6. Définissez un mot de passe pour l'utilisateur `admin` APEX. Pour ce faire, utilisez SQL*Plus pour vous connecter à votre instance de base de données en tant qu'utilisateur principal, puis exécutez les commandes suivantes.

   ```
   EXEC rdsadmin.rdsadmin_util.grant_apex_admin_role;
   grant APEX_ADMINISTRATOR_ROLE to master;
   @/home/apexuser/apex/apxchpwd.sql
   ```

   Remplacez *`master`* par votre identifiant principal. Lorsque le script `apxchpwd.sql` vous y invite, entrez un nouveau mot de passe `admin`.
7. Démarrez l'écouteur ORDS. Exécutez le code suivant.

   ```
   java -jar ords.war
   ```

   La première fois que vous démarrez ORDS, vous devez fournir l'emplacement des ressources statiques APEX. Ce dossier d'images se trouve dans le répertoire `/apex/images` du répertoire d'installation d'APEX.
8. Revenez à la fenêtre d'administration APEX de votre navigateur et choisissez Administration. Ensuite, choisissez Application Express Internal Administration. Lorsque vous êtes invité à saisir les informations d'identification, entrez les informations suivantes :

   - Nom d'utilisateur – `admin`
   - Mot de passe – Mot de passe que vous avez défini en utilisant le script `apxchpwd.sql`.

   ChoisissezLogin, puis définissez un nouveau mot de passe pour l'utilisateur `admin`.

L'écouteur est maintenant prêt à être utilisé.

Configuration du processus d'écoute Oracle APEX

Note

L'écouteur Oracle APEX est obsolète.

Amazon RDS pour Oracle continue à prendre en charge APEX version 4.1.1 et l'écouteur Oracle APEX version 1.1.4. Nous vous recommandons d'utiliser les dernières versions prises en charge d'Oracle APEX et d'ORDS.

Installez l'écouteur Oracle APEX sur un hôte distinct, tel qu'une instance Amazon EC2, un serveur sur site de votre entreprise ou votre ordinateur de bureau. Nous partons du principe que le nom de votre hôte est `myapexhost.example.com` et qu'il exécute Linux.

Préparation de l'installation d'un écouteur Oracle APEX

Avant de pouvoir installer l'écouteur Oracle APEX, vous devez créer un utilisateur du système d'exploitation non privilégié, puis télécharger et décompresser le fichier d'installation APEX.

Pour préparer l'installation de l'écouteur Oracle APEX

1. Connectez-vous à `myapexhost.example.com` en tant que `root`.
2. Créez un utilisateur du système d'exploitation non privilégié qui sera propriétaire de l'installation de l'écouteur. La commande suivante crée un utilisateur nommé apexuser.

   ```
   useradd -d /home/apexuser apexuser
   ```

   La commande suivante affecte un mot de passe au nouvel utilisateur.

   ```
   passwd apexuser;
   ```

3. Connectez-vous à `myapexhost.example.com` en tant qu'`apexuser` et téléchargez le fichier d'installation d'APEX à partir d'Oracle dans le répertoire `/home/apexuser` :

   - http://www.oracle.com/technetwork/developer-tools/apex/downloads/index.html
   - Archives de versions antérieures d'Oracle Application Express
4. Décompressez le fichier dans le répertoire `/home/apexuser`.

   ```
   unzip apex_<version>.zip
   ```

   Une fois le fichier décompressé, un répertoire `apex` se trouve dans le répertoire `/home/apexuser`.
5. Pendant que vous êtes toujours connecté à `myapexhost.example.com` en tant que `apexuser`, téléchargez le fichier de l'écouteur Oracle APEX depuis Oracle vers votre répertoire `/home/apexuser`.

Installation et configuration de l'écouteur Oracle APEX

Avant de pouvoir utiliser APEX, vous devez télécharger le fichier apex.war, utiliser Java pour installer l'écouteur Oracle APEX, puis démarrer l'écouteur.

Pour installer et configurer l'écouteur Oracle APEX

1. Créez un répertoire basé sur l'écouteur Oracle APEX et ouvrez le fichier de l'écouteur.

   Exécutez le code suivant :

   ```
   mkdir /home/apexuser/apexlistener
   cd /home/apexuser/apexlistener
   unzip ../apex_listener.version.zip
   ```

2. Exécutez le code suivant.

```
java -Dapex.home=./apex -Dapex.images=/home/apexuser/apex/images -Dapex.erase -jar ./
apex.war
```

3. Entrez les informations suivantes à l'invitation du programme :

   - Nom d'utilisateur de l'administrateur APEX Listener. Le paramètre par défaut est adminlistener.
   - Un mot de passe pour l'administrateur APEX Listener.
   - Nom d'utilisateur du gestionnaire APEX Listener. La valeur par défaut est managerlistener.
   - Un mot de passe pour l'administrateur APEX Listener.

   Le programme imprime une URL dont vous avez besoin pour terminer la configuration, comme ci-dessous.

```
INFO: Please complete configuration at: http://localhost:8080/apex/listenerConfigure
Database is not yet configured
```

4. Continuez à exécuter l'écouteur Oracle APEX pour pouvoir utiliser Oracle Application Express. Lorsque vous avez terminé la procédure de configuration, vous pouvez exécuter l'écouteur à l'arrière-plan.
5. Depuis votre navigateur web, accédez à l'URL fournie par le programme APEX Listener. La fenêtre d'administration d'Oracle Application Express Listener s'affiche. Entrez les informations suivantes :

   - Nom d'utilisateur – `APEX_PUBLIC_USER`
   - Mot de passe – le mot de passe pour APEX_PUBLIC_USER. Il s'agit du mot de passe que vous avez spécifié précédemment, lorsque vous avez configuré le référentiel APEX. Pour plus d'informations, consultez Déverrouillage du compte utilisateur public (p. 1029).
   - Type de connexion – Basic
   - Nom d'hôte – le point de terminaison de votre instance de base de données Amazon RDS, par exemple `mydb.f9rbfa893tft.us-east-1.rds.amazonaws.com`.
   - Port – 1521
   - SID – le nom de la base de données sur votre instance de base de données Amazon RDS, tel que `mydb`.
6. Choisissez Apply. La fenêtre d'administration APEX s'affiche.
7. Définissez un mot de passe pour l'utilisateur `admin` APEX. Pour ce faire, utilisez SQL*Plus pour vous connecter à votre instance de base de données en tant qu'utilisateur principal, puis exécutez les commandes suivantes.

```
EXEC rdsadmin.rdsadmin_util.grant_apex_admin_role;
grant APEX_ADMINISTRATOR_ROLE to master;
@/home/apexuser/apex/apxchpwd.sql
```

   Remplacez *`master`* par votre identifiant principal. Lorsque le script `apxchpwd.sql` vous y invite, entrez un nouveau mot de passe `admin`.
8. Revenez à la fenêtre d'administration APEX de votre navigateur et choisissez Administration. Ensuite, choisissez Application Express Internal Administration. Lorsque vous êtes invité à saisir les informations d'identification, entrez les informations suivantes :

   - Nom d'utilisateur – `admin`
   - Mot de passe – Mot de passe que vous avez défini en utilisant le script `apxchpwd.sql`.

   ChoisissezLogin, puis définissez un nouveau mot de passe pour l'utilisateur `admin`.

L'écouteur est maintenant prêt à être utilisé.

Mise à niveau de la version d'APEX

> **Important**
>
> Faites une sauvegarde de votre instance de base de données avant de mettre à niveau APEX. Pour plus d'informations, consultez Création d'un instantané de base de données (p. 327) et Test d'une mise à niveau (p. 981).

Pour mettre à niveau APEX et votre instance de base de données, procédez comme suit :

- Créez un nouveau groupe d'options pour la version mise à niveau de votre instance de base de données.
- Ajoutez les versions mises à niveau d'APEX et d'APEX-DEV au nouveau groupe d'options. Assurez-vous d'ajouter toutes les autres options utilisées par votre instance de base de données. Pour plus d'informations, consultez Considérations relatives au groupe d'options (p. 980).
- Lorsque vous mettez à niveau votre instance de base de données, spécifiez le nouveau groupe d'options pour l'instance de base de données mise à niveau.

Une fois la mise à niveau de votre version d'APEX terminée, il est possible que le schéma APEX de la version précédente existe toujours dans votre base de données. Si vous n'en avez plus besoin, vous pouvez supprimer l'ancien schéma APEX de votre base de données après avoir procédé à la mise à niveau.

Si vous effectuez une mise à niveau de la version d'APEX et que les services RESTful n'ont pas été configurés dans la version antérieure d'APEX, nous vous recommandons de les configurer. Pour plus d'informations, consultez Configuration des services RESTful pour Oracle APEX (p. 1029).

Dans certains cas, lorsque vous planifiez d'effectuer une mise à niveau de version majeure de votre instance de base de données, vous pouvez vous rendre compte que vous utilisez une version d'APEX qui n'est pas compatible avec votre version de base de données cible. Dans ce cas, vous pouvez mettre à niveau votre version d'APEX avant de mettre à niveau votre instance de base de données. La mise à niveau préalable d'APEX permet de réduire le temps nécessaire à la mise à niveau de votre instance de base de données.

> **Note**
>
> Après avoir mis à niveau APEX, installez et configurez un écouteur à utiliser avec la version mise à niveau. Pour obtenir des instructions, consultez Configuration du processus d'écoute Oracle APEX (p. 1033).

Suppression de l'option APEX

Vous pouvez supprimer les options APEX Amazon RDS d'une instance de base de données. Pour supprimer les options APEX d'une instance de base de données, effectuez l'une des actions suivantes :

- Pour supprimer les options APEX de plusieurs instances de base de données, supprimez l'option APEX du groupe d'options auquel elles appartiennent. Ce changement affecte toutes les instances de bases de données qui utilisent le groupe d'options. Lorsque vous supprimez les options APEX d'un groupe d'options qui est attaché à plusieurs instances de base de données, une brève interruption de service a lieu pendant le redémarrage de toutes les instances de base de données.

  Pour plus d'informations, consultez Suppression d'une option d'un groupe d'options (p. 222).
- Pour supprimer les options APEX d'une seule instance de base de données, modifiez l'instance de base de données et spécifiez un autre groupe d'options qui n'inclut pas les options APEX. Vous pouvez spécifier le groupe d'options (vide) par défaut, ou un groupe d'options personnalisées différent. Lorsque

vous supprimez les options APEX, une brève interruption de service se produit pendant le redémarrage automatique de votre instance de base de données.

Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Lorsque vous supprimez les options APEX d'une instance de base de données, le schéma APEX est supprimé de votre base de données.

Oracle Enterprise Manager

Amazon RDS prend en charge Oracle Enterprise Manager (OEM). OEM est la gamme de produits Oracle pour la gestion intégrée de la technologie de l'information d'entreprise.

Amazon RDS prend en charge OEM à l'aide des options suivantes.

Option	ID d'option	Prise en charge de
OEM Database Express (p. 1037)	`OEM`	OEM Database Express 12c OEM 11g Database Control
OEM Management Agent (p. 1042)	`OEM_AGENT`	OEM Cloud Control for 13c OEM Cloud Control for 12c

> **Note**
>
> Vous pouvez utiliser OEM Database ou OEM Management Agent, mais pas les deux.

Oracle Enterprise Manager Database Express

Amazon RDS prend en charge Oracle Enterprise Manager (OEM) Database Express via l'utilisation de l'option OEM. Amazon RDS prend en charge les versions suivantes d'OEM Database :

- Oracle Enterprise Manager Database Express pour Oracle 19c, Oracle 18c et Oracle 12c
- Oracle Enterprise Manager 11g Database Control pour Oracle 11g

OEM Database Express et Database Control sont des outils similaires qui ont une interface web pour l'administration des bases de données Oracle. Pour de plus amples informations sur ces outils, veuillez consulter Accessing Enterprise Manager Database Express 18c, Accessing Enterprise Manager Database Express 12c et Accessing Enterprise Manager 11g Database Control dans la documentation Oracle.

Voici quelques limitations à l'utilisation de la base de données OEM :

- La base de données OEM n'est pas prise en charge sur les classes d'instance de base de données db.t3.micro ou db.t3.small.

  Pour de plus amples informations sur les classes d'instance DB, veuillez consulter Prise en charge des classes d'instance de base de données pour Oracle (p. 933).
- OEM 11g Database Control n'est pas compatible avec les fuseaux horaires suivants : Amérique/Argentine/Buenos_Aires, Amérique/Matamoros, Amérique/Monterrey, Amérique/Toronto, Asie/Ashgabat, Asie/Dhaka, Asie/Katmandou, Asie/Kolkata, Asie/Oulan-Bator, Atlantique/Cape_Verde, Australie/Eucla, Pacifique/Kiritimati.

Pour plus d'informations sur la prise en charge des fuseaux horaires, consultez Fuseau horaire Oracle (p. 1088).

Paramètres de l'option base de données OEM

Amazon RDS prend en charge les paramètres suivants pour l'option OEM.

Paramètre d'option	Valeurs valides	Description
Port	Une valeur d'entier	Le port de l'instance de base de données qui écoute la base de données OEM. La valeur par défaut de OEM Database Express est 5500. La valeur par défaut de OEM 11g Database Control est 1158. Pour OEM 11g Database Control, définissez le port sur 1158 ou sur une valeur comprise entre 5500 et 5519.
Groupes de sécurité	—	Un groupe de sécurité qui a accès à Port.

Ajout de l'option de base de données OEM

La procédure générale pour ajouter de l'option OEM à une instance de base de données est la suivante :

1. Créer un groupe d'options ou copier ou modifier un groupe existant.
2. Ajouter l'option au groupe d'options.
3. Associez le groupe d'options à l'instance de base de données.

Lorsque vous ajoutez l'option OEM pour une instance de base de données Oracle 11g, il n'y a pas d'interruption et vous n'avez pas besoin de redémarrer votre instance de base de données. Cependant, lorsque vous ajoutez l'option OEM pour une instance de base de données Oracle 12c, Oracle 18c ou Oracle 19c, une brève interruption se produit pendant le redémarrage automatique de votre instance de base de données.

Pour ajouter l'option OEM à une instance de base de données

1. Déterminez le groupe d'options que vous voulez utiliser. Vous pouvez créer un groupe d'options ou utiliser un groupe d'options existant. Si vous souhaitez utiliser un groupe d'options existant, passez à l'étape suivante. Sinon, créez un groupe d'options DB personnalisé avec les paramètres suivants :

   a. Pour Moteur, choisissez l'édition oracle pour votre instance de base de données.
   b. Pour Version majeure du moteur, choisissez la version de votre instance de base de données.

   Pour plus d'informations, consultez Création d'un groupe d'options (p. 212).
2. Ajoutez l'option OEM au groupe d'options et configurez les paramètres de l'option. Pour plus d'informations sur l'ajout d'options, consultez Ajout d'une option à un groupe d'options (p. 214). Pour plus d'informations sur chaque paramètre, consultez Paramètres de l'option base de données OEM (p. 1038).

Note

Si vous ajoutez l'option OEM à un groupe d'options existant qui est déjà attaché à une ou plusieurs instances de bases de données Oracle 19c, Oracle 18c ou Oracle 12c, une brève interruption de service a lieu pendant le redémarrage automatique de toutes les instances de bases de données.

3. Appliquez le groupe d'options à une instance de base de données nouvelle ou existante:
   - Pour une nouvelle instance de base de données, vous appliquez le groupe d'options lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).
   - Pour une instance de base de données existante, vous appliquez le groupe d'options en modifiant l'instance et en attachant le nouveau groupe d'options. Lorsque vous ajoutez l'option OEM pour une instance de base de données Oracle 19c, Oracle 18c ou Oracle 12c, une brève interruption se produit pendant le redémarrage automatique de votre instance de base de données. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Note

Vous pouvez également utiliser AWS CLI pour ajouter l'option OEM. Pour obtenir des exemples, consultez Ajout d'une option à un groupe d'options (p. 214).

Utilisation d'une base de données OEM

Après avoir activé l'option OEM, vous pouvez commencer à utiliser l'outil de base de données OEM sur votre navigateur web.

Vous pouvez accéder à OEM Database Control ou à OEM Database Express à partir de votre navigateur web. Par exemple, si le point de terminaison pour votre instance de base de données Amazon RDS est `mydb.f9rbfa893tft.us-east-1.rds.amazonaws.com` et que votre post OEM est 1158, l'URL permettant d'accéder à OEM Database Control se présente comme suit.

```
https://mydb.f9rbfa893tft.us-east-1.rds.amazonaws.com:1158/em
```

Quand vous accédez à l'un de ces outils depuis votre navigateur web, une fenêtre de connexion s'affiche, vous demandant de spécifier un nom d'utilisateur et un mot de passe. Tapez le nom d'utilisateur principal et le mot de passe principal de votre instance de base de données. Vous êtes maintenant prêt à gérer vos bases de données Oracle.

Modification des paramètres de la base de données OEM

Après avoir activé la base de données OEM, vous pouvez modifier le paramètre des Groupes de sécurité de l'option.

Vous ne pouvez pas modifier le numéro de port OEM après avoir associé le groupe d'options à une instance de base de données. Pour modifier le numéro de port OEM d'une instance de base de données, procédez comme suit :

1. Créez un nouveau groupe d'options.
2. Ajoutez l'option OEM avec le nouveau numéro de port au nouveau groupe d'options.
3. Supprimez le groupe d'options existant de l'instance de base de données.
4. Ajoutez le nouveau groupe d'options à l'instance de base de données.

Pour plus d'informations sur la modification des paramètres d'options, consultez Modification d'un paramètre d'option (p. 219). Pour plus d'informations sur chaque paramètre, consultez Paramètres de l'option base de données OEM (p. 1038).

Utilisation d'une base de données OEM

Vous pouvez utiliser les procédures Amazon RDS pour exécuter certaines tâches OEM Database Express. Ces procédures vous permettent d'exécuter les tâches indiquées ci-après.

> **Note**
>
> Les tâches OEM Database Express s'exécutent de manière asynchrone.

Tâches

- Basculement du front end du site web OEM Database Express vers Adobe Flash (p. 1040)
- Basculement du front-end du site web OEM Database Express vers Oracle JET (p. 1041)

Basculement du front end du site web OEM Database Express vers Adobe Flash

> **Note**
>
> Cette tâche n'est disponible que sur les instances de base de données Oracle exécutant la version 19c ou versions ultérieures.

À partir d'Oracle 19c, Oracle a rendu obsolète l'ancienne interface utilisateur d'OEM Database Express basée sur Adobe Flash. En conséquence, OEM Database Express utilise désormais une interface conçue avec Oracle JET. Si vous rencontrez des problèmes avec la nouvelle interface, vous pouvez revenir à l'interface obsolète basée sur Flash. Vous pourriez par exemple être bloqué sur un écran `Loading` après vous être connecté à OEM Database Express. Vous pourriez également ne pas avoir accès à certaines fonctions présentes dans la version Flash d'OEM Database Express.

Pour basculer le front end du site web OEM Database Express vers Adobe Flash, exécutez la procédure Amazon RDS `rdsadmin.rdsadmin_oem_tasks.em_express_frontend_to_flash`. Cette procédure est équivalente à la commande SQL `execemx emx`.

Les bonnes pratiques en matière de sécurité déconseillent l'utilisation d'Adobe Flash. Bien que vous puissiez revenir à la version Flash d'OEM Database Express, nous recommandons si possible d'utiliser les sites web OEM Database Express basés sur JET. Si vous recommencez à utiliser Adobe Flash et souhaitez revenir à Oracle JET, utilisez la procédure `rdsadmin.rdsadmin_oem_tasks.em_express_frontend_to_jet`. Après une mise à niveau de la base de données Oracle, une version plus récente d'Oracle JET est susceptible de résoudre les problèmes liés à JET dans OEM Database Express. Pour de plus amples informations sur le basculement vers Oracle JET, veuillez consulter Basculement du front-end du site web OEM Database Express vers Oracle JET (p. 1041).

> **Note**
>
> L'exécution de cette tâche à partir de l'instance de base de données source pour un réplica en lecture entraîne également le basculement des front ends du site web OEM Database Express vers Adobe Flash pour le réplica en lecture.

L'appel de procédure suivant crée une tâche permettant de basculer le site web OEM Database Express vers Adobe Flash et renvoie l'ID de la tâche.

```
SELECT rdsadmin.rdsadmin_oem_tasks.em_express_frontend_to_flash() as TASK_ID from DUAL;
```

Vous pouvez afficher le résultat en affichant le fichier de sortie de la tâche.

```
SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP','dbtask-task-
id.log'));
```

Remplacez *task-id* par l'ID de tâche renvoyé par la procédure. Pour de plus amples informations sur la procédure Amazon RDS `rdsadmin.rds_file_util.read_text_file`, veuillez consulter Lecture de fichiers dans un répertoire d'instance de base de données (p. 1166).

Vous pouvez également afficher le contenu du fichier de sortie de la tâche dans AWS Management Console en recherchant `task-id` dans les entrées de journal de la section Logs & events (Journaux et événements).

Basculement du front-end du site web OEM Database Express vers Oracle JET

> **Note**
>
> Cette tâche n'est disponible que sur les instances de base de données Oracle exécutant la version 19c ou versions ultérieures.

Pour basculer le front end du site web OEM Database Express vers Oracle JET, exécutez la procédure Amazon RDS `rdsadmin.rdsadmin_oem_tasks.em_express_frontend_to_jet`. Cette procédure est équivalente à la commande SQL `execemx omx`.

Par défaut, les sites web OEM Database Express pour les instances de base de données Oracle exécutant la version 19c ou versions ultérieures utilisent Oracle JET. Si vous avez utilisé la procédure `rdsadmin.rdsadmin_oem_tasks.em_express_frontend_to_flash` pour basculer le front end du site web OEM Database Express vers Adobe Flash, vous pouvez revenir à Oracle JET. Pour ce faire, utilisez la procédure `rdsadmin.rdsadmin_oem_tasks.em_express_frontend_to_jet`. Pour de plus amples informations sur le basculement vers Adobe Flash, veuillez consulter Basculement du front end du site web OEM Database Express vers Adobe Flash (p. 1040).

> **Note**
>
> L'exécution de cette tâche à partir de l'instance de base de données source pour un réplica en lecture entraîne également le basculement des front ends du site web OEM Database Express vers Oracle JET pour le réplica en lecture.

L'appel de procédure suivant crée une tâche permettant de basculer le site web OEM Database Express vers Oracle JET et renvoie l'ID de la tâche.

```
SELECT rdsadmin.rdsadmin_oem_tasks.em_express_frontend_to_jet() as TASK_ID from DUAL;
```

Vous pouvez afficher le résultat en affichant le fichier de sortie de la tâche.

```
SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP','dbtask-task-
id.log'));
```

Remplacez *task-id* par l'ID de tâche renvoyé par la procédure. Pour de plus amples informations sur la procédure Amazon RDS `rdsadmin.rds_file_util.read_text_file`, veuillez consulter Lecture de fichiers dans un répertoire d'instance de base de données (p. 1166).

Vous pouvez également afficher le contenu du fichier de sortie de la tâche dans AWS Management Console en recherchant `task-id` dans les entrées de journal de la section Logs & events (Journaux et événements).

Suppression de l'option de base de données OEM

Vous pouvez supprimer l'option OEM d'une instance de base de données. Lorsque vous supprimez l'option OEM pour une instance de base de données Oracle 19c, Oracle 18c ou Oracle 12c, une brève interruption se produit pendant le redémarrage automatique de votre instance de base de données. Une fois que vous avez supprimé l'option OEM, vous n'avez pas besoin de redémarrer votre instance de base de données. Lorsque vous supprimez l'option OEM pour une instance de base de données Oracle 11g, il n'y a pas d'interruption et vous n'avez pas besoin de redémarrer votre instance de base de données.

Pour supprimer l'option OEM d'une instance de base de données, effectuez l'une des actions suivantes :

- Supprimez l'option OEM du groupe d'options auquel elle appartient. Ce changement affecte toutes les instances de bases de données qui utilisent le groupe d'options. Pour plus d'informations, consultez Suppression d'une option d'un groupe d'options (p. 222).
- Modifiez l'instance de base de données et spécifiez un groupe d'options différent qui n'inclut pas l'option OEM Ce changement affecte une seule instance de base de données. Vous pouvez spécifier le groupe d'options (vide) par défaut, ou un groupe d'options personnalisées différent. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Oracle Management Agent pour Enterprise Manager Cloud Control

Amazon RDS prend en charge Oracle Enterprise Manager (OEM) Management Agent via l'utilisation de l'option `OEM_AGENT`. Amazon RDS prend en charge Management Agent pour les versions suivantes d'OEM :

- Oracle Enterprise Manager Cloud Control pour 13c
- Oracle Enterprise Manager Cloud Control pour 12c

Management Agent est un composant logiciel qui surveille les cibles en cours d'exécution sur les hôtes et communique ces informations au Oracle Management Service (OMS) de niveau intermédiaire. Pour plus d'informations, consultez les présentations Overview of Oracle Enterprise Manager Cloud Control 12c et Overview of Oracle Enterprise Manager Cloud Control 13c dans la documentation Oracle.

Vous trouverez, ci-après, les versions Oracle prises en charge pour chaque version de Management Agent.

Version de Management Agent	Oracle 19c	Oracle 18c	Oracle 12c version 12.2	Oracle 12c version 12.1	Oracle 11g
13.3.0.0.v2	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
13.3.0.0.v1	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
13.2.0.0.v3	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
13.2.0.0.v2	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
13.2.0.0.v1	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
13.1.0.0.v1	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
12.1.0.5.v1	Non pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
12.1.0.4.v1	Non pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge

Voici quelques restrictions quant à l'utilisation de Management Agent :

- Les tâches d'administration telles que l'exécution de tâches et l'application de correctifs de bases de données, qui requièrent des informations d'identification de l'hôte, ne sont pas prises en charge.
- Les métriques de l'hôte et la liste des processus ne reflètent pas nécessairement l'état réel du système. Par conséquent, vous ne devez pas utiliser OEM pour surveiller le système de fichiers racine ou le

système de fichiers de point de montage. Pour de plus amples informations sur la surveillance du système d'exploitation, veuillez consulter Surveillance améliorée (p. 394).

- La découverte automatique n'est pas prise en charge. Vous devez ajouter manuellement les cibles de base de données.
- La disponibilité du module OMS dépend de l'édition de votre base de données. Par exemple, le module de diagnostic et de réglage des performances des bases de données n'est disponible que pour Oracle Database Enterprise Edition.
- Management Agent consomme des ressources de mémoire et de calcul supplémentaires. Si vous rencontrez des problèmes de performances après avoir activé l'option `OEM_AGENT`, nous vous recommandons d'augmenter la taille de la classe d'instance de base de données Pour plus d'informations, consultez Classes d'instances de base de données (p. 6) et Modification d'une instance de base de données Amazon RDS (p. 243).
- Dans la mesure où l'accès du système d'exploitation au journal d'alertes n'est pas octroyé à l'utilisateur qui exécute `OEM_AGENT` sur l'hôte Amazon RDS, il n'est pas possible de collecter les métriques pour `DB Alert Log` et `DB Alert Log Error Status` dans OEM.

Conditions préalables pour Management Agent

Pour pouvoir utiliser Management Agent, vous devez impérativement disposer des éléments suivants :

- Une instance de base de données Amazon RDS exécutant Oracle version 19.0.0.0, 18.0.0.0, 12.2.0.1, 12.1.0.2 ou 11.2.0.4.
- Au moins 8,5 Gio d'espace de stockage pour OEM 13c Version 3.
- Au moins 5,5 Gio d'espace de stockage pour OEM 13c Version 2.
- Au moins 4,5 Gio d'espace de stockage pour OEM 13c Version 1.
- Au moins 2.5 Gio d'espace de stockage pour OEM 12c.
- Pour Oracle version 19.0.0.0, le paramètre d'option `AGENT_VERSION` minimal est 13.1.0.0.v1.
- Une instance Oracle Management Service (OMS), configurée pour se connecter à votre instance de base de données Amazon RDS.

  Pour une instance de base de données Amazon RDS exécutant Oracle version 18.0.0.0 ou supérieure, respectez les prérequis suivants :

  - Pour OMS 13c2, appliquez Enterprise Manager 13.2 Master Bundle Patch List, qui comprend les plug-ins 13.2.1, 13.2.2, 13.2.3, 13.2.4 (Oracle Doc ID 2219797.1).
  - Pour OMS 13c2, appliquez le correctif 28970534 d'OMS PSU System.
  - Pour OMS 13c2, appliquez le correctif 29201709 OMS-Side Plugin System 13.2.2.0.190131.

  Pour une instance de base de données Amazon RDS exécutant Oracle version 12.2.0.1 ou inférieure, respectez les prérequis suivants :

  - Pour OMS 13c Version 2 avec le correctif Oracle 25163555 appliqué, utilisez l'agent OEM 13.2.0.0.v2 ou version ultérieure.

    Utilisez OMSPatcher pour appliquer le correctif.
  - Pour OMS 13c Version 2 sans correctif, utilisez l'agent OEM 13.2.0.0.v1.

  Utilisez OMSPatcher pour appliquer les correctifs.
- Dans la plupart des cas, vous devez configurer votre VPC de façon à autoriser les connexions entre OMS et votre instance de base de données. Si vous n'êtes pas familiarisé avec Amazon Virtual Private Cloud (Amazon VPC), nous vous recommandons d'effectuer les étapes de Didacticiel : créer un Amazon VPC à utiliser avec une instance de base de données (p. 1629) avant de poursuivre.
- Si vous utilisez les versions Management Agent `OEM_AGENT 13.2.0.0.v3` et `13.3.0.0.v2`, et que vous souhaitez utiliser la connectivité TCPS, suivez les instructions de la section Configuring Third Party CA Certificates for Communication With Target Databases de la documentation Oracle. De

même, mettez à jour le JDK sur votre OMS en suivant les instructions du document Oracle dont l'ID de document Oracle est : 2241358.1. Ainsi, l'OMS prendra en charge toutes les suites de chiffrement prises en charge par la base de données.

> **Note**
>
> La connectivité TCPS entre Management Agent et l'instance de base de données est uniquement prise en charge pour les versions `OEM_AGENT 13.2.0.0.v3` et `13.3.0.0.v2` de Management Agent.

Une configuration supplémentaire est requise pour autoriser votre hôte OMS et votre instance de base de données Amazon RDS à communiquer. Vous devez également effectuer les opérations suivantes :

- Pour établir une connexion entre Management Agent et votre instance OMS, si cette dernière se trouve derrière un pare-feu, vous devez ajouter les adresses IP de vos instances de base de données à votre instance OMS.

  Pour l'instance OMS, vérifiez que le pare-feu autorise le trafic en provenance du port de l'écouteur de base de données (par défaut, le port 1521) et du port de l'agent OEM (par défaut, le port 3872), à partir de l'adresse IP de l'instance de base de données.
- Pour établir une connexion entre votre instance OMS et Management Agent, si votre instance OMS possède un nom d'hôte publiquement résolu, vous devez ajouter l'adresse OMS à un groupe de sécurité. Votre groupe de sécurité doit avoir des règles de trafic entrant qui autorisent l'accès au port de l'instance de base de données et au port de Management Agent. Pour obtenir un exemple de création de règles de sécurité et d'ajout de règles de trafic entrant, consultez Didacticiel : créer un Amazon VPC à utiliser avec une instance de base de données (p. 1629).
- Pour vous connecter depuis votre OMS à l'agent de gestion, si votre OMS ne possède pas de nom d'hôte publiquement résolu, procédez d'une des manières suivantes :
  - Si votre OMS est hébergé sur une instance Amazon Elastic Compute Cloud (Amazon EC2) dans un VPC privé, vous pouvez configurer un appairage de VPC pour vous connecter depuis l'OMS à l'agent de gestion. Pour plus d'informations, consultez Une instance de base de données d'un VPC accédée par une instance EC2 d'un autre VPC (p. 1615).
  - Si votre OMS est hébergé sur site, vous pouvez configurer une connexion VPN pour autoriser l'accès entre OMS et l'agent de gestion. Pour plus d'informations, consultez Une instance de base de données d'un VPC accessible par une application cliente via Internet (p. 1617) ou Connexions VPN.

Paramètres de l'option Management Agent

Amazon RDS prend en charge les paramètres suivants pour l'option Management Agent.

Paramètre d'option	Obligatoire	Valeurs valides	Description

Version (`AGENT_VERSION`)	Oui	`13.3.0.0.v2`
		`13.3.0.0.v1`
		`13.2.0.0.v3`
		`13.2.0.0.v2`
		`13.2.0.0.v1`
		`13.1.0.0.v1`
		`12.1.0.5.v1`
			La version du logiciel Management Agent.
			Le nom de l'option AWS CLI est `OptionVersion`.
			Note
			Dans la région AWS GovCloud (US-West), les versions 12.1 et 13.1 ne sont pas disponibles.

Paramètre d'option	Obligatoire	Valeurs valides	Description
		`12.1.0.4.v1`	
Port (`AGENT_PORT`)	Oui	Une valeur d'entier	Le port de l'instance de base de données qui écoute l'hôte OMS. La valeur par défaut est 3872. Votre hôte OMS doit appartenir à un groupe de sécurité qui a accès à ce port. Le nom de l'option AWS CLI est `Port`.
Groupes de sécurité	Oui	Groupes de sécurité existants	Un groupe de sécurité qui a accès à Port. Votre hôte OMS doit appartenir à ce groupe de sécurité. Le nom de l'option AWS CLI est `VpcSecurityGroupMemberships` ou `DBSecurityGroupMemberships`.
OMS_HOST	Oui	Une valeur de chaîne, par exemple *`my.example.oms`*	Le nom d'hôte accessible au public ou l'adresse IP de l'OMS. Le nom de l'option AWS CLI est `OMS_HOST`.
OMS_PORT	Oui	Une valeur d'entier	Le port de chargement HTTPS de l'hôte OMS qui écoute l'agent de gestion. Pour déterminer le port de chargement the HTTPS, connectez-vous à l'hôte OMS et exécutez la commande suivante (sui nécessite le mot de passe `SYSMAN`) : `emctl status oms -details` Le nom de l'option AWS CLI est `OMS_PORT`.
AGENT_REGISTRATION_PASSWORD	Oui	Une valeur de chaîne	Le mot de passe que l'agent de gestion utilise pour s'authentifier auprès de l'OMS. Nous vous recommandons de créer un mot de passe permanent dans votre OMS avant d'activer l'option `OEM_AGENT`. Avec un mot de passe permanent, vous pouvez partager un groupe particulier de l'option Management Agent entre plusieurs bases de données Amazon RDS. Le nom de l'option AWS CLI est `AGENT_REGISTRATION_PASSWORD`.
ALLOW_TLS_ONLY	Non	`true`, `false` (par défaut)	Valeur qui configure l'agent OEM pour ne prendre en charge que le protocole `TLSv1` pendant que l'agent écoute en tant que serveur. Ce paramètre n'est pris en charge que pour les versions de l'agent 12.1. Les versions ultérieures de l'agent prennent uniquement en charge le protocole TLS (Transport Layer Security) par défaut.

Paramètre d'option	Obligatoire	Valeurs valides	Description
MINIMUM_TLS_VERSION	Non	`TLSv1` (par défaut), `TLSv1.2`	Valeur qui spécifie la version TLS minimale prise en charge par l'agent OEM pendant que l'agent écoute en tant que serveur. Ce paramètre n'est pris en charge que pour les versions de l'agent 13.1.0.0.v1 et supérieures. Les versions antérieures de l'agent prennent uniquement en charge le paramètre `TLSv1`.
TLS_CIPHER_SUITE	Non	`TLS_RSA_WITH_AES_128_CBC_SHA` (prise en charge par défaut par toutes les versions de l'agent) `TLS_RSA_WITH_AES_128_CBC_SHA256` (nécessite la version 13.1.0.0.v1 ou supérieure) `TLS_RSA_WITH_AES_256_CBC_SHA` (nécessite la version 13.2.0.0.v3 ou supérieure) `TLS_RSA_WITH_AES_256_CBC_SHA256` (nécessite la version 13.2.0.0.v3 ou supérieure)	Valeur qui spécifie la suite de chiffrement TLS utilisée par l'agent OEM pendant que l'agent écoute en tant que serveur.

Ajout de l'option Management Agent

Le processus général d'ajout de l'option Management Agent à une instance de base de données est le suivant :

1. Créer un groupe d'options ou copier ou modifier un groupe existant.
2. Ajouter l'option au groupe d'options.
3. Associez le groupe d'options à l'instance de base de données.

Si vous rencontrez des erreurs, vous pouvez consulter les documents My Oracle Support pour savoir comment résoudre des problèmes spécifiques.

Après avoir ajouté l'option Management Agent, vous n'avez pas besoin de redémarrer votre instance de base de données. Dès que le groupe d'options est actif, l'agent OEM est actif.

Si votre hôte OMS utilise un certificat tiers non approuvé, Amazon RDS renvoie l'erreur suivante :

```
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.
```

S'il vous renvoie une erreur, l'option Management Agent n'est pas activée avant que le problème soit résolu. Pour plus d'informations sur la résolution des problèmes, consultez le document du Support My Oracle 2202569.1.

Console

Pour ajouter l'option Management Agent à une instance de base de données

1. Déterminez le groupe d'options que vous voulez utiliser. Vous pouvez créer un groupe d'options ou utiliser un groupe d'options existant. Si vous souhaitez utiliser un groupe d'options existant, passez à l'étape suivante. Sinon, créez un groupe d'options DB personnalisé avec les paramètres suivants :

   a. Pour Moteur, choisissez l'édition oracle pour votre instance de base de données.

   b. Pour Version majeure du moteur, choisissez la version de votre instance de base de données.

   Pour de plus amples informations, veuillez consulter Création d'un groupe d'options (p. 212).
2. Ajoutez l'option OEM_AGENT pour le groupe d'options et configurez les paramètres de l'option. Pour plus d'informations sur l'ajout d'options, consultez Ajout d'une option à un groupe d'options (p. 214). Pour plus d'informations sur chaque paramètre, consultez Paramètres de l'option Management Agent (p. 1044).
3. Appliquez le groupe d'options à une instance de base de données nouvelle ou existante:

   - Pour une nouvelle instance de base de données, vous appliquez le groupe d'options lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).
   - Pour une instance de base de données existante, vous appliquez le groupe d'options en modifiant l'instance et en attachant le nouveau groupe d'options. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

AWS CLI

L'exemple suivant utilise la commande add-option-to-option-group de l'AWS CLI pour ajouter l'option `OEM_AGENT` à un groupe d'options appelé `myoptiongroup`.

Pour Linux, macOS ou 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
```

Pour 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
```

Utilisation de l'option Management Agent

Lorsque vous avez activé l'option Management Agent, exécutez les étapes suivantes pour commencer à l'utiliser.

Pour utiliser l'option Management Agent

1. Déverrouillez et réinitialisez les informations d'identification de compte DBSNMP. Pour cela, exécutez le code suivant sur votre base de données cible de votre instance de base de données en utilisant votre compte utilisateur principal.

   ```
   ALTER USER dbsnmp IDENTIFIED BY new_password ACCOUNT UNLOCK;
   ```

2. Ajoutez vos cibles dans la console OMS manuellement :

   a. Dans la console OMS, choisissez Setup (Configuration), Add Target (Ajouter une cible), Add Targets Manually (Ajouter des cibles manuellement).
   b. Choisissez Add Targets Declaratively by Specifying Target Monitoring Properties (Ajouter déclarativement des cibles en spécifiant les propriétés de surveillance cibles).
   c. Pour Target Type (Type de cible), choisissez Database Instance (Instance de base de données).
   d. Pour Monitoring Agent (Agent de surveillance), sélectionnez l'agent ayant le même identifiant que votre identifiant d'instance de base de données RDS.
   e. Choisissez Add Manually (Ajouter manuellement).
   f. Entrez le point de terminaison de l'instance de base de données Amazon RDS ou sélectionnez-le dans la liste de noms d'hôte. Vérifiez que le nom d'hôte spécifié correspond au point de terminaison de l'instance de base de données Amazon RDS.

      Pour plus d'informations sur la recherche du point de terminaison de votre instance de base de données Amazon RDS, consultez Recherche du point de terminaison de votre instance de base de données (p. 961).
   g. Spécifiez les propriétés de base de données suivantes :

      - Pour Target Name (Nom de la cible), entrez un nom.
      - Pour Database system name (Nom du système de base de données), entrez un nom.
      - Pour Monitor username (Nom d'utilisateur de surveillance), entrez **dbsnmp**.
      - Pour Monitor password (Mot de passe de surveillance), entrez le mot de passe de l'étape 1.
      - Pour Role (Rôle), entrez normal.
      - Pour Oracle home path (Chemin d'origine Oracle), entrez **/oracle**.
      - Pour Listener Machine name (Nom de machine d'écouteur), l'identifiant de l'agent est déjà affiché.
      - Pour Port, entrez le port de la base de données. La port RDS par défaut est 1521.
      - Pour Database name (Nom de la base de données), entrez le nom de votre base de données.
   h. Choisissez Test Connection (Connexion test).
   i. Choisissez Suivant. La base de données cible apparaît dans votre liste de ressources surveillées.

Modification des paramètres de l'agent de gestion

Lorsque vous avez activé l'agent de gestion, vous pouvez modifier les paramètres de l'option. Pour plus d'informations sur la modification des paramètres d'options, consultez Modification d'un paramètre d'option (p. 219). Pour plus d'informations sur chaque paramètre, consultez Paramètres de l'option Management Agent (p. 1044).

Exécution de tâches de base de données avec l'option Management Agent

Vous pouvez utiliser les procédures Amazon RDS pour exécuter certaines commandes EMCTL sur Management Agent. Ces procédures vous permettent d'exécuter les tâches indiquées ci-après.

> Note
>
> Les tâches sont exécutées de manière asynchrone.

Tâches

- Obtenir le statut de l'agent de gestion (p. 1049)
- Redémarrage du Management Agent (p. 1049)
- Liste des cibles surveillées par le Management Agent (p. 1049)
- Constitution de la liste des threads de collecte surveillés par Management Agent (p. 1050)
- Suppression de l'état du Management Agent (p. 1050)
- Chargement de l'OMS par le Management Agent (p. 1050)
- Envoi de la commande Ping vers l'OMS (p. 1051)
- Affichage du statut d'une tâche en cours (p. 1051)

Obtenir le statut de l'agent de gestion

Pour obtenir le statut de l'agent de gestion, exécutez la procédure Amazon RDS `rdsadmin.rdsadmin_oem_agent_tasks.get_status_oem_agent`. Cette procédure est équivalente à la commande `emctl status agent`.

La procédure suivante crée une tâche permettant d'obtenir le statut du Management Agent et renvoie l'ID de la tâche.

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.get_status_oem_agent() as TASK_ID from DUAL;
```

Pour voir le résultat en affichant le fichier de sortie de la tâche, veuillez consulter Affichage du statut d'une tâche en cours (p. 1051).

Redémarrage du Management Agent

Pour redémarrer le Management Agent, exécutez la procédure Amazon RDS `rdsadmin.rdsadmin_oem_agent_tasks.get_status_oem_agent`. Cette procédure équivaut à exécuter les commandes `emctl stop agent` et `emctl start agent`.

La procédure suivante crée une tâche permettant de redémarrer Management Agent et renvoie l'ID de la tâche.

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.restart_oem_agent() as TASK_ID from DUAL;
```

Pour voir le résultat en affichant le fichier de sortie de la tâche, veuillez consulter Affichage du statut d'une tâche en cours (p. 1051).

Liste des cibles surveillées par le Management Agent

Pour répertorier les cibles surveillées par le Management Agent, exécutez la procédure Amazon RDS `rdsadmin.rdsadmin_oem_agent_tasks.list_targets_oem_agent`. Cette procédure équivaut à exécuter la commande `emctl config agent listtargets`.

La procédure suivante crée une tâche pour répertorier les cibles surveillées par Management Agent et renvoie l'ID de la tâche.

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.list_targets_oem_agent() as TASK_ID from DUAL;
```

Pour voir le résultat en affichant le fichier de sortie de la tâche, veuillez consulter Affichage du statut d'une tâche en cours (p. 1051).

Constitution de la liste des threads de collecte surveillés par Management Agent

Pour répertorier tous les threads de collecte (en cours d'exécution, prêts et planifiés) surveillés par Management Agent, exécutez la procédure Amazon RDS `rdsadmin.rdsadmin_oem_agent_tasks.list_clxn_threads_oem_agent`. Cette procédure est équivalente à la commande `emctl status agent scheduler`.

La procédure suivante crée une tâche pour répertorier les threads de collecte et renvoie l'ID de la tâche.

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.list_clxn_threads_oem_agent() as TASK_ID from
 DUAL;
```

Pour voir le résultat en affichant le fichier de sortie de la tâche, veuillez consulter Affichage du statut d'une tâche en cours (p. 1051).

Suppression de l'état du Management Agent

Pour supprimer l'état du Management Agent, exécutez la procédure Amazon RDS `rdsadmin.rdsadmin_oem_agent_tasks.clearstate_oem_agent`. Cette procédure équivaut à exécuter la commande `emctl clearstate agent`.

La procédure suivante crée une tâche permettant d'annuler le statut de Management Agent et renvoie l'ID de la tâche.

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.clearstate_oem_agent() as TASK_ID from DUAL;
```

Pour voir le résultat en affichant le fichier de sortie de la tâche, veuillez consulter Affichage du statut d'une tâche en cours (p. 1051).

Chargement de l'OMS par le Management Agent

Pour que le Management Agent charge l'OMS (Oracle Management Server) qui lui est associé, exécutez la procédure Amazon RDS `rdsadmin.rdsadmin_oem_agent_tasks.upload_oem_agent`. Cette procédure équivaut à exécuter la commande `emclt upload agent`.

La procédure suivante crée une tâche dans laquelle Management Agent charge son OMS associé et renvoie l'ID de la tâche.

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.upload_oem_agent() as TASK_ID from DUAL;
```

Pour voir le résultat en affichant le fichier de sortie de la tâche, veuillez consulter Affichage du statut d'une tâche en cours (p. 1051).

Envoi de la commande Ping vers l'OMS

Pour envoyer la commande Ping à l'OMS du Management Agent, exécutez la procédure Amazon RDS `rdsadmin.rdsadmin_oem_agent_tasks.ping_oms_oem_agent`. Cette procédure équivaut à exécuter la commande `emctl pingOMS`.

La procédure suivante crée une tâche permettant de pinger l'OMS de Management Agent et renvoie l'ID de la tâche.

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.ping_oms_oem_agent() as TASK_ID from DUAL;
```

Pour voir le résultat en affichant le fichier de sortie de la tâche, veuillez consulter Affichage du statut d'une tâche en cours (p. 1051).

Affichage du statut d'une tâche en cours

Vous pouvez consulter le statut d'une tâche en cours dans un fichier bdump. Les fichiers bdump se trouvent dans le répertoire `/rdsdbdata/log/trace`. Chaque nom de fichier bdump a le format suivant.

```
dbtask-task-id.log
```

Lorsque vous souhaitez surveiller une tâche, remplacez *`task-id`* par l'ID de la tâche que vous souhaitez surveiller.

Pour afficher le contenu des fichiers bdump, exécutez la procédure Amazon RDS `rdsadmin.rds_file_util.read_text_file`. La requête suivante renvoie le contenu du fichier bdump `dbtask-1546988886389-2444.log`.

```
SELECT text FROM
 table(rdsadmin.rds_file_util.read_text_file('BDUMP','dbtask-1546988886389-2444.log'));
```

Pour de plus amples informations sur la procédure Amazon RDS `rdsadmin.rds_file_util.read_text_file`, veuillez consulter Lecture de fichiers dans un répertoire d'instance de base de données (p. 1166).

Suppression de l'option Management Agent

Vous pouvez supprimer l'agent OEM d'une instance de base de données. Lorsque vous avez supprimé l'agent OEM, vous n'avez pas besoin de redémarrer votre instance de base de données.

Pour supprimer l'agent OEM d'une instance de base de données, effectuez l'une des actions suivantes :

- Supprimez l'option OEM Agent du groupe d'options auquel elle appartient. Ce changement affecte toutes les instances de bases de données qui utilisent le groupe d'options. Pour plus d'informations, consultez Suppression d'une option d'un groupe d'options (p. 222).
- Modifiez l'instance de base de données et spécifiez un groupe d'options différent qui n'inclut pas l'option OEM Agent. Ce changement affecte une seule instance de base de données. Vous pouvez spécifier le groupe d'options (vide) par défaut, ou un groupe d'options personnalisées différent. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Oracle Java Virtual Machine

Amazon RDS prend en charge Oracle Java Virtual Machine (JVM) par l'intermédiaire de l'option `JVM`. Oracle Java fournit un schéma SQL et des fonctions facilitant les fonctionnalités Oracle Java dans une base de données Oracle. Pour de plus amples informations, veuillez consulter Introduction to Java in Oracle Database dans la documentation Oracle.

Vous pouvez utiliser Oracle JVM avec les versions Oracle Database suivantes :

- Oracle 19c, 19.0.0.0, toutes les versions
- Oracle 18c, 18.0.0.0, toutes les versions
- Oracle 12c, 12.2.0.1, toutes les versions
- Oracle 12c, 12.1.0.2.v13 ou versions ultérieures
- Oracle 11g, 11.2.0.4.v17 ou versions ultérieures

L'implémentation Java dans Amazon RDS a un jeu d'autorisations limité. L'utilisateur principal dispose du rôle `RDS_JAVA_ADMIN`, qui attribue un sous-ensemble des privilèges associés au rôle `JAVA_ADMIN`. Afin de répertorier les privilèges attribués au rôle `RDS_JAVA_ADMIN`, exécutez la requête suivante sur votre instance de base de données :

```
SELECT * FROM dba_java_policy
   WHERE grantee IN ('RDS_JAVA_ADMIN', 'PUBLIC')
   AND enabled = 'ENABLED'
   ORDER BY type_name, name, grantee;
```

Prérequis pour Oracle JVM

Les conditions suivantes sont requises pour utiliser Oracle Java :

- Votre instance de base de données doit être dans un Virtual Private Cloud (VPC). Pour plus d'informations, consultez Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611).
- Votre instance de base de données doit être d'une classe de taille suffisante. Oracle Java n'est pas pris en charge pour les classes d'instance de base de données db.t3.micro ou db.t3.small. Pour plus d'informations, consultez Classes d'instances de base de données (p. 6).
- Votre instance de base de données doit avoir l'option Auto Minor Version Upgrade (Mise à niveau automatique des versions mineures) activée. Cette option permet à votre instance de base de données de recevoir des mises à niveau mineures de version de moteur de base de données automatiquement, dès qu'elles sont disponibles. Amazon RDS utilise cette option pour mettre à jour votre instance de base de données avec le dernier correctif Oracle Patch Set Update (PSU) ou la mise à jour version Release Update (RU). Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).
- Si votre instance de base de données s'exécute sur la version majeure 11.2, vous devez installer l'option `XMLDB`. Pour plus d'informations, consultez Oracle XML DB (p. 1096).

Bonnes pratiques pour Oracle JVM

Les bonnes pratiques suivantes sont requises pour utiliser Oracle Java :

- Pour une sécurité maximale, utilisez l'option `JVM` avec Secure Sockets Layer (SSL). Pour plus d'informations, consultez Oracle Secure Sockets Layer (SSL) (p. 1068).

- Configurez votre instance de base de données afin de restreindre l'accès réseau. Pour plus d'informations, consultez Scénarios d'accès à une instance de base de données d'un VPC (p. 1613) et Utilisation d'une instance de base de données dans un VPC (p. 1620).

Ajout de l'option Oracle JVM

La procédure générale suivante permet d'ajouter l'option `JVM` à une instance de base de données :

1. Créer un groupe d'options ou copier ou modifier un groupe existant.
2. Ajouter l'option au groupe d'options.
3. Associer un groupe d'options à une instance de base de données.

L'ajout de l'option `JVM` entraîne une brève indisponibilité. Une fois que vous ajoutez l'option , vous n'avez pas besoin de redémarrer votre instance de base de données. Dès que le groupe d'options est actif, Oracle Java est disponible.

> **Note**
>
> Durant cette interruption, les fonctions de vérification de mot de passe sont brièvement désactivées. Vous pouvez également vous attendre à voir des événements liés aux fonctions de vérification de mot de passe durant l'interruption. Les fonctions de vérification de mot de passe sont activées de nouveau avant que l'instance de base de données Oracle ne soit disponible.

Pour ajouter l'option JVM à une instance de base de données

1. Déterminez le groupe d'options que vous voulez utiliser. Vous pouvez créer un groupe d'options ou utiliser un groupe d'options existant. Si vous souhaitez utiliser un groupe d'options existant, passez à l'étape suivante. Sinon, créez un groupe d'options DB personnalisé avec les paramètres suivants :

   - Pour Moteur, choisissez le moteur de base de données utilisé par l'instance de base de données (oracle-ee, oracle-se, oracle-se1 ou oracle-se2).
   - Pour Version majeure du moteur, choisissez la version de votre instance de base de données.

   Pour de plus amples informations, veuillez consulter Création d'un groupe d'options (p. 212).
2. Ajouter l'option JVM au groupe d'options. Pour plus d'informations sur l'ajout d'options, consultez Ajout d'une option à un groupe d'options (p. 214).
3. Appliquez le groupe d'options à une instance de base de données nouvelle ou existante:

   - Pour une nouvelle instance de base de données, appliquez le groupe d'options lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).
   - Pour une instance de base de données existante, appliquez le groupe d'options en modifiant l'instance et en attachant le nouveau groupe d'options. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).
4. Accordez les autorisations requises aux utilisateurs.

   L'utilisateur principal Amazon RDS est autorisé à utiliser l'option `JVM` par défaut. Si d'autres utilisateurs ont besoin de ces permissions, connectez-vous à l'instance de base de données en tant qu'utilisateur principal dans un client SQL et accordez les autorisations aux utilisateurs.

   L'exemple suivant accorde les autorisation d'utiliser l'option `JVM` à l'utilisateur `test_proc`.

```
create user test_proc identified by password;
```

```
CALL dbms_java.grant_permission('TEST_PROC',
 'oracle.aurora.security.JServerPermission', 'LoadClassInPackage.*', '');
```

Une fois que les autorisations sont accordées à l'utilisateur, la requête suivante doit renvoyer un résultat.

```
select * from dba_java_policy where grantee='TEST_PROC';
```

> **Note**
>
> Le nom d'utilisateur Oracle est sensible à la casse et comportent généralement seulement des caractères majuscules.

Suppression de l'option Oracle JVM

Vous pouvez supprimer l'option `JVM` d'une instance de base de données. La suppression de l'option entraîne une brève indisponibilité. Une fois que vous supprimez l'option `JVM`, vous n'avez pas besoin de redémarrer votre instance de base de données.

> **Warning**
>
> La suppression de l'option `JVM` peut entraîner une perte de données si l'instance de base de données utilise des types de données qui ont été activés avec cette option. Sauvegardez vos données avant de continuer. Pour plus d'informations, consultez Sauvegarde et restauration d'une instance de base de données Amazon RDS (p. 317).

Pour supprimer l'option `JVM` d'une instance de base de données, effectuez l'une des actions suivantes :

- Supprimez l'option `JVM` du groupe d'options auquel elle appartient. Ce changement affecte toutes les instances de bases de données qui utilisent le groupe d'options. Pour plus d'informations, consultez Suppression d'une option d'un groupe d'options (p. 222).
- Modifiez l'instance de base de données et spécifiez un groupe d'options différent qui n'inclut pas l'option `JVM`. Ce changement affecte une seule instance de base de données. Vous pouvez spécifier le groupe d'options (vide) par défaut, ou un groupe d'options personnalisées différent. Pour de plus amples informations, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

Oracle Label Security

Amazon RDS prend en charge Oracle Label Security pour Oracle Enterprise Edition, version 12c, grâce à l'utilisation de l'option OLS.

La plupart des contrôles de sécurité de base de données accèdent au niveau de l'objet. Oracle Label Security offre un contrôle d'accès précis aux lignes de table individuelles. Par exemple, vous pouvez utiliser Label Security pour assurer la conformité réglementaire avec un modèle d'administration basé sur stratégie. Vous pouvez utiliser des stratégies Label Security pour contrôler l'accès aux données sensibles et limiter l'accès aux seuls utilisateurs dotés du niveau d'autorisation approprié. Pour plus d'informations, consultez Introduction to Oracle Label Security dans la documentation Oracle.

> **Important**
>
> Pour Oracle 19c, Oracle 18c et Oracle 12c version 12.2 sur Amazon RDS, Oracle Label Security est une option permanente et persistante. Vous ne pouvez pas supprimer Oracle Label Security d'une instance de base de données Oracle version 19c, 18c ou 12.2.

Prérequis pour Oracle Label Security

Pour pouvoir utiliser Oracle Label Security, vous devez impérativement disposer des éléments suivants :

- Votre instance de base de données doit utiliser le modèle Bring Your Own License. Pour plus d'informations, consultez Options de licence Oracle (p. 930).
- Vous devez disposer d'une licence valide pour Oracle Enterprise Edition avec la licence de mise à jour du logiciel et le support.
- Votre licence Oracle doit inclure l'option Label Security.

Ajout de l'option Oracle Label Security

Le processus général d'ajout de l'option Oracle Label Security à une instance de base de données est le suivant :

1. Créer un groupe d'options ou copier ou modifier un groupe existant.
2. Ajouter l'option au groupe d'options.
3. Associez le groupe d'options à l'instance de base de données.

Lorsque vous ajoutez l'option Label Security, dès que le groupe d'options est actif, l'option Label Security est active.

Pour ajouter l'option Label Security à une instance de base de données

1. Déterminez le groupe d'options que vous voulez utiliser. Vous pouvez créer un groupe d'options ou utiliser un groupe d'options existant. Si vous souhaitez utiliser un groupe d'options existant, passez à l'étape suivante. Sinon, créez un groupe d'options DB personnalisé avec les paramètres suivants :

   a. Pour Moteur, choisissez oracle-ee.

   b. Pour Version majeure du moteur, choisissez la version de votre instance de base de données.

   Pour de plus amples informations, veuillez consulter Création d'un groupe d'options (p. 212).
2. Ajouter l'option OLS au groupe d'options. Pour de plus amples informations sur l'ajout d'options, veuillez consulter Ajout d'une option à un groupe d'options (p. 214).

   > **Important**
   >
   > Si vous ajoutez l'option Label Security dans un groupe d'options existant qui est déjà attaché à une ou plusieurs instances de base de données, toutes les instances de base de données sont redémarrées.
3. Appliquez le groupe d'options à une instance de base de données nouvelle ou existante:

   - Pour une nouvelle instance de base de données, vous appliquez le groupe d'options lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).
   - Pour une instance de base de données existante, vous appliquez le groupe d'options en modifiant l'instance et en attachant le nouveau groupe d'options. Lorsque vous ajoutez l'option Label Security à une instance de base de données existante, une brève panne se produit pendant le redémarrage automatique de votre instance de base de données. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Utilisation d'Oracle Label Security

Pour utiliser Oracle Label Security, vous créez des stratégies qui contrôlent l'accès à des lignes spécifiques dans vos tables. Pour plus d'informations, consultez Creating an Oracle Label Security Policy (Créer une stratégie Oracle Label Security) dans la documentation Oracle.

Lorsque vous travaillez avec Label Security, vous effectuez toutes les actions au rôle de LBAC_DBA. L'utilisateur principal pour votre instance de base de données se voit accorder le rôle LBAC_DBA. Vous pouvez accorder le rôle LBAC_DBA à d'autres utilisateurs pour leur permettre d'administrer des stratégies Label Security.

Pour les instances de bases de données Amazon RDS pour Oracle 19c, 18c et 12.2, vous devez accorder l'accès au package `OLS_ENFORCEMENT` à tous les nouveaux utilisateurs qui ont besoin d'accéder à Oracle Label Security. Pour accorder l'accès au package `OLS_ENFORCEMENT`, connectez-vous à l'instance de base de données en tant qu'utilisateur principal, puis exécutez l'instruction SQL suivante :

```
GRANT ALL ON LBACSYS.OLS_ENFORCEMENT TO username;
```

Vous pouvez configurer Label Security via Oracle Enterprise Manager (OEM) Cloud Control. Amazon RDS prend en charge OEM Cloud Control via l'option Management Agent. Pour plus d'informations, consultez Oracle Management Agent pour Enterprise Manager Cloud Control (p. 1042).

Suppression de l'option Oracle Label Security

Vous pouvez supprimer Oracle Label Security sur une instance de base de données.

Pour supprimer Label Security sur une instance de base de données, effectuez l'une des actions suivantes :

- Pour supprimer Label Security sur plusieurs instances de base de données, supprimez l'option Label Security du groupe d'options auquel elles appartiennent. Ce changement affecte toutes les instances de bases de données qui utilisent le groupe d'options. Lorsque vous supprimez Label Security sur un groupe d'options qui est attaché à plusieurs instances de base de données, toutes les instances de base de données sont redémarrées. Pour plus d'informations, consultez Suppression d'une option d'un groupe d'options (p. 222).
- Pour supprimer Label Security d'une instance de base de données particulière, modifiez l'instance de base de données et spécifiez un autre groupe d'options qui n'inclut pas l'option Label Security. Vous pouvez spécifier le groupe d'options (vide) par défaut, ou un groupe d'options personnalisées différent. Lorsque vous supprimez l'option Label Security, une brève panne se produit pendant le redémarrage automatique de votre instance de base de données. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Dépannage

Ci-après des problèmes que vous pouvez rencontrer en utilisant Oracle Label Security.

Problème	Suggestions de dépannage
Lorsque vous essayez de créer une stratégie, vous voyez un message d'erreur similaire à ce qui suit : `insufficient authorization for the SYSDBA package`.	Un problème connu avec la fonctionnalité Label Security d'Oracle empêche les utilisateurs avec des noms d'utilisateur de 16 ou 24 caractères d'exécuter des commandes Label Security.

Problème	Suggestions de dépannage
	Vous pouvez créer un nouvel utilisateur comportant un nombre différent de caractères, accorder LBAC_DBA au nouvel utilisateur, vous connecter comme le nouvel utilisateur et exécuter les commandes OLS en tant que ce nouvel utilisateur. Pour plus d'informations, veuillez contacter le support d'Oracle.

Oracle Locator

Amazon RDS prend en charge Oracle Locator par l'intermédiaire de l'option `LOCATOR`. Oracle Locator fournit des capacités généralement requises pour prendre en charge les applications basées sur des services sans fil et sur Internet, ainsi que les solutions GIS basées sur le partenariat. Oracle Locator est un sous-ensemble limité d'Oracle Spatial. Pour plus d'informations, consultez Oracle Locator dans la documentation d'Oracle.

> **Important**
>
> Si vous utilisez Oracle Locator, Amazon RDS met automatiquement à jour votre instance de base de données vers le PSU Oracle le plus récent en cas de vulnérabilités de sécurité présentant un score de Common Vulnerability Scoring System (CVSS) égal ou supérieur à 9, ou d'autres vulnérabilités de sécurité annoncées.

Amazon RDS prend en charge Oracle Locator pour les éditions et versions suivantes d'Oracle :

- Oracle Standard Edition (SE2) ou Enterprise Edition, version 19.0.0.0, toutes les versions
- Oracle Standard Edition (SE2) ou Enterprise Edition, version 18.0.0.0, toutes les versions
- Oracle Standard Edition (SE2) ou Enterprise Edition, version 12.2.0.1, toutes les versions
- Oracle Standard Edition (SE2) ou Enterprise Edition, version 12.1.0.2.v13 ou ultérieure
- Oracle Standard Edition (SE, SE1) ou Enterprise Edition, version 11.2.0.4.v17 ou ultérieure

Prérequis pour Oracle Locator

Les conditions suivantes sont requises pour utiliser Oracle Locator :

- Votre instance de base de données doit être dans un Virtual Private Cloud (VPC). Pour plus d'informations, consultez Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611).
- Votre instance de base de données doit être d'une classe suffisante. Oracle Locator n'est pas pris en charge pour les classes d'instance de base de données db.t3.micro ou db.t3.small. Pour plus d'informations, consultez Prise en charge des classes d'instance de base de données pour Oracle (p. 933).
- Votre instance de base de données doit avoir l'option Auto Minor Version Upgrade (Mise à niveau automatique des versions mineures) activée. Cette option permet à votre instance de base de données de recevoir automatiquement des mises à niveau mineures de version du moteur de base de données lorsqu'elles sont disponibles et est requise pour toutes les options qui installent la machine virtuelle Java Oracle (JVM). Amazon RDS utilise cette option pour mettre à jour votre instance de base de données avec le dernier correctif Oracle Patch Set Update (PSU) ou la dernière mise à jour de version (RU). Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

- Si votre instance de base de données s'exécute sur la version majeure 11.2, vous devez installer l'option `XMLDB`. Pour plus d'informations, consultez Oracle XML DB (p. 1096).

Bonnes pratiques pour Oracle Locator

Les bonnes pratiques suivantes sont requises pour utiliser Oracle Locator :

- Pour une sécurité maximale, utilisez l'option `LOCATOR` avec Secure Sockets Layer (SSL). Pour plus d'informations, consultez Oracle Secure Sockets Layer (SSL) (p. 1068).
- Configurez votre instance de base de données pour en restreindre l'accès. Pour plus d'informations, consultez Scénarios d'accès à une instance de base de données d'un VPC (p. 1613) et Utilisation d'une instance de base de données dans un VPC (p. 1620).

Ajout de l'option Oracle Locator

La procédure générale suivante permet d'ajouter l'option `LOCATOR` à une instance de base de données :

1. Créer un groupe d'options ou copier ou modifier un groupe existant.
2. Ajouter l'option au groupe d'options.
3. Associez le groupe d'options à l'instance de base de données.

Si Oracle Java Virtual Machine (JVM) n'est pas installé sur l'instance de base de données, il y a une brève panne lorsque l'option `LOCATOR` est ajoutée. Il n'y a pas de panne si Oracle Java Virtual Machine (JVM) est déjà installé sur l'instance de base de données. Une fois que vous ajoutez l'option, vous n'avez pas besoin de redémarrer votre instance de base de données. Dès que le groupe d'options est actif, Oracle Locator est disponible.

> **Note**
>
> Durant cette interruption, les fonctions de vérification de mot de passe sont brièvement désactivées. Vous pouvez également vous attendre à voir des événements liés aux fonctions de vérification de mot de passe durant l'interruption. Les fonctions de vérification de mot de passe sont activées de nouveau avant que l'instance de base de données Oracle ne soit disponible.

Pour ajouter l'option **`LOCATOR`** à une instance de base de données

1. Déterminez le groupe d'options que vous voulez utiliser. Vous pouvez créer un groupe d'options ou utiliser un groupe d'options existant. Si vous souhaitez utiliser un groupe d'options existant, passez à l'étape suivante. Sinon, créez un groupe d'options DB personnalisé avec les paramètres suivants :

   a. Pour Moteur, choisissez l'édition oracle pour votre instance de base de données.
   b. Pour Version majeure du moteur, choisissez la version de votre instance de base de données.

   Pour de plus amples informations, veuillez consulter Création d'un groupe d'options (p. 212).
2. Ajoutez l'option LOCATOR au groupe d'options. Pour plus d'informations sur l'ajout d'options, consultez Ajout d'une option à un groupe d'options (p. 214).
3. Appliquez le groupe d'options à une instance de base de données nouvelle ou existante:

   - Pour une nouvelle instance de base de données, vous appliquez le groupe d'options lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).
   - Pour une instance de base de données existante, vous appliquez le groupe d'options en modifiant l'instance et en attachant le nouveau groupe d'options. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Utilisation d'Oracle Locator

Une fois que vous activez l'option Oracle Locator, vous pouvez commencer à l'utiliser. Utilisez uniquement les fonctions Oracle Locator. N'utilisez pas les fonctions Oracle Spatial, sauf si vous avez la licence correspondante.

Pour obtenir la liste des fonctions prises en charge pour Oracle Locator, consultez Fonctions incluses avec Locator dans la documentation d'Oracle.

Pour obtenir la liste des fonctions qui ne sont pas prises en charge pour Oracle Locator, consultez Fonctions non incluses avec Locator dans la documentation d'Oracle.

Suppression de l'option Oracle Locator

Après avoir supprimé tous les objets qui utilisent des types de données fournis par l'option `LOCATOR`, vous pouvez supprimer l'option d'une instance de base de données. Si Oracle Java Virtual Machine (JVM) n'est pas installé sur l'instance de base de données, il y a une brève panne lorsque l'option `LOCATOR` est supprimée. Il n'y a pas de panne si Oracle Java Virtual Machine (JVM) est déjà installé sur l'instance de base de données. Une fois que vous supprimez l'option `LOCATOR`, vous n'avez pas besoin de redémarrer votre instance de base de données.

Pour supprimer l'option **`LOCATOR`**

1. Sauvegardez vos données.

   Warning

   Si l'instance utilise des types de données qui ont été activés dans le cadre de l'option, et si vous supprimez l'option `LOCATOR`, vous pouvez perdre des données. Pour plus d'informations, consultez Sauvegarde et restauration d'une instance de base de données Amazon RDS (p. 317).

2. Vérifiez si des objets existants font référence à des types de données ou à des fonctionnalités de l'option `LOCATOR`.

   Si des options `LOCATOR` existent, l'instance peut rester bloquée lors de l'application du nouveau groupe d'options qui n'a pas l'option `LOCATOR`. Vous pouvez identifier les objets à l'aide des requêtes suivantes :

```
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. Supprimez tous les objets qui font référence à des types de données ou à des fonctionnalités de l'option `LOCATOR`.
4. Effectuez l'une des actions suivantes :

- Supprimez l'option `LOCATOR` du groupe d'options auquel elle appartient. Ce changement affecte toutes les instances de bases de données qui utilisent le groupe d'options. Pour plus d'informations, consultez Suppression d'une option d'un groupe d'options (p. 222).
- Modifiez l'instance de base de données et spécifiez un groupe d'options différent qui n'inclut pas l'option `LOCATOR`. Ce changement affecte une seule instance de base de données. Vous pouvez spécifier le groupe d'options (vide) par défaut, ou un groupe d'options personnalisées différent. Pour de plus amples informations, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

Oracle Multimedia

Amazon RDS prend en charge Oracle Multimedia par l'intermédiaire de l'option `MULTIMEDIA`. Vous pouvez utiliser Oracle Multimedia pour stocker, gérer et récupérer des images, des fichiers audio et vidéo, ainsi que d'autres données multimédias hétérogènes. Pour plus d'informations, consultez Oracle Multimedia dans la documentation d'Oracle.

> **Important**
>
> Si vous utilisez Oracle Multimedia, Amazon RDS met automatiquement à jour votre instance de base de données vers le PSU Oracle le plus récent en cas de vulnérabilités de sécurité présentant un score de Common Vulnerability Scoring System (CVSS) égal ou supérieur à 9, ou d'autres vulnérabilités de sécurité annoncées.

Amazon RDS prend en charge Oracle Multimedia pour les éditions et versions suivantes d'Oracle :

- Oracle Standard Edition (SE2) ou Oracle Enterprise Edition, version 18.0.0.0, toutes les versions
- Oracle Standard Edition (SE2) ou Oracle Enterprise Edition, version 12.2.0.1, toutes les versions
- Oracle Standard Edition (SE2) ou Oracle Enterprise Edition, version 12.1.0.2.v13 ou ultérieure
- Oracle Standard Edition (SE, SE1) ou Oracle Enterprise Edition, version 11.2.0.4.v17 ou ultérieure

> **Note**
>
> Oracle a annulé la prise en charge d'Oracle Multimedia dans Oracle Database 19c. Donc, Oracle Multimedia n'est pas pris en charge pour les instances de bases de données Oracle 19c. Pour de plus amples informations, veuillez consulter Desupport of Oracle Multimedia dans la documentation Oracle.

Prérequis pour Oracle Multimedia

Les conditions suivantes sont requises pour utiliser Oracle Multimedia :

- Votre instance de base de données doit être dans un Virtual Private Cloud (VPC). Pour plus d'informations, consultez Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611).
- Votre instance de base de données doit être d'une classe suffisante. Oracle Multimedia n'est pas pris en charge pour les classes d'instance de base de données db.t3.micro ou db.t3.small. Pour plus d'informations, consultez Prise en charge des classes d'instance de base de données pour Oracle (p. 933).
- Votre instance de base de données doit avoir l'option Auto Minor Version Upgrade (Mise à niveau automatique des versions mineures) activée. Cette option permet à votre instance de base de données de recevoir automatiquement des mises à niveau mineures de version du moteur de base de données lorsqu'elles sont disponibles et est requise pour toutes les options qui installent la machine virtuelle Java Oracle (JVM). Amazon RDS utilise cette option pour mettre à jour votre instance de base de données

avec le dernier correctif Oracle Patch Set Update (PSU) ou la dernière mise à jour de version (RU). Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).
- Si votre instance de base de données s'exécute sur la version majeure 11.2, vous devez installer l'option `XMLDB`. Pour plus d'informations, consultez Oracle XML DB (p. 1096).

Bonnes pratiques pour Oracle Multimedia

Les bonnes pratiques suivantes sont requises pour utiliser Oracle Multimedia :

- Pour une sécurité maximale, utilisez l'option `MULTIMEDIA` avec Secure Sockets Layer (SSL). Pour plus d'informations, consultez Oracle Secure Sockets Layer (SSL) (p. 1068).
- Configurez votre instance de base de données pour en restreindre l'accès. Pour plus d'informations, consultez Scénarios d'accès à une instance de base de données d'un VPC (p. 1613) et Utilisation d'une instance de base de données dans un VPC (p. 1620).

Ajout de l'option Oracle Multimedia

La procédure générale suivante permet d'ajouter l'option `MULTIMEDIA` à une instance de base de données :

1. Créer un groupe d'options ou copier ou modifier un groupe existant.
2. Ajouter l'option au groupe d'options.
3. Associez le groupe d'options à l'instance de base de données.

Si Oracle Java Virtual Machine (JVM) n'est pas installé sur l'instance de base de données, il y a une brève panne lorsque l'option `MULTIMEDIA` est ajoutée. Il n'y a pas de panne si Oracle Java Virtual Machine (JVM) est déjà installé sur l'instance de base de données. Une fois que vous ajoutez l'option, vous n'avez pas besoin de redémarrer votre instance de base de données. Dès que le groupe d'options est actif, Oracle Multimedia est disponible.

> **Note**
>
> Durant cette interruption, les fonctions de vérification de mot de passe sont brièvement désactivées. Vous pouvez également vous attendre à voir des événements liés aux fonctions de vérification de mot de passe durant l'interruption. Les fonctions de vérification de mot de passe sont activées de nouveau avant que l'instance de base de données Oracle ne soit disponible.

Pour ajouter l'option **`MULTIMEDIA`** à une instance de base de données

1. Déterminez le groupe d'options que vous voulez utiliser. Vous pouvez créer un groupe d'options ou utiliser un groupe d'options existant. Si vous souhaitez utiliser un groupe d'options existant, passez à l'étape suivante. Sinon, créez un groupe d'options DB personnalisé avec les paramètres suivants :

   a. Pour Moteur, choisissez oracle-ee.
   b. Pour Version majeure du moteur, choisissez la version de votre instance de base de données.

   Pour de plus amples informations, veuillez consulter Création d'un groupe d'options (p. 212).
2. Ajoutez l'option MULTIMEDIA au groupe d'options. Pour plus d'informations sur l'ajout d'options, consultez Ajout d'une option à un groupe d'options (p. 214).
3. Appliquez le groupe d'options à une instance de base de données nouvelle ou existante:

   - Pour une nouvelle instance de base de données, vous appliquez le groupe d'options lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).

- Pour une instance de base de données existante, vous appliquez le groupe d'options en modifiant l'instance et en attachant le nouveau groupe d'options. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Suppression de l'option Oracle Multimedia

Après avoir supprimé tous les objets qui utilisent des types de données fournis par l'option `MULTIMEDIA`, vous pouvez supprimer l'option d'une instance de base de données. Si Oracle Java Virtual Machine (JVM) n'est pas installé sur l'instance de base de données, il y a une brève panne lorsque l'option `MULTIMEDIA` est supprimée. Il n'y a pas de panne si Oracle Java Virtual Machine (JVM) est déjà installé sur l'instance de base de données. Une fois que vous supprimez l'option `MULTIMEDIA`, vous n'avez pas besoin de redémarrer votre instance de base de données.

Pour supprimer l'option **`MULTIMEDIA`**

1. Sauvegardez vos données.

   Warning

   Si l'instance utilise des types de données qui ont été activés dans le cadre de l'option, et si vous supprimez l'option `MULTIMEDIA`, vous pouvez perdre des données. Pour de plus amples informations, veuillez consulter Sauvegarde et restauration d'une instance de base de données Amazon RDS (p. 317).
2. Vérifiez si des objets existants font référence à des types de données ou à des fonctionnalités de l'option `MULTIMEDIA`.
3. Supprimez tous les objets qui font référence à des types de données ou à des fonctionnalités de l'option `MULTIMEDIA`.
4. Effectuez l'une des actions suivantes :

   - Supprimez l'option `MULTIMEDIA` du groupe d'options auquel elle appartient. Ce changement affecte toutes les instances de bases de données qui utilisent le groupe d'options. Pour plus d'informations, consultez Suppression d'une option d'un groupe d'options (p. 222).
   - Modifiez l'instance de base de données et spécifiez un groupe d'options différent qui n'inclut pas l'option `MULTIMEDIA`. Ce changement affecte une seule instance de base de données. Vous pouvez spécifier le groupe d'options (vide) par défaut, ou un groupe d'options personnalisées différent. Pour de plus amples informations, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

Oracle NNE (Native Network Encryption)

Amazon RDS prend en charge le chiffrement Oracle NNE. Avec le chiffrement réseau natif, vous pouvez chiffrer les données lors de leur déplacement vers ou depuis une instance de base de données. Amazon RDS prend en charge NNE pour toutes les éditions d'Oracle.

Une présentation détaillée d'Oracle NNE dépasse le propos de ce guide, mais vous devez bien comprendre les points forts et les points faibles de chaque algorithme et de chaque clé avant de choisir une solution pour votre déploiement. Pour plus d'informations sur les algorithmes et les clés qui sont disponibles via Oracle NNE, consultez Configuration du chiffrement des données réseau dans la documentation Oracle. Pour plus d'informations sur la sécurité AWS, consultez le Centre de sécurité AWS.

Note

Vous pouvez utiliser le chiffrement réseau natif ou le protocole SSL (Secure Sockets Layer), mais pas les deux. Pour plus d'informations, consultez Oracle Secure Sockets Layer (SSL) (p. 1068).

Paramètres d'option NNE

Amazon RDS prend en charge les paramètres suivants pour l'option NNE.

> **Note**
>
> Lorsque vous utilisez des virgules pour séparer les valeurs d'un paramètre d'option, ne placez pas d'espace après la virgule.

Paramètre d'option	Valeurs valides	Valeur par défaut	Description
SQLNET.ENCRYPTION_SERVER	`Accepted`, `Rejected`, `Requested`, `Required`	`Requested`	Comportement de chiffrement quand un client, ou un serveur agissant en tant que client, se connecte à l'instance de base de données. `Requested` indique que l'instance de base de données ne requiert pas que le trafic depuis le client soit chiffré.
SQLNET.CRYPTO_CHECKSUM_SERVER	`Accepted`, `Rejected`, `Requested`, `Required`	`Requested`	Comportement d'intégrité des données quand un client, ou un serveur agissant en tant que client, se connecte à l'instance de base de données. `Requested` indique que l'instance de base de données ne nécessite pas que le client effectue un total de contrôle.
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`	Liste d'algorithmes de chiffrement utilisés par l'instance de base de données. L'instance de base de données utilise chaque algorithme, dans l'ordre, pour tenter de déchiffrer l'entrée du client jusqu'à ce qu'un algorithme réussisse ou que la fin de la liste soit atteinte. Amazon RDS utilise la liste par défaut suivante d'Oracle. Vous pouvez modifier l'ordre ou limiter les algorithmes que l'instance de base de données accepte. 1. `RC4_256` : RSA RC4 (taille de clé 256 bits) 2. `AES256` : AES (taille de clé 256 bits) 3. `AES192` : AES (taille de clé 192 bits) 4. `3DES168`: 3-key Triple-DES (taille de clé effective 112 bits) 5. `RC4_128` : RSA RC4 (taille de clé 128 bits)

Paramètre d'option	Valeurs valides	Valeur par défaut	Description
			6. `AES128` : AES (taille de clé 128 bits) 7. `3DES112` : 2-key Triple-DES (taille de clé effective 80 bits) 8. `RC4_56` : RSA RC4 (taille de clé 56 bits) 9. `DES` : Standard DES (taille de clé 56 bits) 10 `RC4_40` : RSA RC4 (taille de clé 40 bits) 11 `DES40` : DES40 (taille de clé 40 bits) Vous pouvez spécifier une valeur ou une liste de valeurs séparées par des virgules. Si vous spécifiez une virgule, n'insérez pas d'espace après celle-ci ; sinon, vous recevez une erreur `InvalidParameterValue`.
SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER	`SHA256`, `SHA384`, `SHA512`, `SHA1`, `MD5`	`SHA256`, `SHA384`, `SHA512`, `SHA1`, `MD5`	Une liste d'algorithmes de somme de contrôle. Vous pouvez spécifier une valeur ou une liste de valeurs séparées par des virgules. Si vous spécifiez une virgule, n'insérez pas d'espace après celle-ci ; sinon, vous recevez une erreur `InvalidParameterValue`.

Ajout de l'option NNE

La procédure générale pour ajouter de l'option NNE à une instance de base de données est la suivante :

1. Créer un groupe d'options ou copier ou modifier un groupe existant.
2. Ajouter l'option au groupe d'options.
3. Associer un groupe d'options à une instance de base de données.

Une fois que vous avez ajouté l'option NNE, dès que le groupe d'options est actif, NNE est actif.

Pour ajouter l'option NNE à une instance de base de données

1. Pour Moteur, sélectionnez l'édition d'Oracle que vous voulez utiliser. NNE est pris en charge par toutes les éditions.
2. Pour Version majeure du moteur, choisissez la version de votre instance de base de données.

   Pour de plus amples informations, veuillez consulter Création d'un groupe d'options (p. 212).
3. Ajouter l'option NNE au groupe d'options. Pour de plus amples informations sur l'ajout d'options, veuillez consulter Ajout d'une option à un groupe d'options (p. 214).

Note

Une fois que vous ajoutez l'option NNE, vous n'avez pas besoin de redémarrer vos instances de base de données. Dès que le groupe d'options est actif, NNE est actif.

4. Appliquez le groupe d'options à une instance de base de données nouvelle ou existante:

   - Pour une nouvelle instance de base de données, vous appliquez le groupe d'options lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).
   - Pour une instance de base de données existante, vous appliquez le groupe d'options en modifiant l'instance et en attachant le nouveau groupe d'options. Une fois que vous ajoutez l'option NNE, vous n'avez pas besoin de redémarrer votre instance de base de données. Dès que le groupe d'options est actif, NNE est actif. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Utilisation de NNE

Avec Oracle NNE, vous pouvez aussi spécifier le chiffrement réseau côté client. Sur le client (l'ordinateur utilisé pour la connexion à l'instance de base de données), vous pouvez utiliser le fichier sqlnet.ora pour spécifier les paramètres clients suivants : SQLNET.CRYPTO_CHECKSUM_CLIENT, SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT, SQLNET.ENCRYPTION_CLIENT et SQLNET.ENCRYPTION_TYPES_CLIENT. Pour plus d'informations, consultez Configuration du chiffrement des données réseau et intégrité des clients et serveurs Oracle dans la documentation Oracle.

Parfois, l'instance de base de données rejette une demande de connexion à partir d'une application : par exemple, s'il existe une différence entre les algorithmes de chiffrement sur le client et sur le serveur.

Pour tester le chiffrement réseau natif Oracle, ajoutez les lignes suivantes dans le fichier sqlnet.ora sur le client :

```
DIAG_ADR_ENABLED=off
TRACE_DIRECTORY_CLIENT=/tmp
TRACE_FILE_CLIENT=nettrace
TRACE_LEVEL_CLIENT=16
```

Ces lignes génèrent un fichier de trace sur le client appelé `/tmp/nettrace*` lors de la tentative de connexion. Le fichier de trace contient des informations sur la connexion. Pour plus d'informations sur les problèmes liés à la connexion lorsque vous utilisez le chiffrement de réseau natif Oracle, consultez A propos de la négociation du chiffrement et de l'intégrité dans la documentation Oracle.

Modification des paramètres NNE

Une fois que vous activez NNE, vous pouvez modifier les paramètres de l'option. Pour plus d'informations sur la modification des paramètres d'options, consultez Modification d'un paramètre d'option (p. 219). Pour plus d'informations sur chaque paramètre, consultez Paramètres d'option NNE (p. 1063).

Suppression de l'option NNE

Vous pouvez supprimer NNE d'une instance de base de données.

Pour supprimer NNE d'une instance de base de données, exécutez l'une des actions suivantes :

- Pour supprimer NNE de plusieurs instances de base de données, supprimez l'option NNE du groupe d'options auquel elles appartiennent. Ce changement affecte toutes les instances de bases de données qui utilisent le groupe d'options. Une fois l'option NNE supprimée, vous n'avez pas besoin de redémarrer vos instances de base de données. Pour plus d'informations, consultez Suppression d'une option d'un groupe d'options (p. 222).

- Pour supprimer l'option NNE d'une seule instance de base de données, modifiez l'instance de base de données et spécifiez un autre groupe d'options qui n'inclut pas l'option NNE. Vous pouvez spécifier le groupe d'options (vide) par défaut, ou un groupe d'options personnalisées différent. Une fois que vous supprimez l'option NNE, vous n'avez pas besoin de redémarrer votre instance de base de données. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Oracle OLAP

Amazon RDS prend en charge Oracle OLAP par l'intermédiaire de l'option `OLAP`. L'option OLAP (Online Analytical Processing) est proposée pour les instances de base de données Oracle. Vous pouvez utiliser Oracle OLAP pour analyser de grandes quantités de données en créant des objets et des cubes dimensionnels conformément à la norme OLAP. Pour de plus amples informations, veuillez consulter la documentation Oracle.

> **Important**
>
> Si vous utilisez Oracle OLAP, Amazon RDS met automatiquement à jour votre instance de base de données vers le PSU Oracle le plus récent en cas de vulnérabilités de sécurité présentant un score CVSS (Common Vulnerability Scoring System) égal ou supérieur à 9, ou d'autres vulnérabilités de sécurité annoncées.

Amazon RDS prend en charge Oracle OLAP pour les éditions et versions suivantes d'Oracle :

- Oracle Enterprise Edition, version 19.0.0.0, toutes les versions
- Oracle Enterprise Edition, version 18.0.0.0, toutes les versions
- Oracle Enterprise Edition, version 12.2.0.1, toutes les versions
- Oracle Enterprise Edition, version 12.1.0.2.v13 or ultérieure

Prérequis pour Oracle OLAP

Les conditions suivantes sont requises pour utiliser Oracle OLAP :

- Vous devez disposer d'une licence Oracle OLAP d'Oracle. Pour de plus amples informations, veuillez consulter la section relative aux informations sur les licences dans la documentation Oracle.
- Votre instance de base de données doit être dans un Virtual Private Cloud (VPC). Pour plus d'informations, consultez Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611).
- La classe d'instance de votre instance de base de données doit être suffisante. Oracle OLAP n'est pas pris en charge pour les classes d'instance de base de données db.t3.micro ou db.t3.small. Pour plus d'informations, consultez Prise en charge des classes d'instance de base de données pour Oracle (p. 933).
- Votre instance de base de données doit avoir l'option Auto Minor Version Upgrade (Mise à niveau automatique des versions mineures) activée. Cette option permet à votre instance de base de données de recevoir automatiquement des mises à niveau mineures de version du moteur de base de données lorsqu'elles sont disponibles et est requise pour toutes les options qui installent la machine virtuelle Java Oracle (JVM). Amazon RDS utilise cette option pour mettre à jour votre instance de base de données avec le dernier correctif Oracle Patch Set Update (PSU) ou la dernière mise à jour de version (RU). Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).
- Votre instance de base de données ne doit pas contenir d'utilisateur nommé `OLAPSYS`. Si votre instance en contient, l'installation de l'option OLAP échoue.

Bonnes pratiques pour Oracle OLAP

Les bonnes pratiques suivantes sont requises pour utiliser Oracle OLAP :

- Pour une sécurité maximale, utilisez l'option `OLAP` avec Secure Sockets Layer (SSL). Pour plus d'informations, consultez Oracle Secure Sockets Layer (SSL) (p. 1068).
- Configurez votre instance de base de données pour en restreindre l'accès. Pour plus d'informations, consultez Scénarios d'accès à une instance de base de données d'un VPC (p. 1613) et Utilisation d'une instance de base de données dans un VPC (p. 1620).

Ajout de l'option Oracle OLAP

La procédure générale suivante permet d'ajouter l'option `OLAP` à une instance de base de données :

1. Créer un groupe d'options ou copier ou modifier un groupe existant.
2. Ajouter l'option au groupe d'options.
3. Associez le groupe d'options à l'instance de base de données.

Si Oracle Java Virtual Machine (JVM) n'est pas installé sur l'instance de base de données, il y a une brève panne lorsque l'option `OLAP` est ajoutée. Il n'y a pas de panne si Oracle Java Virtual Machine (JVM) est déjà installé sur l'instance de base de données. Une fois que vous ajoutez l'option, vous n'avez pas besoin de redémarrer votre instance de base de données. Dès que le groupe d'options est actif, Oracle OLAP est disponible.

Pour ajouter l'option OLAP à une instance de base de données

1. Déterminez le groupe d'options que vous voulez utiliser. Vous pouvez créer un groupe d'options ou utiliser un groupe d'options existant. Si vous souhaitez utiliser un groupe d'options existant, passez à l'étape suivante. Sinon, créez un groupe d'options DB personnalisé avec les paramètres suivants :

   - Pour Moteur, choisissez l'édition Oracle de votre instance de base de données.
   - Pour Version majeure du moteur, choisissez la version de votre instance de base de données.

   Pour plus d'informations, consultez Création d'un groupe d'options (p. 212).
2. Ajoutez l'option OLAP au groupe d'options. Pour plus d'informations sur l'ajout d'options, consultez Ajout d'une option à un groupe d'options (p. 214).
3. Appliquez le groupe d'options à une instance de base de données nouvelle ou existante:

   - Pour une nouvelle instance de base de données, appliquez le groupe d'options lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).
   - Pour une instance de base de données existante, appliquez le groupe d'options en modifiant l'instance et en attachant le nouveau groupe d'options. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Utilisation d'Oracle OLAP

Une fois que vous activez l'option Oracle OLAP, vous pouvez commencer à l'utiliser. Pour obtenir la liste des fonctions prises en charge par Oracle OLAP, veuillez consulter la documentation Oracle.

Suppression de l'option Oracle OLAP

Après avoir supprimé tous les objets qui utilisent des types de données fournis par l'option `OLAP`, vous pouvez supprimer l'option d'une instance de base de données. Si Oracle Java Virtual Machine (JVM) n'est pas installé sur l'instance de base de données, il y a une brève panne lorsque l'option `OLAP` est supprimée.

Il n'y a pas de panne si Oracle Java Virtual Machine (JVM) est déjà installé sur l'instance de base de données. Une fois que vous supprimez l'option `OLAP`, vous n'avez pas besoin de redémarrer votre instance de base de données.

Pour supprimer l'option **`OLAP`**

1. Sauvegardez vos données.

   Warning

   Si l'instance utilise des types de données qui ont été activés dans le cadre de l'option, et si vous supprimez l'option `OLAP`, vous pouvez perdre des données. Pour de plus amples informations, veuillez consulter Sauvegarde et restauration d'une instance de base de données Amazon RDS (p. 317).
2. Vérifiez si des objets existants font référence à des types de données ou à des fonctionnalités de l'option `OLAP`.
3. Supprimez tous les objets qui font référence à des types de données ou à des fonctionnalités de l'option `OLAP`.
4. Effectuez l'une des actions suivantes :
   - Supprimez l'option `OLAP` du groupe d'options auquel elle appartient. Ce changement affecte toutes les instances de bases de données qui utilisent le groupe d'options. Pour plus d'informations, consultez Suppression d'une option d'un groupe d'options (p. 222).
   - Modifiez l'instance de base de données et spécifiez un groupe d'options différent qui n'inclut pas l'option `OLAP`. Ce changement affecte une seule instance de base de données. Vous pouvez spécifier le groupe d'options (vide) par défaut, ou un groupe d'options personnalisées différent. Pour de plus amples informations, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

Oracle Secure Sockets Layer (SSL)

Vous activez le chiffrement SSL (Secure Sockets Layer) pour une instance de base de données Oracle en ajoutant l'option Oracle SSL au groupe d'options associé à une instance de base de données Oracle. Vous spécifiez le port via lequel vous voulez communiquer à l'aide de SSL. Vous devez configurer SQL*Plus, comme illustré dans la section suivante.

Vous activez le chiffrement SSL (Secure Sockets Layer) pour une instance de base de données Oracle en ajoutant l'option Oracle SSL au groupe d'options associé à l'instance de base de données Oracle. Amazon RDS utilise un deuxième port requis par Oracle pour les connexions SSL. Cette approche permet aussi bien aux communications en texte clair qu'à celles à chiffrement SSL de se produire simultanément entre une instance de base de données et SQL*Plus. Par exemple, vous pouvez utiliser le port avec une communication en texte clair pour communiquer avec d'autres ressources à l'intérieur d'un VPC, tout en utilisant le port avec une communication à chiffrement SSL pour communiquer avec des ressources extérieures au VPC.

Note

Vous pouvez utiliser le protocole SSL (Secure Sockets Layer) ou le chiffrement réseau natif, mais pas les deux. Pour plus d'informations, consultez Oracle NNE (Native Network Encryption) (p. 1062).

Vous pouvez utiliser le chiffrement SSL avec les éditions et versions de bases de données Oracle suivantes :

- 19.0.0.0 : toutes les versions, toutes les éditions, y compris Standard Edition Two
- 18.0.0.0 : toutes les versions, toutes les éditions, y compris Standard Edition Two

- 12.2.0.1 : toutes les versions, toutes les éditions, y compris Standard Edition Two
- 12.1.0.2 : toutes les versions, toutes les éditions, y compris Standard Edition Two
- 11.2.0.4 : toutes les versions, Enterprise Edition
- 11.2.0.4 : version 6 et ultérieures, Standard Edition, Standard Edition One, Enterprise Edition

> **Note**
>
> Vous ne pouvez pas utiliser le chiffrement SSL et Oracle NNE sur la même instance. Si vous utilisez le chiffrement SSL, vous devez désactiver tout autre chiffrement de connexion.

Versions TLS pour l'option Oracle SSL

Amazon RDS pour Oracle prend en charge le protocole TLS (Transport Layer Security) version 1.0 et 1.2. Pour utiliser l'option Oracle SSL, utilisez le paramètre d'option `SQLNET.SSL_VERSION`. Les valeurs suivantes sont autorisées pour ce paramètre d'option :

- `"1.0"` – Les clients ne peuvent se connecter à l'instance de base de données qu'avec TLS 1.0.
- `"1.2"` – Les clients ne peuvent se connecter à l'instance de base de données qu'avec TLS 1.2.
- `"1.2 or 1.0"` – Les clients peuvent se connecter à l'instance de base de données avec TLS 1.2 ou 1.0.

Pour utiliser l'option Oracle SSL, le paramètre d'option `SQLNET.SSL_VERSION` est également obligatoire :

- Pour les options Oracle SSL existantes, `SQLNET.SSL_VERSION` est défini automatiquement sur `"1.0"`. Vous pouvez modifier au besoin ce paramètre.
- Lorsque vous ajoutez une nouvelle option Oracle SSL, vous devez définir `SQLNET.SSL_VERSION` explicitement sur une valeur valide.

Le tableau suivant affiche les paramètres d'option TLS pris en charge pour différentes versions et éditions du moteur Oracle.

Version de moteur Oracle	SQLNET.SSL_VERSION = "1.0"	SQLNET.SSL_VERSION = "1.2"	SQLNET.SSL_VERSION = "1.2 ou 1.0"
19.0.0.0 (toutes les éditions)	Pris en charge	Pris en charge	Pris en charge
18.0.0.0 (toutes les éditions)	Pris en charge	Pris en charge	Pris en charge
12.2.0.1 (toutes les éditions)	Pris en charge	Pris en charge	Pris en charge
12.1.0.2 (toutes les éditions)	Pris en charge	Pris en charge	Pris en charge
11.2.0.4 (Oracle EE)	Pris en charge	Pris en charge pour 11.2.0.4.v8 et versions ultérieures	Pris en charge pour 11.2.0.4.v8 et versions ultérieures
11.2.0.4 (Oracle SE1)	Pris en charge	Non pris en charge	Non pris en charge
11.2.0.4 (Oracle SE)	Pris en charge	Non pris en charge	Non pris en charge

Suites de chiffrement pour l'option Oracle SSL

Amazon RDS pour Oracle prend en charge plusieurs suites de chiffrement SSL. Par défaut, l'option Oracle SSL est configurée pour utiliser la suite de chiffrement `SSL_RSA_WITH_AES_256_CBC_SHA`. Pour indiquer une autre suite de chiffrement à utiliser sur les connexions SSL, utilisez le paramètre d'option `SQLNET.CIPHER_SUITE`. Les valeurs admises pour ce paramètre d'option sont les suivantes :

- `"SSL_RSA_WITH_AES_256_CBC_SHA"` : le paramètre par défaut, compatible avec TLS 1.0 et TLS 1.2
- `"SSL_RSA_WITH_AES_256_CBC_SHA256"` : uniquement compatible avec TLS 1.2
- `"SSL_RSA_WITH_AES_256_GCM_SHA384"` : uniquement compatible avec TLS 1.2

Pour les options Oracle SSL existantes, `SQLNET.CIPHER_SUITE` est défini automatiquement sur `"SSL_RSA_WITH_AES_256_CBC_SHA"`. Vous pouvez modifier au besoin ce paramètre.

Le tableau suivant affiche les paramètres d'option de suite de chiffrement pris en charge pour différentes versions et éditions du moteur Oracle.

Version de moteur Oracle	SQLNET.CIPHER_SUITE = "SSL_RSA_WITH_AES_2	SQLNET.CIPHER_SUITE = "SSL_RSA_WITH_AES_2	SQLNET.CIPHER_SUITE = "SSL_RSA_WITH_AES_256_GCM_SH
19.0.0.0 (toutes les éditions)	Pris en charge	Pris en charge	Pris en charge
18.0.0.0 (toutes les éditions)	Pris en charge	Pris en charge	Pris en charge
12.2.0.1 (toutes les éditions)	Pris en charge	Pris en charge	Pris en charge
12.1.0.2 (toutes les éditions)	Pris en charge	Pris en charge	Pris en charge
11.2.0.4 (Oracle EE)	Pris en charge	Non pris en charge	Non pris en charge
11.2.0.4 (Oracle SE1)	Pris en charge	Non pris en charge	Non pris en charge
11.2.0.4 (Oracle SE)	Pris en charge	Non pris en charge	Non pris en charge

Support FIPS

Amazon RDS pour Oracle vous permet d'utiliser la norme FIPS (Federal Information Processing Standard) 140-2. FIPS 140-2 est une norme du gouvernement américain qui définit les exigences de sécurité du module de chiffrement. Pour activer la norme FIPS, vous définissez le paramètre `FIPS.SSLFIPS_140` sur `TRUE` pour l'option Oracle SSL. Lorsque la norme FIPS 140-2 est configurée pour SSL, les bibliothèques de chiffrement sont conçues pour chiffrer les données entre le client et l'instance de base de données Oracle.

Vous pouvez activer le paramètre FIPS avec les éditions et versions de bases de données Oracle suivantes :

- 19.0.0.0 : toutes les versions, toutes les éditions, y compris Standard Edition Two
- 18.0.0.0 : toutes les versions, toutes les éditions, y compris Standard Edition Two
- 12.2.0.1 : toutes les versions, toutes les éditions, y compris Standard Edition Two
- 12.1.0.2 : version 2 et versions ultérieures, toutes les éditions, y compris Standard Edition Two

Les clients doivent utiliser la suite de chiffrement conforme à FIPS. Lors de l'établissement d'une connexion, le client et l'instance de base de données Oracle négocient concernant la suite de chiffrement à utiliser lors de la transmission de messages dans les deux sens. Le tableau suivant présente les suites de chiffrement SSL conformes à FIPS pour chaque version de TLS.

SQLNET.SSL_VERSION	Suites de chiffrement prises en charge
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

Pour de plus amples informations, veuillez consulter Oracle Database FIPS 140-2 Settings dans la documentation Oracle.

Ajout de l'option SSL

Pour utiliser SSL, votre instance de base de données Oracle Amazon RDS doit être associée à un groupe d'options qui inclut l'option `SSL`.

Console

Pour ajouter l'option SSL à un groupe d'options

1. Créez un groupe d'options ou identifiez un groupe d'options existant auquel vous pouvez ajouter l'option `SSL`.

   Pour de plus amples informations sur la création d'un groupe d'options, veuillez consulter Création d'un groupe d'options (p. 212).
2. Ajoutez l'option `SSL` au groupe d'options.

   Si vous souhaitez utiliser uniquement des suites de chiffrement conformes à la norme FIPS pour les connexions SSL, définissez l'option `FIPS.SSLFIPS_140` sur `TRUE`. Pour de plus amples informations sur la norme FIPS, veuillez consulter Support FIPS (p. 1070).

   Pour de plus amples informations sur l'ajout d'une option à un groupe d'options, veuillez consulter Ajout d'une option à un groupe d'options (p. 214).
3. Créez une instance de base de données Oracle et associez le groupe d'options à cette instance ou modifiez une instance de base de données Oracle pour lui associer le groupe d'options.

   Pour de plus amples informations sur la création d'une instance de base de données, veuillez consulter Création d'une instance de base de données Amazon RDS (p. 146).

   Pour plus d'informations sur la modification d'une instance de base de données , consultez Modification d'une instance de base de données Amazon RDS (p. 243).

AWS CLI

Pour ajouter l'option SSL à un groupe d'options

1. Créez un groupe d'options ou identifiez un groupe d'options existant auquel vous pouvez ajouter l'option `SSL`.

   Pour de plus amples informations sur la création d'un groupe d'options, veuillez consulter Création d'un groupe d'options (p. 212).

2. Ajoutez l'option `SSL` au groupe d'options.

   Spécifiez les paramètres d'option suivants :

   - `Port` – Numéro du port SSL
   - `VpcSecurityGroupMemberships` – Groupe de sécurité pour lequel l'option est activée
   - `SQLNET.SSL_VERSION` – Version TLS que le client peut utiliser pour se connecter à l'instance de base de données

   Par exemple, la commande AWS CLI suivante ajoute l'option `SSL` à un groupe d'options nommé `ora-option-group`.

   Example

   Pour Linux, macOS ou 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.S
```

   Pour 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.S
```

3. Créez une instance de base de données Oracle et associez le groupe d'options à cette instance ou modifiez une instance de base de données Oracle pour lui associer le groupe d'options.

   Pour de plus amples informations sur la création d'une instance de base de données, veuillez consulter Création d'une instance de base de données Amazon RDS (p. 146).

   Pour plus d'informations sur la modification d'une instance de base de données , consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Configuration de SQL*Plus de façon à utiliser SSL avec une instance de base de données Oracle

Vous devez configurer SQL*Plus avant de vous connecter à une instance de base de données Oracle utilisant l'option Oracle SSL.

Note

Pour permettre l'accès à l'instance de base de données à partir des clients appropriés, assurez-vous que vous groupes de sécurité soient bien configurés. Pour plus d'informations, consultez Contrôle d'accès par groupe de sécurité (p. 1590). Ces instructions s'appliquent également à SQL*Plus et à d'autres clients qui utilisent directement un Oracle Home. Pour les connexions JDBC, consultez Configuration d'une connexion SSL via JDBC (p. 1075).

Pour configurer SQL*Plus de façon à utiliser SSL pour se connecter à une instance de bases de données Oracle

1. Configurez la variable d'environnement `ORACLE_HOME` sur l'emplacement de votre répertoire de base Oracle.

   Le chemin vers votre répertoire de base Oracle dépend de votre installation. L'exemple suivant définit la variable d'environnement `ORACLE_HOME`.

   ```
   prompt>export ORACLE_HOME=/home/user/app/user/product/12.1.0/dbhome_1
   ```

   Pour plus d'informations sur la définition de variables d'environnement Oracle, consultez SQL*Plus Environment Variables dans la documentation Oracle, ainsi que le guide d'installation Oracle pour votre système d'exploitation.
2. Ajoutez `$ORACLE_HOME/lib` à la variable d'environnement `LD_LIBRARY_PATH`.

   Voici un exemple qui définit la variable d'environnement LD_LIBRARY_PATH.

   ```
   prompt>export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
   ```
3. Créez un répertoire pour le portefeuille Oracle dans `$ORACLE_HOME/ssl_wallet`.

   Voici un exemple qui crée le répertoire du portefeuille Oracle.

   ```
   prompt>mkdir $ORACLE_HOME/ssl_wallet
   ```
4. Téléchargez le certificat racine qui fonctionne pour toutes les régions AWS et placez le fichier dans le répertoire ssl_wallet.

   Pour plus d'informations sur le téléchargement du certificat racine, consultez Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).
5. Dans le répertoire `$ORACLE_HOME/network/admin`, modifiez ou créez le fichier tnsnames.ora file et incluez l'entrée suivante.

   ```
   <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. Dans le même répertoire, modifiez ou créez le fichier sqlnet.ora et incluez les paramètres suivants.

   Note

   Pour communiquer avec des entités via une connexion sécurisée TLS, Oracle a besoin d'un portefeuille avec les certificats nécessaire pour l'authentification. Vous pouvez utiliser l'utilitaire ORAPKI d'Oracle pour créer et gérer des portefeuilles Oracle, comme illustré à l'étape 7. Pour de plus amples informations, veuillez consulter Setting Up Oracle Wallet Using ORAPKI dans la documentation Oracle.

   ```
   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

Vous pouvez définir `SSL_VERSION` sur une valeur plus élevée si votre instance de base de données la prend en charge.

7. Exécutez les commandes suivantes pour créer le portefeuille Oracle.

```
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
```

Remplacez le nom de fichier par le nom de celui que vous avez téléchargé.

Connexion à une instance de base de données Oracle à l'aide de SSL

Une fois que vous avez configuré SQL*Plus pour utiliser SSL comme décrit précédemment, vous pouvez vous connecter à l'instance de base de données Oracle avec l'option SSL. Vous pouvez éventuellement d'abord exporter la valeur `TNS_ADMIN` qui pointe vers le répertoire qui contient les fichiers tnsnames.ora et sqlnet.ora. Vous vous assurez ainsi que SQL*Plus peut trouver ces fichiers de manière cohérente. L'exemple suivant exporte la valeur `TNS_ADMIN`.

```
export TNS_ADMIN = ${ORACLE_HOME}/network/admin
```

Connectez-vous à l'instance de base de données. Par exemple, vous pouvez vous connecter en utilisant SQL*Plus et *<net_service_name>* dans un fichier tnsnames.ora.

```
sqlplus <mydbuser>@<net_service_name>
```

Vous pouvez également vous connecter à l'instance de base de données à l'aide de SQL*Plus sans fichier tnsnames.ora, en utilisant la commande suivante.

```
sqlplus '<mydbuser>@(DESCRIPTION = (ADDRESS = (PROTOCOL = TCPS)(HOST = <endpoint>) (PORT
 = <ssl port number>))(CONNECT_DATA = (SID = <database name>)))'
```

Vous pouvez également vous connecter à l'instance de base de données Oracle sans utiliser SSL. Par exemple, la commande suivante se connecte à l'instance de base de données via le port en texte clair sans chiffrement SSL.

```
sqlplus '<mydbuser>@(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = <endpoint>) (PORT
 = <port number>))(CONNECT_DATA = (SID = <database name>)))'
```

Si vous voulez fermer l'accès au port TCP, créez un groupe de sécurité sans entrée d'adresse IP et ajoutez-le à l'instance. Cet ajout ferme les connexions sur le port TCP, tout en continuant à autoriser les connexions sur le port SSL spécifiées à partir d'adresses IP au sein de la plage autorisée par le groupe de sécurité de l'option SSL.

Configuration d'une connexion SSL via JDBC

Pour utiliser une connexion SSL via JDBC, vous devez créer un keystore, approuver le certificat d'autorité de certification racine Amazon RDS et utiliser l'extrait de code suivant.

Pour créer le keystore au format JKS, utilisez la commande suivante. Pour plus d'informations sur la création du keystore, consultez la documentation Oracle.

```
keytool -keystore clientkeystore -genkey -alias client
```

Ensuite, suivez les étapes ci-après pour approuver le certificat d'autorité de certification racine Amazon RDS.

Pour approuver le certificat de l'autorité de certification racine Amazon RDS

1. Téléchargez le certificat racine qui fonctionne pour toutes les régions AWS et placez le fichier dans le répertoire ssl_wallet.

   Pour plus d'informations sur le téléchargement du certificat racine, consultez Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).
2. Convertissez le certificat au format .der à l'aide de la commande suivante.

   ```
   openssl x509 -outform der -in rds-ca-2019-root.pem -out rds-ca-2019-root.der
   ```

   Remplacez le nom de fichier par le nom de celui que vous avez téléchargé.
3. Importez le certificat dans le keystore à l'aide de la commande suivante.

   ```
   keytool -import -alias rds-root -keystore clientkeystore -file rds-ca-2019-root.der
   ```
4. Vérifiez que le magasin de clés a été créé avec succès.

   ```
   keytool -list -v -keystore clientkeystore.jks
   ```

   Entrez le mot de passe du magasin de clés lorsque vous y êtes invité.

L'exemple de code suivant montre comment configurer la connexion SSL à l'aide de 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
    }
}
```

Application d'une correspondance de nom unique avec une connexion SSL

Vous pouvez utiliser le paramètre Oracle `SSL_SERVER_DN_MATCH` pour imposer que le nom unique du serveur de base de données corresponde à son nom de service. Si vous appliquez les vérifications de correspondance, SSL garantit que le certificat provient du serveur. Si vous n'appliquez pas la vérification de correspondance, SSL effectue le contrôle, mais autorise la connexion, qu'il y ait correspondance ou pas. Si vous n'appliquez pas la correspondance, vous autorisez le serveur à falsifier potentiellement son identité.

Pour appliquer la correspondance de nom unique, ajoutez la propriété DN Match et utilisez la chaîne de connexion spécifiée ci-dessous.

Ajoutez la propriété à la connexion client pour appliquer la correspondance de nom unique.

```
properties.put("oracle.net.ssl_server_dn_match", "TRUE");
```

Utilisez la chaîne de connexion suivante pour appliquer la correspondance de nom unique lors de l'utilisation de 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 prend en charge Oracle Spatial par l'intermédiaire de l'option `SPATIAL`. Oracle Spatial fournit un schéma SQL et des fonctions qui facilitent le stockage, la récupération, la mise à jour et la requête de collections de données spatiales dans une base de données Oracle. Pour plus d'informations, consultez Concepts spatiaux dans la documentation d'Oracle.

> **Important**
>
> Si vous utilisez Oracle Spatial, Amazon RDS met automatiquement à jour votre instance de base de données vers le dernier PSU Oracle si un des éléments suivants existe :
>
> - Vulnérabilités de sécurité avec un score CVSS (Common Vulnerability Scoring System) de 9+
> - Autres vulnérabilités de sécurité annoncées

Amazon RDS prend en charge Oracle Spatial uniquement dans Oracle Enterprise Edition (EE) et Oracle Standard Edition 2 (SE2). Le tableau suivant présente les versions du moteur de base de données qui prennent en charge EE et SE2.

Version de base de donnes Oracle	EE	SE2
19.0.0.0, toutes versions	Oui	Oui
18.0.0.0, toutes versions	Oui	Oui
12.2.0.1, toutes versions	Oui	Oui
12.1.0.2.v13 ou ultérieure	Oui	Non
11.2.0.4.v17 ou ultérieure	Oui	S/O

Prérequis pour Oracle Spatial

Les conditions suivantes sont requises pour utiliser Oracle Spatial :

- Assurez-vous que votre instance de base de données se trouve dans un virtual private cloud (VPC). Pour plus d'informations, consultez Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611).
- Assurez-vous que votre instance de base de données est d'une classe d'instance suffisante. Oracle Spatial n'est pas pris en charge pour les classes d'instance de base de données db.t3.micro ou db.t3.small. Pour plus d'informations, consultez Prise en charge des classes d'instance de base de données pour Oracle (p. 933).
- Assurez-vous que Mise à niveau automatique des versions mineures est activée pour votre instance de base de données. Cette option permet à votre instance de base de données de recevoir automatiquement des mises à niveau mineures de version du moteur de base de données lorsqu'elles sont disponibles et est requise pour toutes les options qui installent la machine virtuelle Java Oracle (JVM). Amazon RDS utilise cette option pour mettre à jour votre instance de base de données avec le

dernier correctif Oracle Patch Set Update (PSU) ou la dernière mise à jour de version (RU). Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

- Si votre instance de base de données est en cours d'exécution sur la version majeure 11.2, assurez-vous d'installer l'option `XMLDB`. Pour plus d'informations, consultez Oracle XML DB (p. 1096).

Bonnes pratiques pour Oracle Spatial

Les bonnes pratiques suivantes sont requises pour utiliser Oracle Spatial :

- Pour une sécurité maximale, utilisez l'option `SPATIAL` avec Secure Sockets Layer (SSL). Pour plus d'informations, consultez Oracle Secure Sockets Layer (SSL) (p. 1068).
- Configurez votre instance de base de données pour en restreindre l'accès. Pour plus d'informations, consultez Scénarios d'accès à une instance de base de données d'un VPC (p. 1613) et Utilisation d'une instance de base de données dans un VPC (p. 1620).

Ajout de l'option Oracle Spatial

La procédure générale suivante permet d'ajouter l'option `SPATIAL` à une instance de base de données :

1. Créer un groupe d'options ou copier ou modifier un groupe existant.
2. Ajouter l'option au groupe d'options.
3. Associez le groupe d'options à l'instance de base de données.

Si Oracle Java Virtual Machine (JVM) n'est pas installé sur l'instance de base de données, il y a une brève panne lorsque l'option `SPATIAL` est ajoutée. Il n'y a pas de panne si Oracle Java Virtual Machine (JVM) est déjà installé sur l'instance de base de données. Une fois que vous ajoutez l'option, vous n'avez pas besoin de redémarrer votre instance de base de données. Dès que le groupe d'options est actif, Oracle Spatial est disponible.

> **Note**
>
> Durant cette interruption, les fonctions de vérification de mot de passe sont brièvement désactivées. Vous pouvez également vous attendre à voir des événements liés aux fonctions de vérification de mot de passe durant l'interruption. Les fonctions de vérification de mot de passe sont activées de nouveau avant que l'instance de base de données Oracle ne soit disponible.

Pour ajouter l'option **`SPATIAL`** à une instance de base de données

1. Déterminez le groupe d'options que vous voulez utiliser. Vous pouvez créer un groupe d'options ou utiliser un groupe d'options existant. Si vous souhaitez utiliser un groupe d'options existant, passez à l'étape suivante. Sinon, créez un groupe d'options DB personnalisé avec les paramètres suivants :

   a. Pour Moteur, choisissez l'édition Oracle de votre instance de base de données.
   b. Pour Version majeure du moteur, choisissez la version de votre instance de base de données.

   Pour de plus amples informations, veuillez consulter Création d'un groupe d'options (p. 212).
2. Ajoutez l'option SPATIAL au groupe d'options. Pour plus d'informations sur l'ajout d'options, consultez Ajout d'une option à un groupe d'options (p. 214).
3. Appliquez le groupe d'options à une instance de base de données nouvelle ou existante:

   - Pour une nouvelle instance de base de données, vous appliquez le groupe d'options lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).

- Pour une instance de base de données existante, vous appliquez le groupe d'options en modifiant l'instance et en attachant le nouveau groupe d'options. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Suppression de l'option Oracle Spatial

Après avoir abandonné tous les objets qui utilisent des types de données fournis par l'option `SPATIAL`, vous pouvez supprimer l'option à partir d'une instance de base de données. Si Oracle Java Virtual Machine (JVM) n'est pas installé sur l'instance de base de données, il y a une brève panne lorsque l'option `SPATIAL` est supprimée. Il n'y a pas de panne si Oracle Java Virtual Machine (JVM) est déjà installé sur l'instance de base de données. Une fois que vous supprimez l'option `SPATIAL`, vous n'avez pas besoin de redémarrer votre instance de base de données.

Pour supprimer l'option **`SPATIAL`**

1. Sauvegardez vos données.

   Warning

   Si l'instance utilise des types de données qui ont été activés dans le cadre de l'option, et si vous supprimez l'option `SPATIAL`, vous pouvez perdre des données. Pour plus d'informations, consultez Sauvegarde et restauration d'une instance de base de données Amazon RDS (p. 317).

2. Vérifiez si des objets existants font référence à des types de données ou à des fonctionnalités de l'option `SPATIAL`.

   Si des options `SPATIAL` existent, l'instance peut rester bloquée lors de l'application du nouveau groupe d'options qui n'a pas l'option `SPATIAL`. Vous pouvez identifier les objets à l'aide des requêtes suivantes :

```
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. Supprimez tous les objets qui font référence à des types de données ou à des fonctionnalités de l'option `SPATIAL`.
4. Effectuez l'une des actions suivantes :

   - Supprimez l'option `SPATIAL` du groupe d'options auquel elle appartient. Ce changement affecte toutes les instances de bases de données qui utilisent le groupe d'options. Pour plus d'informations, consultez Suppression d'une option d'un groupe d'options (p. 222).
   - Modifiez l'instance de base de données et spécifiez un groupe d'options différent qui n'inclut pas l'option `SPATIAL`. Ce changement affecte une seule instance de base de données. Vous pouvez spécifier le groupe d'options (vide) par défaut, ou un groupe d'options personnalisées différent. Pour de plus amples informations, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

Oracle SQLT

Amazon RDS prend en charge Oracle SQLTXPLAIN (SQLT) via l'utilisation de l'option SQLT.

L'instruction `EXPLAIN PLAN` Oracle peut déterminer la plan d'exécution d'une instruction SQL. Elle peut vérifier si l'optimiseur d'Oracle choisit un plan d'exécution particulier, comme une jointure de boucles imbriquées. Elle vous aide également à comprendre les décisions de l'optimiseur, par exemple, pourquoi celui-ci a choisi une jointure de boucles imbriquées plutôt qu'une jointure de hachage. `EXPLAIN PLAN` vous aide donc à comprendre les performances de l'instruction.

SQLT est un utilitaire Oracle qui génère un rapport. Le rapport inclut des statistiques d'objet, des métadonnées d'objet, des paramètres d'initialisation liés à l'optimiseur et d'autres informations qu'un administrateur de base de données peut utiliser pour régler une instruction SQL afin d'obtenir des performances optimales. SQLT génère un rapport HTML avec des liens hypertexte vers toutes les sections du rapport.

Contrairement aux rapports Automatic Workload Repository ou Statspack, SQLT travaille sur des instructions SQL individuelles. SQLT est un ensemble de fichiers SQL, PL/SQL et SQL* qui collectent, stockent et affichent des données de performance.

Vous trouverez, ci-après, les versions Oracle prises en charge pour chaque version SQLT.

Version SQLT	Oracle 19c	Oracle 18c	Oracle 12c version 12.2	Oracle 12c version 12.1	Oracle 11g
12.2.180725	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
12.2.180331	Non pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
12.1.160429	Non pris en charge	Non pris en charge	Pris en charge	Pris en charge	Pris en charge

Pour télécharger SQLT et accéder aux instructions d'utilisation :

- Connectez-vous à votre compte My Oracle Support et ouvrez les documents suivants :
- Pour télécharger SQLT : Document 215187.1
- Pour des instructions d'utilisation de SQLT : Document 1614107.1
- Pour les questions fréquentes sur SQLT : Document 1454160.1
- Pour plus d'informations sur la lecture de la sortie de SQLT : Document 1456176.1
- Pour interpréter le rapport principal : Document 1922234.1

Vous pouvez utiliser SQLT avec n'importe quelle édition des versions d'Oracle Database suivantes :

- Oracle 19c, 19.0.0.0
- Oracle 18c, 18.0.0.0
- Oracle 12c, 12.2.0.1
- Oracle 12c, 12.1.0.2
- Oracle 11g, 11.2.0.4

Amazon RDS ne prend pas en charge les méthodes SQLT suivantes :

- `XPLORE`

- `XHUME`

Prérequis pour SQLT

Les conditions suivantes sont requises pour utiliser SQLT :

- Vous devez supprimer les utilisateurs et les rôles qui sont requis par SQLT, s'ils existent.

  L'option SQLT crée les utilisateurs et rôles suivants sur une instance de base de données :
  - `SQLTXPLAIN` user
  - `SQLTXADMIN` user
  - `SQLT_USER_ROLE` rôle

  Si votre instance de base de données comporte ces utilisateurs ou rôles, connectez-vous à l'instance à l'aide d'un client SQL et supprimez-les avec les instructions suivantes :

```
DROP USER SQLTXPLAIN CASCADE;
DROP USER SQLTXADMIN CASCADE;
DROP ROLE SQLT_USER_ROLE CASCADE;
```

- Vous devez supprimer les espaces de table qui sont requis par SQLT, s'ils existent.

  L'option SQLT crée les espaces de table suivants sur une instance de base de données :
  - `RDS_SQLT_TS`
  - `RDS_TEMP_SQLT_TS`

  Si votre instance de base de données comporte ces espaces de table, connectez-vous à l'instance à l'aide d'un client SQL et supprimez-les.

Paramètres d'option SQLT

SQLT peut utiliser les fonctions sous licence fournies par Oracle Tuning Pack et Oracle Diagnostics Pack. Oracle Tuning Pack inclut SQL Tuning Advisor, et Oracle Diagnostics Pack comprend Automatic Workload Repository. Les paramètres SQLT activent ou désactivent l'accès à ces fonctions depuis SQLT.

Amazon RDS prend en charge les paramètres suivants pour l'option SQLT.

Paramètre d'option	Valeurs valides	Valeur par défaut	Description
`LICENSE_PACK`	`T`, `D`, `N`	`N`	Les Oracle Management Packs auxquels vous souhaitez accéder avec SQLT. Entrez l'une des valeurs suivantes : • `T` indique que vous possédez une licence pour Oracle Tuning Pack et Oracle Diagnostics Pack, et que vous souhaitez accéder à SQL Tuning Advisor et Automatic Workload Repository depuis SQLT. • `D` indique que vous possédez une licence pour Oracle Diagnostics Pack, et que vous souhaitez accéder à Automatic Workload Repository depuis SQLT. • `N` indique que vous ne possédez pas de licence pour Oracle Tuning Pack et Oracle Diagnostics Pack, ou que vous avez une licence pour l'un de ces packs ou

Paramètre d'option	Valeurs valides	Valeur par défaut	Description
			les deux, mais que vous ne souhaitez pas que SQLT y accède. Note Amazon RDS ne fournit pas de licences pour ces Oracle Management Packs. Si vous indiquez que vous souhaitez utiliser un pack qui n'est pas inclus dans votre instance de base de données, vous pouvez utiliser SQLT avec cette instance. Toutefois, SQLT ne peut pas accéder au pack et le rapport SQLT n'inclut pas de données pour le pack. Par exemple, si vous spécifiez `T`, mais que l'instance de base de données n'inclut pas Oracle Tuning Pack, SQLT fonctionne sur cette instance, mais le rapport qu'il génère ne contient pas de données liées à Oracle Tuning Pack.
`VERSION`	`2016-04-29.v1`, `2018-03-31.v1`, `2018-07-25.v1`	`2016-04-29.v1`	Version de SQLT que vous voulez installer. Note Pour Oracle version 19.0.0.0, la seule version prise en charge est `2018-07-25.v1`. Cette version est également l'option par défaut pour Oracle version 19.0.0.0.

Ajout de l'option SQLT

La procédure générale suivante permet d'ajouter l'option SQLT à une instance de base de données :

1. Créer un groupe d'options ou copier ou modifier un groupe existant.
2. Ajouter l'option SQLT au groupe d'options.
3. Associez le groupe d'options à l'instance de base de données.

Une fois que vous avez ajouté l'option SQLT, dès que le groupe d'options est actif, SQLT est actif.

Pour ajouter l'option SQLT à une instance de base de données

1. Déterminez le groupe d'options que vous voulez utiliser. Vous pouvez créer un groupe d'options ou utiliser un groupe d'options existant. Si vous souhaitez utiliser un groupe d'options existant, passez à l'étape suivante. Sinon, créez un groupe d'options DB personnalisé avec les paramètres suivants :

   a. Pour Moteur, sélectionnez l'édition d'Oracle que vous voulez utiliser. L'option SQLT est prise en charge sur toutes les éditions.

   b. Pour Version majeure du moteur, choisissez la version de votre instance de base de données.

   Pour de plus amples informations, veuillez consulter Création d'un groupe d'options (p. 212).
2. Ajouter l'option SQLT au groupe d'options. Pour de plus amples informations sur l'ajout d'options, veuillez consulter Ajout d'une option à un groupe d'options (p. 214).
3. Appliquez le groupe d'options à une instance de base de données nouvelle ou existante:

- Pour une nouvelle instance de base de données, vous appliquez le groupe d'options lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).
- Pour une instance de base de données existante, vous appliquez le groupe d'options en modifiant l'instance et en attachant le nouveau groupe d'options. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

4. (Facultatif) Vérifiez l'installation SQLT sur chaque instance de base de données avec l'option SQLT.

   a. Utilisez un client SQL pour vous connecter à l'instance de base de données en tant qu'utilisateur principal.

      Pour plus d'informations sur la connexion à une instance de base de données Oracle à l'aide d'un client SQL, consultez Connexion à une instance de base de données Oracle (p. 961).

   b. Exécutez la requête suivante :

```
SELECT sqltxplain.sqlt$a.get_param('tool_version') sqlt_version FROM DUAL;
```

      La requête renvoie la version actuelle de l'option SQLT sur Amazon RDS. `12.1.160429` est un exemple de version de SQLT disponible sur Amazon RDS.

5. Modifiez les mots de passe des utilisateurs créés par l'option SQLT.

   a. Utilisez un client SQL pour vous connecter à l'instance de base de données en tant qu'utilisateur principal.

   b. Exécutez l'instruction SQL suivante pour modifier le mot de passe de l'utilisateur `SQLTXADMIN` :

```
ALTER USER SQLTXADMIN IDENTIFIED BY new_password ACCOUNT UNLOCK;
```

   c. Exécutez l'instruction SQL suivante pour modifier le mot de passe de l'utilisateur `SQLTXPLAIN` :

```
ALTER USER SQLTXPLAIN IDENTIFIED BY new_password ACCOUNT UNLOCK;
```

Note

La mise à niveau de SQLT nécessite la désinstallation d'une ancienne version de SQLT, puis l'installation de la nouvelle version. Par conséquent, toutes les métadonnées de SQLT peuvent être perdues quand vous mettez à niveau SQLT. Une mise à niveau de version majeure d'une base de données désinstalle et réinstalle également SQLT. Un exemple de mise à niveau de version majeure est une mise à niveau depuis Oracle 11g vers Oracle 12c.

Utilisation de SQLT

SQLT fonctionne avec l'utilitaire Oracle SQL*Plus.

Pour utiliser SQLT

1. Téléchargez le fichier .zip SQLT depuis Document 215187.1 sur le site My Oracle Support.

Note

Vous ne pouvez pas télécharger SQLT 12.1.160429 depuis le site My Oracle Support. Oracle a supprimé cette ancienne version.

2. Décompressez le fichier .zip SQLT.
3. Depuis une invite de commande et accédez au répertoire `sqlt/run` sur votre système de fichiers.
4. Depuis l'invite de commande, ouvrez SQL*Plus et connectez-vous à l'instance de base de données en tant qu'utilisateur principal.

   Pour plus d'informations sur la connexion à une instance de base de données à l'aide de SQL*Plus, consultez Connexion à une instance de base de données Oracle (p. 961).
5. Obtenez l'ID SQL d'une instruction SQL :

```
SELECT SQL_ID FROM V$SQL WHERE SQL_TEXT='sql_statement';
```

   Votre sortie est similaire à ce qui suit :

```
SQL_ID
-------------
chvsmttqjzjkn
```

6. Analysez une instruction SQL avec SQLT :

```
START sqltxtract.sql sql_id sqltxplain_user_password
```

   Par exemple, pour l'ID SQL `chvsmttqjzjkn`, entrez ce qui suit :

```
START sqltxtract.sql chvsmttqjzjkn sqltxplain_user_password
```

   SQLT génère le rapport HTML et les ressources connexes sous la forme d'un fichier .zip dans le répertoire à partir duquel la commande SQLT a été exécutée.
7. (Facultatif) Pour permettre à des utilisateurs de l'application de diagnostiquer des instructions SQL avec SQLT, accordez le rôle `SQLT_USER_ROLE` à chaque utilisateur avec l'instruction suivante :

```
GRANT SQLT_USER_ROLE TO application_user_name;
```

   Note

   Oracle ne recommande pas d'exécuter SQLT avec le ou les utilisateurs `SYS` détenant le rôle `DBA`. Une bonne pratique consiste à exécuter des diagnostics SQLT à l'aide du compte de l'utilisateur d'application en octroyant le rôle `SQLT_USER_ROLE` à cet utilisateur.

Mise à niveau de l'option SQLT

Avec Amazon RDS pour Oracle, vous pouvez mettre à niveau l'option SQLT de la version existante vers une version ultérieure. Pour mettre à niveau l'option SQLT, effectuez les étapes 1–3 dans Utilisation de SQLT (p. 1083) pour la nouvelle version de SQLT. Par ailleurs, si vous avez accordé des privilèges pour la version précédente de SQLT à l'étape 7 de cette section, accordez à nouveau les privilèges pour la version SQLT.

La mise à niveau de l'option SQLT entraîne la perte des métadonnées de l'ancienne version SQLT. Le schéma de l'ancienne version SQLT et les objets connexes sont supprimés, et la version SQLT la plus récente est installée. Pour de plus amples informations sur les modifications de la dernière version SQLT, veuillez consulter Document 1614201.1 sur le site My Oracle Support.

> Note
>
> Les mises à niveau vers une version antérieure ne sont pas prises en charge.

Modification des paramètres SQLT

Une fois que vous avez activé SQLT, vous pouvez modifier les paramètres `LICENSE_PACK` et `VERSION` de l'option.

Pour plus d'informations sur la modification des paramètres d'options, consultez Modification d'un paramètre d'option (p. 219). Pour plus d'informations sur chaque paramètre, consultez Paramètres d'option SQLT (p. 1081).

Suppression de l'option SQLT

Vous pouvez supprimer SQLT d'une instance de base de données.

Pour supprimer SQLT d'une instance de base de données, exécutez l'une des actions suivantes :

- Pour supprimer SQLT de plusieurs instances de base de données, supprimez l'option SQLT du groupe d'options auquel celles-ci appartiennent. Ce changement affecte toutes les instances de bases de données qui utilisent le groupe d'options. Pour plus d'informations, consultez Suppression d'une option d'un groupe d'options (p. 222).
- Pour supprimer l'option SQLT d'une seule instance de base de données, modifiez l'instance de base de données et spécifiez un autre groupe d'options qui n'inclut pas l'option SQLT. Vous pouvez spécifier le groupe d'options (vide) par défaut, ou un groupe d'options personnalisées différent. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Voir aussi

- Utilisation de groupes d'options (p. 209)
- Options propres aux instances de bases de données Oracle (p. 1013)

Oracle Statspack

L'option Oracle Statspack installe et active la fonction de statistiques de performances Oracle Statspack. Oracle Statspack est un ensemble de scripts SQL, PL/SQL et SQL*Plus qui collectent, stockent et affichent les données de performance. Pour plus d'informations sur l'utilisation d'Oracle Statspack, consultez Oracle Statspack dans la documentation Oracle.

> Note
>
> Oracle Statspack n'est plus pris en charge par Oracle et a été remplacé par l'option Automatic Workload Repository (AWR) plus avancée. AWR est disponible uniquement pour les clients

Oracle Enterprise Edition ayant acheté le pack Diagnostics. Vous pouvez utiliser Oracle Statspack avec n'importe quel moteur de base de données Oracle sur Amazon RDS. Vous ne pouvez pas exécuter Oracle Statspack sur les réplicas en lecture Amazon RDS.

Configurer Oracle Statspack

Pour exécuter des scripts Statspack, vous devez ajouter l'option Statspack.

Pour configurer Oracle Statspack

1. Dans un client SQL, connectez-vous à la base de données Oracle avec un compte administratif.
2. Procédez comme suit, selon que Statspack est installé ou pas :
   - Si Statspack est installé et que le compte `PERFSTAT` lui est associé, passez à l'étape 4.
   - Si Statspack n'est pas installé et que le compte `PERFSTAT` existe, supprimez le compte comme suit :

     ```
     DROP USER PERFSTAT CASCADE;
     ```

     Sinon, une tentative d'ajout de l'option Statspack génère une erreur et un `RDS-Event-0058`.
3. Ajoutez l'option Statspack à un groupe d'options. Voir Ajout d'une option à un groupe d'options (p. 214).

   Amazon RDS installe automatiquement les scripts Statspack sur l'instance de base de données, puis configure le compte `PERFSTAT`.
4. Réinitialisez le mot de passe à l'aide de l'instruction SQL suivante, en remplaçant pwd par votre nouveau mot de passe :

   ```
   ALTER USER PERFSTAT IDENTIFIED BY pwd ACCOUNT UNLOCK;
   ```

   Vous pouvez vous connecter à l'aide du compte d'utilisateur `PERFSTAT` et exécuter les scripts Statspack.
5. Procédez comme suit, en fonction de la version du moteur de votre base de données :
   - Si vous utilisez Oracle 18c ou une version antérieure, passez cette étape.
   - Si vous utilisez Oracle 19c ou une version ultérieure, accordez le privilège `CREATE JOB` au compte `PERFSTAT` à l'aide de l'instruction suivante :

     ```
     GRANT CREATE JOB TO PERFSTAT;
     ```
6. Assurez-vous que les événements d'attente inactifs dans la table `PERFSTAT.STATS$IDLE_EVENT` sont renseignés.

   En raison du bogue 28523746 d'Oracle, les événements d'attente inactifs dans `PERFSTAT.STATS$IDLE_EVENT` peuvent ne pas être renseignés. Pour vous assurer que tous les événements inactifs sont disponibles, exécutez l'instruction suivante :

   ```
   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;
   ```

Génération de rapports Statspack

Un rapport Statspack compare deux instantanés.

Pour générer des rapports Statspack

1. Dans un client SQL, connectez-vous à la base de données Oracle avec le compte `PERFSTAT`.
2. Créez un instantané à l'aide de l'une des techniques suivantes :
   - Créez manuellement un instantané Statspack.
   - Créez une tâche qui prend un instantané Statspack après un intervalle de temps donné. Par exemple, la tâche suivante crée un instantané Statspack chaque heure :

     ```
     VARIABLE jn NUMBER;
     exec dbms_job.submit(:jn, 'statspack.snap;',SYSDATE,'TRUNC(SYSDATE+1/24,''HH24'')');
     COMMIT;
     ```
3. Affichez les instantanés à l'aide de la requête suivante :

   ```
   SELECT SNAP_ID, SNAP_TIME FROM STATS$SNAPSHOT ORDER BY 1;
   ```
4. Exécutez la procédure Amazon RDS `rdsadmin.rds_run_spreport`, en remplaçant begin_snap et end_snap par les ID d'instantané :

   ```
   exec rdsadmin.rds_run_spreport(begin_snap,end_snap);
   ```

   Par exemple, la commande suivante crée un rapport basé sur l'intervalle entre les instantanés Statspack 1 et 2 :

   ```
   exec rdsadmin.rds_run_spreport(1,2);
   ```

   Le nom de fichier du rapport Statspack inclut le numéro des deux instantanés. Par exemple, un fichier de rapport créé à l'aide des instantanés Statspack 1 et 2 se nommera `ORCL_spreport_1_2.lst`.
5. Surveillez la sortie pour détecter des erreurs.

   Oracle Statspack effectue des vérifications avant d'exécuter le rapport. Par conséquent, vous pouvez également voir des messages d'erreur dans la sortie de la commande. Vous pouvez par exemple essayer de générer un rapport basé sur une plage non valable, dans laquelle la valeur de l'instantané Statspack de début est supérieure à la valeur de fin. Dans ce cas, la sortie affiche le message d'erreur, mais le moteur de base de données ne génère pas de fichier d'erreur.

   ```
   exec rdsadmin.rds_run_spreport(2,1);
   *
   ERROR at line 1:
   ORA-20000: Invalid snapshot IDs. Find valid ones in perfstat.stats$snapshot.
   ```

   Si vous utilisez un numéro erroné d'instantané Statspack, la sortie affiche une erreur. Par exemple, si vous essayez de générer un rapport pour les instantanés 1 et 50, mais que l'instantané 50 n'existe pas, la sortie affiche une erreur.

   ```
   exec rdsadmin.rds_run_spreport(1,50);
   *
   ERROR at line 1:
   ORA-20000: Could not find both snapshot IDs
   ```
6. (Facultatif)

Pour récupérer le rapport, appelez les procédures du fichier de trace, selon les explications de la section Utilisation des fichiers de trace Oracle (p. 516).

Vous pouvez également télécharger le rapport Statspack depuis la console RDS. Accédez à la section Journal des détails de l'instance de base de données et choisissez Télécharger :

Si une erreur se produit lors de la génération d'un rapport, le moteur de base de données utilise les mêmes conventions de dénomination que pour un rapport, mais avec une extension .err. Par exemple, si une erreur s'est produite lors de la création d'un rapport à l'aide des instantanés Statspack 1 et 7, le fichier de rapport sera nommé `ORCL_spreport_1_7.err`. Vous pouvez télécharger le rapport d'erreurs en utilisant les mêmes techniques que pour un rapport d'instantané standard.

Suppression de fichiers Statspack

Pour supprimer les fichiers Oracle Statspack, utilisez la commande suivante :

```
exec statspack.purge(begin snap, end snap);
```

Fuseau horaire Oracle

L'option de fuseau horaire vous permet de modifier le fuseau horaire système utilisé par votre instance de base de données Oracle. Par exemple, vous devrez peut-être modifier le fuseau horaire d'une instance de base de données afin qu'elle soit compatible avec un environnement sur site ou une application héritée. L'option de fuseau horaire change le fuseau horaire au niveau de l'hôte. La modification du fuseau horaire impacte toutes les valeurs et colonnes date, y compris `SYSDATE` et `SYSTIMESTAMP`.

L'option de fuseau horaire diffère de la commande `rdsadmin_util.alter_db_time_zone`. La commande `alter_db_time_zone` modifie le fuseau horaire uniquement pour certains types de données. L'option du fuseau horaire modifie le fuseau horaire de toutes les valeurs et colonnes date. Pour de plus amples informations sur `alter_db_time_zone`, veuillez consulter Définition du fuseau horaire de la base de données (p. 1117). Pour de plus amples informations sur les VPC, veuillez consulter Considérations relatives au fuseau horaire (p. 980).

Prérequis pour le fuseau horaire

L'option de fuseau horaire est persistante et permanente. Vous ne pouvez pas supprimer l'option d'un groupe d'options après l'avoir ajoutée. Vous ne pouvez pas supprimer le groupe d'options d'une instance de base de données après l'avoir ajouté. Vous ne pouvez pas remplacer le paramètre de fuseau horaire de l'option par un autre fuseau horaire.

Nous vous conseillons fortement de prendre un instantané de base de données de votre instance de base de données avant d'ajouter l'option de fuseau horaire à une instance de base de données. Grace à l'instantané, vous pouvez restaurer l'instance de base de données si vous définissez l'option de fuseau horaire de manière incorrecte. Pour plus d'informations, consultez Création d'un instantané de base de données (p. 327).

Nous vous conseillons fortement de tester l'option de fuseau horaire sur une instance de base de données avant de l'ajouter à une instances de bases de données de production. L'ajout de l'option de fuseau horaire

peut entraîner des problèmes avec les tables qui utilisent la date système pour ajouter des dates ou des heures. Analysez vos données et applications pour déterminer l'incidence du changement de fuseau horaire.

Paramètres d'option de fuseau horaire

Amazon RDS prend en charge les paramètres suivants pour l'option de fuseau horaire.

Paramètre d'option	Valeurs valides	Description
`TIME_ZONE`	Un des fuseaux horaires disponibles. Pour obtenir la liste complète, consultez Fuseaux horaires disponibles (p. 1090).	Nouveau fuseau horaire de votre instance de base de données.

Ajout de l'option de fuseau horaire

Le processus général d'ajout de l'option de fuseau horaire à une instance de base de données est le suivant :

1. Créer un groupe d'options ou copier ou modifier un groupe existant.
2. Ajouter l'option au groupe d'options.
3. Associer un groupe d'options à une instance de base de données.

Lorsque vous ajoutez l'option de fuseau horaire, une brève interruption de service se produit pendant le redémarrage automatique de votre instance de base de données.

Console

Pour ajouter l'option de fuseau horaire à une instance de base de données

1. Déterminez le groupe d'options que vous voulez utiliser. Vous pouvez créer un groupe d'options ou utiliser un groupe d'options existant. Si vous souhaitez utiliser un groupe d'options existant, passez à l'étape suivante. Sinon, créez un groupe d'options DB personnalisé avec les paramètres suivants :

   a. Pour Moteur, choisissez l'édition oracle pour votre instance de base de données.

   b. Pour Version majeure du moteur, choisissez la version de votre instance de base de données.

   Pour de plus amples informations, veuillez consulter Création d'un groupe d'options (p. 212).

2. Ajoutez l'option Fuseau horaire pour le groupe d'options et configurez les paramètres de l'option.

   > **Important**
   >
   > Si vous ajoutez l'option de fuseau horaire à un groupe d'options existant qui est déjà attaché à une ou plusieurs instances de bases de données, une brève interruption de service a lieu pendant le redémarrage automatique de toutes les instances de bases de données.

   Pour plus d'informations sur l'ajout d'options, consultez Ajout d'une option à un groupe d'options (p. 214). Pour plus d'informations sur chaque paramètre, consultez Paramètres d'option de fuseau horaire (p. 1089).

3. Appliquez le groupe d'options à une instance de base de données nouvelle ou existante:

- Pour une nouvelle instance de base de données, vous appliquez le groupe d'options lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).
- Pour une instance de base de données existante, vous appliquez le groupe d'options en modifiant l'instance et en attachant le nouveau groupe d'options. Lorsque vous ajoutez l'option de fuseau horaire à une instance de base de données existante, une brève panne se produit pendant le redémarrage automatique de votre instance de base de données. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

AWS CLI

L'exemple suivant utilise la commande add-option-to-option-group de l'AWS CLI pour ajouter l'option `Timezone` et le paramètre d'option `TIME_ZONE` à un groupe d'options appelé `myoptiongroup`. Le fuseau horaire par défaut est défini sur `Africa/Cairo`.

Pour Linux, macOS ou Unix :

```
aws rds add-option-to-option-group \
    --option-group-name "myoptiongroup" \
    --options "OptionName=Timezone,OptionSettings=[{Name=TIME_ZONE,Value=Africa/Cairo}]" \
    --apply-immediately
```

Pour Windows :

```
aws rds add-option-to-option-group ^
    --option-group-name "myoptiongroup" ^
    --options "OptionName=Timezone,OptionSettings=[{Name=TIME_ZONE,Value=Africa/Cairo}]" ^
    --apply-immediately
```

Modification des paramètres de fuseau horaire

L'option de fuseau horaire est persistante et permanente. Vous ne pouvez pas supprimer l'option d'un groupe d'options après l'avoir ajoutée. Vous ne pouvez pas supprimer le groupe d'options d'une instance de base de données après l'avoir ajouté. Vous ne pouvez pas remplacer le paramètre de fuseau horaire de l'option par un autre fuseau horaire. Si vous définissez le fuseau horaire de manière incorrecte, restaurez un instantané de votre instance de base de données antérieur à l'ajout de l'option de fuseau horaire.

Suppression de l'option de fuseau horaire

L'option de fuseau horaire est persistante et permanente. Vous ne pouvez pas supprimer l'option d'un groupe d'options après l'avoir ajoutée. Vous ne pouvez pas supprimer le groupe d'options d'une instance de base de données après l'avoir ajouté. Pour supprimer l'option de fuseau horaire, restaurez un instantané de votre instance de base de données antérieur à l'ajout de l'option de fuseau horaire.

Fuseaux horaires disponibles

Les valeurs suivantes peuvent être utilisées pour l'option de fuseau horaire.

disponibilité	Fuseau horaire
Afrique	Afrique/le Caire, Afrique/Casablanca, Afrique/Harare, Afrique/Lagos, Afrique/Luanda, Afrique/Monrovia, Afrique/Nairobi, Afrique/Tripoli, Afrique/Windhoek

disponibilité	Fuseau horaire
Amérique	Amérique/Araguaina, Amérique/Argentine/Buenos_Aires, Amérique/Asuncion, Amérique/Bogota, Amérique/Caracas, Amérique/Chicago, Amérique/Chihuahua, Amérique/Cuiaba, Amérique/Denver, Amérique/Detroit, Amérique/Fortaleza, Amérique/Godthab, Amérique/Guatemala, Amérique/Halifax, Amérique/Lima, Amérique/Los_Angeles, Amérique/Manaus, Amérique/Matamoros, Amérique/Mexico_City, Amérique/Monterrey, Amérique/Montevideo, Amérique/New_York, Amérique/Phoenix, Amérique/Santiago, Amérique/Sao_Paulo, Amérique/Tijuana, Amérique/Toronto
Asie	Asie/Amman, Asie/Achgabat, Asie/Bagdad, Asie/Bakou, Asie/Bangkok, Asie/Beyrouth, Asie/Calcutta, Asie/Damas, Asie/Dhaka, Asie/Hong_Kong, Asie/Irkoutsk, Asie/Jakarta, Asie/Jérusalem, Asie/Kaboul, Asie/Karachi, Asie/Katmandou, Asie/Kolkata, Asie/Krasnoïarsk, Asie/Magadan, Asie/Manille, Asie/Muscat, Asie/Novosibirsk, Asie/Rangoon, Asie/Riyad, Asie/Séoul, Asie/Shanghai, Asie/Singapour, Asie/Taipei, Asie/Téhéran, Asie/Tokyo, Asie/Oulan_Bator, Asie/Vladivostok, Asie/Iakoutsk, Asie/Yerevan
Atlantique	Atlantique/Açores, Atlantic/Cap_Vert
Australie	Australie/Adelaide, Australie/Brisbane, Australie/Darwin, Australie/Eucla, Australie/Hobart, Australie/Lord_Howe, Australie/Perth, Australie/Sydney
Brésil	Brésil/DeNoronha, Brésil/Est
Canada	Canada/Terre-Neuve, Canada/Saskatchewan
Etc	Etc/GMT-3
Europe	Europe/Amsterdam, Europe/Athènes, Europe/Berlin, Europe/Dublin, Europe/Helsinki, Europe/Kaliningrad, Europe/Londres, Europe/Madrid, Europe/Moscou, Europe/Paris, Europe/Prague, Europe/Rome, Europe/Sarajevo
Pacifique	Pacifique/Apia, Pacifique/Auckland, Pacifique/Chatham, Pacifique/Fidji, Pacifique/Guam, Pacifique/Honolulu, Pacifique/Kiritimati, Pacifique/Marquises, Pacifique/Samoa, Pacifique/Tongatapu, Pacifique/Wake
ETATS-UNIS	États-Unis/Alaska, États-Unis/Centre, États-Unis/Indiana Est, États-Unis/Est, États-Unis/Pacifique
UTC	UTC

Voir aussi

- Utilisation de groupes d'options (p. 209)
- Options propres aux instances de bases de données Oracle (p. 1013)
- Définition du fuseau horaire pour les tâches d'Oracle Scheduler (p. 1155)

Oracle Transparent Data Encryption

Amazon RDS prend en charge Oracle TDE (Transparent Data Encryption), fonction de l'option Oracle Advanced Security disponible dans Oracle Enterprise Edition. Cette fonction chiffre automatiquement les données avant qu'elles ne soient écrites dans le stockage et déchiffre automatiquement les données lorsqu'elles sont lues depuis le stockage.

L'option Oracle TDE est utilisée dans les scénarios où vous avez besoin de chiffrer les données sensibles au cas où les sauvegardes et les fichiers de données seraient obtenus par un tiers ou lorsque vous avez besoin de traiter les questions de conformité réglementaire relatives à la sécurité.

L'option TDE est une option permanente qui ne peut pas être supprimée d'un groupe d'options. Vous ne pouvez pas désactiver TDE à partir d'une instance de base de données une fois que cette instance est associée à un groupe d'options avec l'option Oracle TDE. Vous pouvez modifier le groupe d'options d'une instance de base de données qui utilise l'option TDE, mais le groupe d'options associé à l'instance de base de données doit inclure l'option TDE. Vous pouvez également modifier un groupe d'options qui inclut l'option TDE en ajoutant ou en supprimant d'autres options.

Une explication détaillée sur Oracle TDE est au-delà du propos de ce guide. Pour de plus amples informations sur l'utilisation d'Oracle TDE, veuillez consulter Sécurisation des données stockées à l'aide de TDE. Pour de plus amples informations sur Oracle Advanced Security, veuillez consulter Sécurité avancée Oracle dans la documentation Oracle. Pour de plus amples informations sur la sécurité AWS, veuillez consulter le Centre de sécurité AWS.

> **Note**
>
> Vous ne pouvez pas partager un instantané de bases de données qui utilise cette option. Pour plus d'informations sur le partage d'instantanés de base de données, consultez Partage d'un instantané de de base de données (p. 342).

Modes de chiffrement TDE

Oracle TDE prend en charge deux modes de chiffrement : le chiffrement d'espace de table TDE et le chiffrement de colonne TDE. Le chiffrement d'espace de table TDE permet de chiffrer des tables d'application complètes. Le chiffrement de colonne TDE permet de chiffrer les éléments de données qui contiennent des données sensibles. Vous pouvez également appliquer une solution de chiffrement hybride qui utilise les deux chiffrements TDE d'espace de table et de colonne.

> **Note**
>
> Amazon RDS assure la gestion du portefeuille (« wallet ») Oracle et de la clé principale TDE pour l'instance de base de données. Vous n'avez pas besoin de définir la clé de chiffrement à l'aide de la commande `ALTER SYSTEM set encryption key`.

Pour de plus amples informations sur les bonnes pratiques TDE, veuillez consulter Bonnes pratiques d'Oracle Advanced Security TDE (Transparent Data Encryption).

Une fois que l'option est activée, vous pouvez vérifier l'état du portefeuille Oracle en utilisant la commande suivante :

```
SELECT * FROM v$encryption_wallet;
```

Pour créer un espace de table chiffré, utilisez la commande suivante :

```
CREATE TABLESPACE encrypt_ts ENCRYPTION DEFAULT STORAGE (ENCRYPT);
```

Pour spécifier l'algorithme de chiffrement, utilisez la commande suivante :

```
CREATE TABLESPACE encrypt_ts ENCRYPTION USING 'AES256' DEFAULT STORAGE (ENCRYPT);
```

Notez que les commandes précédentes pour chiffrer un tablespace sont les mêmes que celles que vous utiliseriez avec une installation Oracle autre que sur Amazon RDS, et que la syntaxe ALTER TABLE pour chiffrer une colonne est également la même que celle que vous utiliseriez pour une installation Oracle autre que sur Amazon RDS.

Vous devez déterminer si votre instance de base de données est associée à un groupe d'options ayant l'option TDE. Pour afficher le groupe d'options auquel une instance de base de données est associée,

vous pouvez utiliser la console RDS, la commande describe-db-instance de l'AWS CLI ou l'opération d'API DescribeDBInstances.

Pour se conformer à plusieurs normes de sécurité, Amazon RDS travaille à implémenter une rotation automatique régulière de la clé principale.

Ajout de l'option TDE

Le processus d'utilisation d'Oracle TDE avec Amazon RDS est le suivant :

1. Si l'instance de base de données n'est pas associée à un groupe d'options pour lequel l'option TDE est activée, vous devez soit créer un groupe d'options et ajouter l'option TDE soit modifier le groupe d'options associé pour ajouter l'option TDE. Pour plus d'informations sur la création ou la modification d'un groupe d'options, consultez Utilisation de groupes d'options (p. 209). Pour plus d'informations sur l'ajout d'une option à un groupe d'options, consultez Ajout d'une option à un groupe d'options (p. 214).
2. Associez l'instance de base de données au groupe d'options avec l'option TDE. Pour plus d'informations sur l'association d'une instance de base de données à un groupe d'options, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Suppression de l'option TDE

Si vous ne souhaitez plus utiliser l'option TDE avec une instance de base de données, vous devez déchiffrer toutes vos données sur l'instance de base de données, copier les données sur une nouvelle instance de base de données qui n'est pas associée à un groupe d'options pour lequel TDE est activé, puis supprimer l'instance d'origine. Vous pouvez renommer la nouvelle instance avec le même nom que celui de l'instance de base de données précédente, si vous le souhaitez.

Utilisation de TDE avec Oracle Data Pump

Vous pouvez utiliser Oracle Data Pump pour importer ou exporter des fichiers de vidage chiffrés. Amazon RDS prend en charge le mode de chiffrement de mot de passe (ENCRYPTION_MODE=PASSWORD) pour Oracle Data Pump. Amazon RDS ne prend pas en charge le mode de chiffrement transparent (ENCRYPTION_MODE=TRANSPARENT) pour Oracle Data Pump. Pour plus d'informations sur l'utilisation d'Oracle Data Pump avec Amazon RDS, consultez Importation à l'aide d'Oracle Data Pump (p. 991).

Oracle UTL_MAIL

Amazon RDS prend en charge Oracle UTL_MAIL via l'utilisation de l'option UTL_MAIL et des serveurs SMTP. Vous pouvez directement envoyez des e-mail de votre base de données à l'aide du package UTL_MAIL. Amazon RDS prend en charge UTL_MAIL pour les versions suivantes d'Oracle :

- Oracle version 19.0.0.0, toutes les versions
- Oracle version 18.0.0.0, toutes les versions
- Oracle version 12.2.0.1, toutes les versions
- Oracle, versions 12.1.0.2.v5 et ultérieures
- Oracle, versions 11.2.0.4.v9 et ultérieures

Voici quelques limitations à l'utilisation de UTL_MAIL :

- UTL_MAIL ne prend pas en charge le certificat TLS (Transport Layer Security) et les e-mails ne sont donc pas chiffrés.

  Pour vous connecter en toute sécurité aux ressources SSL/TLS distantes en créant et en chargeant des portefeuilles Oracle personnalisés, suivez les instructions dans Utilisation de utl_http, utl_tcp et utl_smtp avec une instance de base de données Oracle (p. 957).

Les certificats spécifiques requis pour votre portefeuille varient par service. Pour les services AWS, vous les trouverez généralement dans le Référentiel des services d'approbation Amazon.

- UTL_MAIL ne prend pas en charge l'authentification avec les serveurs SMTP.
- Vous ne pouvez envoyer qu'une seule pièce jointe dans un e-mail.
- Vous ne pouvez pas envoyer de pièces jointes de plus de 32 Ko.
- Vous pouvez uniquement utiliser des codages de caractères ASCII et EBCDIC (Extended Binary Coded Decimal Interchange Code).
- Le port SMTP (25) est limité en fonction des stratégies du propriétaire de l'interface réseau Elastic.

Lorsque vous activez UTL_MAIL, seul l'utilisateur principal pour votre instance de base de données se voir accorder le privilège d'exécution. Si nécessaire, l'utilisateur principal peut accorder le privilège d'exécution à d'autres utilisateurs de sorte qu'ils puissent utiliser UTL_MAIL.

> **Important**
>
> Nous vous recommandons d'activer la fonctionnalité d'audit intégrée d'Oracle pour suivre l'utilisation des procédures UTL_MAIL.

Prérequis pour Oracle UTL_MAIL

Les conditions suivantes sont requises pour utiliser Oracle UTL_MAIL :

- Un ou plusieurs serveurs SMTP et les adresses IP correspondantes ou noms DNS (Domain Name Server) publics ou privés correspondants. Pour plus d'informations sur la résolution des noms DNS privés grâce à un serveur DNS personnalisé, consultez Configuration d'un serveur DNS personnalisé (p. 1114).
- Pour les versions d'Oracle antérieures à 12c, votre instance de base de données doit également utiliser l'option DB XML. Pour plus d'informations, consultez Oracle XML DB (p. 1096).

Ajout de l'option UTL_MAIL d'Oracle

Le processus général d'ajout de l'option UTL_MAIL d'Oracle à une instance de base de données est le suivant :

1. Créer un groupe d'options ou copier ou modifier un groupe existant.
2. Ajouter l'option au groupe d'options.
3. Associez le groupe d'options à l'instance de base de données.

Une fois l'option UTL_MAIL ajoutée, dès que le groupe d'options est actif, UTL_MAIL est actif.

Pour ajouter l'option UTL_MAIL à une instance de base de données

1. Déterminez le groupe d'options que vous voulez utiliser. Vous pouvez créer un groupe d'options ou utiliser un groupe d'options existant. Si vous souhaitez utiliser un groupe d'options existant, passez à l'étape suivante. Sinon, créez un groupe d'options DB personnalisé avec les paramètres suivants :

   a. Pour Moteur, sélectionnez l'édition d'Oracle que vous voulez utiliser.
   b. Pour Version majeure du moteur, choisissez la version de votre instance de base de données.

   Pour de plus amples informations, veuillez consulter Création d'un groupe d'options (p. 212).
2. Ajouter l'option UTL_MAIL au groupe d'options. Pour de plus amples informations sur l'ajout d'options, veuillez consulter Ajout d'une option à un groupe d'options (p. 214).

3. Appliquez le groupe d'options à une instance de base de données nouvelle ou existante:
   - Pour une nouvelle instance de base de données, vous appliquez le groupe d'options lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).
   - Pour une instance de base de données existante, vous appliquez le groupe d'options en modifiant l'instance et en attachant le nouveau groupe d'options. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Utilisation de l'option UTL_MAIL d'Oracle

Une fois que vous activez l'option UTL_MAIL, vous devez configurer le serveur SMTP avant de pouvoir commencer à l'utiliser.

Vous configurez le serveur SMTP en définissant le paramètre SMTP_OUT_SERVER à une adresse IP ou à un nom DNS public valide. Pour le paramètre SMTP_OUT_SERVER, vous pouvez spécifier une liste séparée par des virgules des adresses de plusieurs serveurs. Si le premier serveur n'est pas disponible, UTL_MAIL essaie le serveur suivant et ainsi de suite.

Vous pouvez définir la valeur par défaut SMTP_OUT_SERVER pour une instance de base de données à l'aide d'un groupe de paramètres de base de données. Vous pouvez définir le paramètre SMTP_OUT_SERVER pour une session en exécutant le code suivant sur votre base de données dans votre instance de base de données.

```
ALTER SESSION SET smtp_out_server = mailserver.domain.com:25;
```

Une fois que l'option UTL_MAIL est activée, et que votre SMTP_OUT_SERVER est configuré, vous pouvez envoyer un message à l'aide de la procédure `SEND`. Pour plus d'informations, consultez UTL_MAIL dans la documentation Oracle.

Suppression de l'option UTL_MAIL d'Oracle

Vous pouvez supprimer l'option UTL_MAIL d'Oracle d'une instance de base de données.

Pour supprimer l'option UTL_MAIL d'une instance de base de données, effectuez une des actions suivantes :

- Pour supprimer l'option UTL_MAIL de plusieurs instances de bases de données, supprimez l'option UTL_MAIL du groupe d'option auquel elles appartiennent. Ce changement affecte toutes les instances de bases de données qui utilisent le groupe d'options. Pour plus d'informations, consultez Suppression d'une option d'un groupe d'options (p. 222).
- Pour supprimer l'option UTL_MAIL d'une seule instance de base de données, modifiez l'instance de base de données et spécifiez un autre groupe d'options qui n'inclut pas l'option UTL_MAIL. Vous pouvez spécifier le groupe d'options (vide) par défaut, ou un groupe d'options personnalisées différent. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Dépannage

Problèmes que vous pouvez rencontrer lorsque vous utilisez UTL_MAIL avec Amazon RDS :

- Limitation. Le port SMTP (25) est limité en fonction des stratégies du propriétaire de l'interface réseau Elastic. Si vous pouvez envoyer des e-mails en utilisant UTL_MAIL et que l'erreur `ORA-29278: SMTP transient error: 421 Service not available` s'affiche, vous faites peut-être l'objet d'une limitation. Si vous rencontrez une limitation dans le cadre de la remise d'e-mails, nous vous

recommandons d'implémenter un algorithme d'interruption. Pour de plus amples informations sur les algorithmes d'interruption, veuillez consulter Nouvelles tentatives après erreur et backoff exponentiel dans AWS et Comment traiter une erreur « Throttling – Maximum sending rate exceeded ».

Vous pouvez demander que cette limitation soit supprimée. Pour de plus amples informations, veuillez consulter Comment supprimer la limitation du port 25 à partir de mon instance EC2 ?.

Oracle XML DB

Oracle XML DB ajoute la prise en charge XML native à votre instance de base de données. Avec XML DB, vous pouvez stocker et récupérer des données XML structurées ou non structurées, en plus des données relationnelles.

XML DB est pré-installé sur la version 12c et ultérieures d'Oracle. Amazon RDS prend en charge Oracle XML DB pour la version 11g via l'utilisation de l'option XMLDB. Une fois que vous avez appliqué l'option XMLDB à votre instance de base de données, vous bénéficiez d'un accès complet au référentiel Oracle XML DB ; aucune tâche n'est requise après l'installation.

> **Note**
>
> L'option Amazon RDS XMLDB n'autorise pas la prise en charge du serveur de protocoles Oracle XML DB.

Ajout de l'option de base de données Oracle XML

Le processus général d'ajout de l'option de base de données Oracle XML à une instance de base de données est le suivant :

1. Créer un groupe d'options ou copier ou modifier un groupe existant.
2. Ajouter l'option au groupe d'options.
3. Associer un groupe d'options à une instance de base de données.

Une fois que vous avez ajouté l'option XML DB, dès que le groupe d'options est actif, XML DB est actif.

Pour ajouter l'option XML DB à une instance de base de données

1. Déterminez le groupe d'options que vous voulez utiliser. Vous pouvez créer un groupe d'options ou utiliser un groupe d'options existant. Si vous souhaitez utiliser un groupe d'options existant, passez à l'étape suivante. Sinon, créez un groupe d'options DB personnalisé avec les paramètres suivants :

   a. Pour Moteur, sélectionnez l'édition d'Oracle que vous voulez utiliser.
   b. Pour Version majeure du moteur, choisissez 11.2.

   Pour plus d'informations, consultez Création d'un groupe d'options (p. 212).
2. Ajoutez l'option XMLDB au groupe d'options. Pour plus d'informations sur l'ajout d'options, consultez Ajout d'une option à un groupe d'options (p. 214).
3. Appliquez le groupe d'options à une instance de base de données nouvelle ou existante:

   - Pour une nouvelle instance de base de données, vous appliquez le groupe d'options lorsque vous lancez l'instance. Pour plus d'informations, consultez Création d'une instance de base de données Amazon RDS (p. 146).
   - Pour une instance de base de données existante, vous appliquez le groupe d'options en modifiant l'instance et en attachant le nouveau groupe d'options. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Suppression de l'option Oracle XML DB

Vous pouvez supprimer l'option XML DB à partir d'une instance de base de données exécutant la version 11g.

Pour supprimer l'option XML DB d'une instance de base de données exécutant la version 11g, effectuez l'une des actions suivantes :

- Pour supprimer l'option XMLDB de plusieurs instances de bases de données, supprimez l'option XMLDB du groupe d'options auquel elles appartiennent. Ce changement affecte toutes les instances de bases de données qui utilisent le groupe d'options. Pour plus d'informations, consultez Suppression d'une option d'un groupe d'options (p. 222).
- Pour supprimer l'option XMLDB d'une instance de base de données particulière, modifiez l'instance de base de données et spécifiez un autre groupe d'options qui n'inclut pas l'option XMLDB. Vous pouvez spécifier le groupe d'options (vide) par défaut, ou un groupe d'options personnalisées différent. Pour plus d'informations, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Tâches DBA courantes pour les instances de bases de données Oracle

Vous trouverez ci-après une description, pour des implémentations spécifiques à Amazon RDS, de certaines tâches DBA courantes pour les instances de base de données RDS exécutant le moteur de base de données Oracle. Pour offrir une expérience de service géré, Amazon RDS ne fournit pas l'accès shell aux instances de base de données et limite l'accès à certaines tables et procédures système qui requièrent des privilèges avancés.

Les tâches DBA courantes pour les instances de base de données exécutant Oracle sont les suivantes :

- Tâches système (p. 1103)

Déconnexion d'une session (p. 1103)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.disconnect` Méthode Oracle: `alter system disconnect session`
Terminer une session (p. 1104)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.kill` Méthode Oracle: `alter system kill session`
Annulation d'une instruction SQL dans une session (p. 1105)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.cancel` Méthode Oracle : `alter system cancel sql`
Activation et désactivation de sessions restreintes (p. 1105)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.restricted_s` Méthode Oracle: `alter system enable restricted session`

Vidage du pool partagé (p. 1106)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.flush_shared` Méthode Oracle: `alter system flush shared_pool`
Vidage du cache de tampon (p. 1107)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.flush_buffer` Méthode Oracle: `alter system flush buffer_cache`
Octroi des privilèges SELECT ou EXECUTE aux objets SYS (p. 1107)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.grant_sys_ob` Méthode Oracle: `grant`
Retrait des privilèges SELECT ou EXECUTE sur les objets SYS (p. 1108)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.revoke_sys_o` Méthode Oracle: `revoke`
Attribution de privilèges à des utilisateurs non-maîtres (p. 1109)	Méthode Amazon RDS : `grant` Méthode Oracle: `grant`
Création de fonctions personnalisées pour vérifier les mots de passe (p. 1110)	Méthode Amazon RDS : `rdsadmin.rdsadmin_password_verify.c` Méthode Amazon RDS : `rdsadmin.rdsadmin_password_verify.c`
Configuration d'un serveur DNS personnalisé (p. 1114)	—

- Tâches de base de données (p. 1115)

Modification du nom global d'une base de données (p. 1115)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.rename_global_name` Méthode Oracle: `alter database rename`
Création et dimensionnement des espaces de table (p. 1116)	Méthode Amazon RDS : `create tablespace` Méthode Oracle: `alter database`
Définition de l'espace de table par défaut (p. 1116)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.alter_default_tablespace` Méthode Oracle : `alter database default tablespace`
Définition de l'espace de table temporaire par défaut (p. 1117)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.alter_default_temp_tablespace` Méthode Oracle : `alter database default temporary tablespace`

Création d'un point de contrôle de base de données (p. 1117)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.checkpoint` Méthode Oracle: `alter system checkpoint`
Définition d'une récupération distribuée (p. 1117)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.enable_distr_recovery` Méthode Oracle : `alter system enable distributed recovery`
Définition du fuseau horaire de la base de données (p. 1117)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.alter_db_time_zone` Méthode Oracle : `alter database set time_zone`
Utilisation de tables externes Oracle (p. 1118)	—
Génération de rapports de performance avec AWR (Automatic Workload Repository) (p. 1119)	Méthode Amazon RDS : procédures `rdsadmin.rdsadmin_diagnostic_util` Méthode Oracle : package `dbms_workload_repository`
Réglage des liens de base de données pour une utilisation avec les instances de base de données dans un VPC (p. 1123)	—
Définition de l'édition par défaut d'une instance de base de données (p. 1123)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.alter_default_edition` Méthode Oracle: `alter database default edition`
Activation de l'audit pour la table SYS.AUD$ (p. 1124)	Méthode Amazon RDS : `rdsadmin.rdsadmin_master_util.audit_all_sys_aud_table` Méthode Oracle : `audit`
Désactivation de l'audit pour la table SYS.AUD$ (p. 1124)	Méthode Amazon RDS : `rdsadmin.rdsadmin_master_util.noaudit_all_sys_aud_table` Méthode Oracle : `noaudit`
Nettoyage de builds d'index en ligne interrompues (p. 1125)	Méthode Amazon RDS : `rdsadmin.rdsadmin_dbms_repair.online_index_clean` Méthode Oracle: `dbms_repair.online_index_clean`
Ignorer les blocs corrompus (p. 1126)	Méthode Amazon RDS : plusieurs procédures `rdsadmin.rdsadmin_dbms_repair` Méthode Oracle : package `dbms_repair`
Redimensionnement de l'espace de table temporaire dans un réplica en lecture (p. 1128)	Méthode Amazon RDS : procédure `rdsadmin.rdsadmin_util.resize_temp_tablespace` ou `rdsadmin.rdsadmin_util.resize_tempfile` Méthode Oracle : —

Purge de la corbeille (p. 1129)	Méthode Amazon RDS : `exec rdsadmin.rdsadmin_util.purge_dba_recyclebin` Méthode Oracle: `purge dba_recyclebin`

- Tâches de journal (p. 1129)

Configuration du mode FORCE LOGGING (p. 1129)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.force_loggin` Méthode Oracle: `alter database force logging`
Configuration d'une journalisation supplémentaire (p. 1130)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.alter_supple` Méthode Oracle: `alter database add supplemental log`
Changement de fichiers journaux en ligne (p. 1131)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.switch_logfi` Méthode Oracle: `alter system switch logfile`
Ajout de journaux redo en ligne (p. 1131)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.add_logfile`
Suppression de journaux redo en ligne (p. 1132)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.drop_logfile`
Redimensionnement de journaux redo en ligne (p. 1132)	—
Conservation des journaux redo archivés (p. 1134)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.set_configur`
Accès aux journaux de transactions (p. 1135)	Méthode Amazon RDS : `rdsadmin.rdsadmin_master_util.creat` Méthode Amazon RDS : `rdsadmin.rdsadmin_master_util.creat`

- Tâches RMAN (p. 1136)

Validation des fichiers d'instance de base de données (p. 1140)	Méthode Amazon RDS : `rdsadmin_rman_util.`*`procedure`* Méthode Oracle : `RMAN VALIDATE`

Activation et désactivation du suivi des modifications de bloc (p. 1143)	Méthode Amazon RDS : `rdsadmin_rman_util.procedure` Méthode Oracle : `ALTER DATABASE`
Recoupement des journaux redo archivés (p. 1144)	Méthode Amazon RDS : `rdsadmin_rman_util.crosscheck_archi` Méthode Oracle : `RMAN BACKUP`
Sauvegarde des journaux redo archivés (p. 1145)	Méthode Amazon RDS : `rdsadmin_rman_util.procedure` Méthode Oracle : `RMAN BACKUP`
Réalisation d'une sauvegarde complète de base de données (p. 1150)	Méthode Amazon RDS : `rdsadmin_rman_util.backup_database_` Méthode Oracle : `RMAN BACKUP`
Réalisation d'une sauvegarde incrémentielle de base de données (p. 1151)	Méthode Amazon RDS : `rdsadmin_rman_util.backup_database_` Méthode Oracle : `RMAN BACKUP`
Réalisation d'une sauvegarde d'espace de table (p. 1152)	Méthode Amazon RDS : `rdsadmin_rman_util.backup_database_` Méthode Oracle : `RMAN BACKUP`

- Tâches Oracle Scheduler (p. 1153)

Modification des travaux DBMS_SCHEDULER (p. 1154)	Méthode Amazon RDS : `dbms_scheduler.set_attribute` Méthode Oracle: `dbms_scheduler.set_attribute`
Définition du fuseau horaire pour les tâches d'Oracle Scheduler (p. 1155)	Méthode Amazon RDS : `dbms_scheduler.set_attribute` Méthode Oracle: `dbms_scheduler.set_attribute`
Désactivation de travaux Oracle Scheduler relevant de SYS (p. 1156)	Méthode Amazon RDS : `rdsadmin.rdsadmin_dbms_scheduler.di` Méthode Oracle : `dbms_scheduler.disable`
Activation de travaux Oracle Scheduler relevant de SYS (p. 1156)	Méthode Amazon RDS : `rdsadmin.rdsadmin_dbms_scheduler.en` Méthode Oracle : `dbms_scheduler.enable`

Modification de l'intervalle de répétition pour des travaux de type CALENDAR (p. 1156)	Méthode Amazon RDS : `rdsadmin.rdsadmin_dbms_scheduler.se` Méthode Oracle: `dbms_scheduler.set_attribute`
Modification de l'intervalle de répétition pour des travaux de type NAMED (p. 1157)	Méthode Amazon RDS : `rdsadmin.rdsadmin_dbms_scheduler.se` Méthode Oracle: `dbms_scheduler.set_attribute`

- Tâches de diagnostic (p. 1158)

Répertorier les incidents (p. 1159)	Méthode Amazon RDS : `rdsadmin.rdsadmin_adrci_util.list_a` Méthode Oracle : commande ADRCI `show incident`
Répertorier les problèmes (p. 1160)	Méthode Amazon RDS : `rdsadmin.rdsadmin_adrci_util.list_a` Méthode Oracle : commande ADRCI `show problem`
Création de packages d'incidents (p. 1162)	Méthode Amazon RDS : `rdsadmin.rdsadmin_adrci_util.create` Méthode Oracle : commande ADRCI `ips create package`
Affichage des fichiers de trace (p. 1163)	Méthode Amazon RDS : `rdsadmin.rdsadmin_adrci_util.show_a` Méthode Oracle : commande ADRCI `show tracefile`

- Autres tâches (p. 1164)

Création et suppression de répertoires dans l'espace de stockage de données principal (p. 1164)	Méthode Amazon RDS : `rdsadmin.rdsadmin_util.create_direc` Méthode Oracle: `CREATE DIRECTORY` Méthode Amazon RDS : `rdsadmin.rdsadmin_util.drop_directo` Méthode Oracle: `DROP DIRECTORY`

Établissement de la liste des fichiers situés dans un répertoire d'instance de base de données (p. 1165)	Méthode Amazon RDS : `rdsadmin.rds_file_util.listdir` Méthode Oracle : —
Lecture de fichiers dans un répertoire d'instance de base de données (p. 1166)	Méthode Amazon RDS : `rdsadmin.rds_file_util.read_text_fi` Méthode Oracle : —
Accès aux fichiers Opatch (p. 1166)	Méthode Amazon RDS : `rdsadmin.rds_file_util.read_text_fi` ou `rdsadmin.tracefile_listing` Méthode Oracle: `opatch`

Vous pouvez également utiliser les procédures Amazon RDS pour l'intégration de Amazon S3 avec Oracle et pour l'exécution de tâches de base de données OEM Management Agent. Pour plus d'informations, consultez Intégration Amazon S3 (p. 1014) et Exécution de tâches de base de données avec l'option Management Agent (p. 1049).

Tâches système DBA courantes pour les instances de bases de données Oracle

Vous trouverez ci-dessous des informations sur la façon d'effectuer certaines tâches DBA courantes liées au système sur vos instances de base de données Amazon RDS exécutant Oracle. Pour offrir une expérience de service géré, Amazon RDS ne fournit pas l'accès shell aux instances de base de données et limite l'accès à certaines tables et procédures système qui requièrent des privilèges avancés.

Rubriques

- Déconnexion d'une session (p. 1103)
- Terminer une session (p. 1104)
- Annulation d'une instruction SQL dans une session (p. 1105)
- Activation et désactivation de sessions restreintes (p. 1105)
- Vidage du pool partagé (p. 1106)
- Vidage du cache de tampon (p. 1107)
- Octroi des privilèges SELECT ou EXECUTE aux objets SYS (p. 1107)
- Retrait des privilèges SELECT ou EXECUTE sur les objets SYS (p. 1108)
- Attribution de privilèges à des utilisateurs non-maîtres (p. 1109)
- Création de fonctions personnalisées pour vérifier les mots de passe (p. 1110)
- Configuration d'un serveur DNS personnalisé (p. 1114)

Déconnexion d'une session

Pour déconnecter la session en cours en mettant fin au processus serveur dédié, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.disconnect`. La procédure `disconnect` comporte les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`sid`	nombre	—	Oui	Identifiant de session.
`serial`	nombre	—	Oui	Numéro de série de la session.
`method`	varchar	'IMMEDIATE'	Non	Les valeurs valides sont `'IMMEDIATE'` ou `'POST_TRANSACTION'`.

L'exemple suivant déconnecte une session.

```
begin
    rdsadmin.rdsadmin_util.disconnect(
        sid     => sid,
        serial => serial_number);
end;
/
```

Pour obtenir l'identifiant et le numéro de série de la session, interrogez la vue `V$SESSION`. L'exemple suivant obtient toutes les sessions pour l'utilisateur `AWSUSER`.

```
select SID, SERIAL#, STATUS from V$SESSION where USERNAME = 'AWSUSER';
```

La base de données doit être ouverte pour pouvoir utiliser cette méthode. Pour plus d'informations sur la déconnexion d'une session, consultez ALTER SYSTEM (MODIFIER SYSTÈME) dans la documentation Oracle.

Terminer une session

Pour arrêter une session, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.kill`. La procédure `kill` comporte les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`sid`	nombre	—	Oui	Identifiant de session.
`serial`	nombre	—	Oui	Numéro de série de la session.
`method`	varchar	null	Non	Les valeurs valides sont `'IMMEDIATE'` ou `'PROCESS'`.

L'exemple suivant met fin à une session.

```
begin
    rdsadmin.rdsadmin_util.kill(
        sid     => sid,
        serial => serial_number);
end;
```

```
/
```

Pour obtenir l'identifiant et le numéro de série de la session, interrogez la vue `V$SESSION`. L'exemple suivant obtient toutes les sessions pour l'utilisateur `AWSUSER`.

```
SELECT SID, SERIAL#, STATUS FROM V$SESSION WHERE USERNAME = 'AWSUSER';
```

Vous pouvez spécifier `IMMEDIATE` ou `PROCESS` comme valeur pour le paramètre `method`. En spécifiant `PROCESS` comme valeur de `method`, vous pouvez arrêter les processus associés à une session. Ne procédez ainsi que si la session n'a pas été arrêtée en utilisant `IMMEDIATE` comme valeur de `method`.

Annulation d'une instruction SQL dans une session

Pour annuler une instruction SQL dans une session, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.cancel`.

> **Note**
>
> Cette procédure est prise en charge pour Oracle version 18.0.0.0 et ultérieures.

La procédure `cancel` comporte les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`sid`	nombre	—	Oui	Identifiant de session.
`serial`	nombre	—	Oui	Numéro de série de la session.
`sql_id`	varchar2	null	Non	Identifiant SQL de l'instruction SQL.

L'exemple suivant annuler une instruction SQL dans une session.

```
begin
    rdsadmin.rdsadmin_util.cancel(
        sid    => sid,
        serial => serial_number,
        sql_id => sql_id);
end;
/
```

Pour obtenir l'identifiant et le numéro de série de la session ainsi que l'identifiant SQL d'une instruction SQL, interrogez la vue `V$SESSION`. L'exemple suivant obtient toutes les sessions et les identifiants SQL pour l'utilisateur `AWSUSER`.

```
select SID, SERIAL#, SQL_ID, STATUS from V$SESSION where USERNAME = 'AWSUSER';
```

Activation et désactivation de sessions restreintes

Pour activer et désactiver des sessions restreintes, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.restricted_session`. La procédure `restricted_session` comporte les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Oui	Description
`p_enable`	booléen	true	Non	Définissez ce paramètre sur `true` pour activer les sessions restreintes ou sur `false` pour les désactiver.

L'exemple suivant montre comment activer et désactiver les sessions restreintes.

```
/* 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
```

Vidage du pool partagé

Pour vider le pool partagé, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.flush_shared_pool`. La procédure `flush_shared_pool` ne comporte aucun paramètre.

L'exemple suivant vide le pool partagé.

```
exec rdsadmin.rdsadmin_util.flush_shared_pool;
```

Vidage du cache de tampon

Pour vider le cache de tampon, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.flush_buffer_cache`. La procédure `flush_buffer_cache` ne comporte aucun paramètre.

L'exemple suivant vide le cache des tampons.

```
exec rdsadmin.rdsadmin_util.flush_buffer_cache;
```

Octroi des privilèges SELECT ou EXECUTE aux objets SYS

Généralement, vous transférez les privilèges en utilisant des rôles, qui peuvent contenir de nombreux objets. Pour accorder des privilèges à un objet unique, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.grant_sys_object`. La procédure accorde uniquement les privilèges qui ont déjà été accordés à l'utilisateur principal par le biais d'un rôle ou d'une attribution directe.

La procédure `grant_sys_object` comporte les paramètres suivants.

> **Important**
>
> Pour toutes les valeurs de paramètre, utilisez les majuscules sauf si vous avez créé l'utilisateur avec un identifiant sensible à la casse. Par exemple, si vous exécutez `CREATE USER myuser` ou `CREATE USER MYUSER`, le dictionnaire de données stocke `MYUSER`. Toutefois, si vous utilisez des guillemets doubles dans `CREATE USER "MyUser"`, le dictionnaire de données stocke `MyUser`.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`p_obj_name`	varchar2	—	Oui	Nom de l'objet pour lequel des privilèges seront accordés. L'objet peut être un répertoire, une fonction, un package, une procédure, une séquence, une table ou une vue. Les noms d'objet doivent être orthographiés correctement lorsqu'ils apparaissent dans `DBA_OBJECTS`. La plupart des objets système sont définis en majuscules, si bien que nous vous recommandons d'essayer cela en premier lieu.
`p_grantee`	varchar2	—	Oui	Nom de l'objet auquel des privilèges seront accordés. L'objet peut être un schéma ou un rôle.
`p_privilege`	varchar2	null	Oui	—
`p_grant_option`	booléen	false	Non	Définissez ce paramètre sur `true` pour l'utiliser avec l'option d'attribution. Le paramètre `p_grant_option` est

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
				pris en charge pour les versions Oracle 11.2.0.4.v8 et ultérieures, 12.1.0.2.v4 et ultérieures, toutes les versions 12.2.0.1, toutes les versions 18.0.0.0 et toutes les versions 19.0.0.

L'exemple suivant accorde des privilèges select sur un objet nommé `V_$SESSION` à un utilisateur nommé `USER1`.

```
begin
    rdsadmin.rdsadmin_util.grant_sys_object(
        p_obj_name  => 'V_$SESSION',
        p_grantee   => 'USER1',
        p_privilege => 'SELECT');
end;
/
```

L'exemple suivant accorde des privilèges select sur un objet nommé `V_$SESSION` à un utilisateur nommé `USER1` avec l'option d'attribution.

```
begin
    rdsadmin.rdsadmin_util.grant_sys_object(
        p_obj_name     => 'V_$SESSION',
        p_grantee      => 'USER1',
        p_privilege    => 'SELECT',
        p_grant_option => true);
end;
/
```

Pour pouvoir attribuer des privilèges sur un objet, votre compte doit avoir ces privilèges directement attribués avec l'option appropriée ou via un rôle accordé avec `with admin option`. Le plus souvent, vous voudrez attribuer `SELECT` sur une vue DBA qui a été attribuée au rôle `SELECT_CATALOG_ROLE`. Si ce rôle n'est pas déjà directement attribué à votre utilisateur avec `with admin option`, vous ne pouvez pas transférer le privilège. Si vous disposez du privilège DBA, vous pouvez accorder le rôle directement à un autre utilisateur.

L'exemple suivant accorde les rôles `SELECT_CATALOG_ROLE` et `EXECUTE_CATALOG_ROLE` à `USER1`. Étant donné que `with admin option` est utilisé, `USER1` peut désormais accorder l'accès aux objets SYS qui ont été attribués à `SELECT_CATALOG_ROLE`.

```
GRANT SELECT_CATALOG_ROLE TO USER1 WITH ADMIN OPTION;
GRANT EXECUTE_CATALOG_ROLE to USER1 WITH ADMIN OPTION;
```

Les objets déjà attribués à `PUBLIC` n'ont pas besoin d'être réattribués. Si vous utilisez la procédure `grant_sys_object` pour accorder de nouveau l'accès, l'appel de procédure réussit.

Retrait des privilèges SELECT ou EXECUTE sur les objets SYS

Pour retirer des privilèges sur un objet unique, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.revoke_sys_object`. La procédure révoque uniquement les privilèges qui ont déjà été accordés au compte principal par le biais d'un rôle ou d'une attribution directe.

La procédure `revoke_sys_object` comporte les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
p_obj_name	varchar2	—	Oui	Nom de l'objet pour lequel des privilèges seront révoqués. L'objet peut être un répertoire, une fonction, un package, une procédure, une séquence, une table ou une vue. Les noms d'objet doivent être orthographiés correctement lorsqu'ils apparaissent dans DBA_OBJECTS. La plupart des objets système sont définis en majuscules, c'est pourquoi nous vous recommandons d'essayer cette méthode en premier lieu.
p_revokee	varchar2	—	Oui	Nom de l'objet pour lequel des privilèges seront révoqués. L'objet peut être un schéma ou un rôle.
p_privilege	varchar2	null	Oui	—

L'exemple suivant révoque des privilèges select sur un objet nommé V_$SESSION à un utilisateur nommé USER1.

```
begin
    rdsadmin.rdsadmin_util.revoke_sys_object(
        p_obj_name  => 'V_$SESSION',
        p_revokee   => 'USER1',
        p_privilege => 'SELECT');
end;
/
```

Attribution de privilèges à des utilisateurs non-maîtres

Vous pouvez accorder des privilèges select pour de nombreux objets dans le schéma SYS grâce au rôle SELECT_CATALOG_ROLE. Le rôle SELECT_CATALOG_ROLE accorde aux utilisateurs des privilèges SELECT sur les vues du dictionnaire de données. L'exemple suivant accorde le rôle SELECT_CATALOG_ROLE à un utilisateur nommé user1.

```
GRANT SELECT_CATALOG_ROLE TO user1;
```

Vous pouvez accorder des privilèges EXECUTE pour de nombreux objets dans le schéma SYS grâce au rôle EXECUTE_CATALOG_ROLE. Le rôle EXECUTE_CATALOG_ROLE accorde aux utilisateurs des privilèges EXECUTE pour les packages et les procédures du dictionnaire de données. L'exemple suivant accorde le rôle EXECUTE_CATALOG_ROLE à un utilisateur nommé user1.

```
GRANT EXECUTE_CATALOG_ROLE TO user1;
```

L'exemple suivant obtient les autorisations permises par les rôles `SELECT_CATALOG_ROLE` et `EXECUTE_CATALOG_ROLE`.

```
  SELECT *
    FROM ROLE_TAB_PRIVS
   WHERE ROLE IN ('SELECT_CATALOG_ROLE','EXECUTE_CATALOG_ROLE')
ORDER BY ROLE, TABLE_NAME ASC;
```

L'exemple suivant crée un utilisateur non maître nommé `user1`, accorde le privilège `CREATE SESSION`, puis accorde le privilège `SELECT` sur une base de données nommée sh.sales.

```
CREATE USER user1 IDENTIFIED BY PASSWORD;
GRANT CREATE SESSION TO user1;
GRANT SELECT ON sh.sales TO user1;
```

Création de fonctions personnalisées pour vérifier les mots de passe

Vous pouvez créer une fonction de vérification de mot de passe personnalisée de deux façons. Si vous voulez utiliser la logique de vérification standard et stocker votre fonction dans le schéma `SYS`, utilisez la procédure `create_verify_function`. Si vous voulez utiliser une logique de vérification personnalisée ou ne souhaitez pas stocker votre fonction dans le schéma `SYS`, utilisez la procédure `create_passthrough_verify_fcn`.

Procédure create_verify_function

La procédure `create_verify_function` est prise en charge pour Oracle version 11.2.0.4.v9 et ultérieures, Oracle version 12.1.0.2.v5 et ultérieures, toutes les versions 12.2.0.1, toutes les versions 18.0.0.0 et toutes les versions 19.0.0.

Vous pouvez créer une fonction personnalisée pour vérifier les mots de passe en utilisant la procédure Amazon RDS `rdsadmin.rdsadmin_password_verify.create_verify_function`. La procédure `create_verify_function` possède les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`p_verify_function_name`	varchar2	—	Oui	Nom de la fonction personnalisée. Cette fonction est automatiquement créée dans le schéma SYS. Elle est affectée à des profils utilisateur.
`p_min_length`	nombre	8	Non	Nombre minimal de caractères requis.
`p_max_length`	nombre	256	Non	Nombre maximal de caractères autorisés.
`p_min_letters`	nombre	1	Non	Nombre minimal de lettres requises.
`p_min_uppercase`	nombre	0	Non	Nombre minimal de lettres majuscules requises.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`p_min_lowercase`	nombre	0	Non	Nombre minimal de lettres minuscules requises.
`p_min_digits`	nombre	1	Non	Nombre minimal de chiffres requis.
`p_min_special`	nombre	0	Non	Nombre minimal de caractères spéciaux requis.
`p_min_different_chars`	nombre	3	Non	Nombre minimal de caractères différents requis entre l'ancien et le nouveau mot de passe.
`p_disallow_username`	booléen	true	Non	Définissez ce paramètre sur `true` pour interdire le nom d'utilisateur dans le mot de passe.
`p_disallow_reverse`	booléen	true	Non	Définissez ce paramètre sur `true` pour interdire le nom d'utilisateur inversé dans le mot de passe.
`p_disallow_db_name`	booléen	true	Non	Définissez ce paramètre sur `true` pour interdire le nom de la base de données ou du serveur dans le mot de passe.
`p_disallow_simple_strings`	booléen	true	Non	Définissez ce paramètre sur `true` pour interdire l'utilisation de chaînes simples comme mot de passe.
`p_disallow_whitespace`	booléen	false	Non	Définissez ce paramètre sur `true` pour interdire les espaces dans le mot de passe.
`p_disallow_at_sign`	booléen	false	Non	Définissez ce paramètre sur `true` pour interdire le caractère @ dans le mot de passe.

Vous pouvez créer plusieurs fonctions de vérification de mot de passe.

Il existe des restrictions sur le nom de votre fonction personnalisée. Votre fonction personnalisée ne peut pas avoir le même nom qu'un objet système existant. Ce nom ne peut pas comporter plus de 30 caractères. De plus, le nom doit inclure l'une des chaînes suivantes : `PASSWORD`, `VERIFY`, `COMPLEXITY`, `ENFORCE` ou `STRENGTH`.

L'exemple suivant crée une fonction nommée `CUSTOM_PASSWORD_FUNCTION`. La fonction exige qu'un mot de passe comporte au moins 12 caractères, 2 majuscules, 1 chiffre et 1 caractère spécial, et interdit le caractère @.

```
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;
/
```

Pour voir le texte de votre fonction de vérification, interrogez `DBA_SOURCE`. L'exemple suivant récupère le texte d'une fonction de mot de passe personnalisé nommée `CUSTOM_PASSWORD_FUNCTION`.

```
COL TEXT FORMAT a150

  SELECT TEXT
    FROM DBA_SOURCE
   WHERE OWNER = 'SYS'
     AND NAME = 'CUSTOM_PASSWORD_FUNCTION'
ORDER BY LINE;
```

Pour associer votre fonction de vérification à un profil utilisateur, utilisez `alter profile`. L'exemple suivant associe une fonction de vérification au profil utilisateur `DEFAULT`.

```
ALTER PROFILE DEFAULT LIMIT PASSWORD_VERIFY_FUNCTION CUSTOM_PASSWORD_FUNCTION;
```

Pour savoir quels profils utilisateur sont associés à quelles fonctions de vérification, interrogez `DBA_PROFILES`. L'exemple suivant obtient les profils qui sont associés à la fonction de vérification personnalisée nommée `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
```

L'exemple suivant récupère tous les profils et les fonctions de vérification de mot de passe associées.

```
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
```

Procédure create_passthrough_verify_fcn

La procédure `create_passthrough_verify_fcn` est prise en charge pour Oracle version 11.2.0.4.v11 et ultérieures, Oracle version 12.1.0.2.v7 et ultérieures, toutes les versions 12.2.0.1, toutes les versions 18.0.0.0 et toutes les versions 19.0.0.

Vous pouvez créer une fonction personnalisée pour vérifier les mots de passe en utilisant la procédure Amazon RDS `rdsadmin.rdsadmin_password_verify.create_passthrough_verify_fcn`. La procédure `create_passthrough_verify_fcn` possède les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`p_verify_function_name`	varchar2	—	Oui	Nom de la fonction de vérification personnalisée. Il s'agit d'une fonction de wrapper qui est automatiquement créée dans le schéma SYS et qui ne contient pas de logique de vérification. Elle est affectée à des profils utilisateur.
`p_target_owner`	varchar2	—	Oui	Propriétaire de schéma de la fonction de vérification personnalisée.
`p_target_function_name`	varchar2	—	Oui	Nom de la fonction personnalisée existante qui contient la logique de vérification. Votre fonction personnalisée doit renvoyer une valeur booléenne. La fonction doit renvoyer la valeur `true` si le mot de passe est valide, ou `false` s'il ne l'est pas.

L'exemple suivant crée une fonction de vérification de mot de passe qui utilise la logique provenant de la fonction nommée `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;
/
```

Pour associer la fonction de vérification à un profil utilisateur, utilisez `alter profile`. L'exemple suivant associe la fonction de vérification au profil utilisateur `DEFAULT`.

```
ALTER PROFILE DEFAULT LIMIT PASSWORD_VERIFY_FUNCTION CUSTOM_PASSWORD_FUNCTION;
```

Configuration d'un serveur DNS personnalisé

Amazon RDS prend en charge l'accès réseau sortant sur vos instances de bases de données exécutant Oracle. Pour plus d'informations sur l'utilisation de l'accès réseau sortant et les prérequis, consultez Utilisation de utl_http, utl_tcp et utl_smtp avec une instance de base de données Oracle (p. 957).

Amazon RDS Oracle permet la résolution DNS (Domain Name Service) à partir d'un serveur DNS personnalisé appartenant au client. Vous pouvez résoudre uniquement les deux noms de domaine complets à partir de votre instance de base de données Amazon RDS via votre serveur DNS personnalisé.

Une fois que votre serveur de nom DNS personnalisé est configuré, la propagation des modifications dans votre instance de base de données peut prendre jusqu'à 30 minutes. Une fois que les modifications sont propagées dans votre instance de base de données, l'ensemble du trafic réseau sortant nécessitant une recherche DNS interroge votre serveur DNS via le port 53.

Pour configurer un serveur DNS personnalisé pour votre instance de base de données Amazon RDS for Oracle, procédez comme suit :

- À partir du jeu d'options DHCP liées à votre VPC (cloud privé virtuel), définissez l'option `domain-name-servers` sur l'adresse IP de votre serveur de noms DNS. Pour de plus amples informations, veuillez consulter Jeux d'options DHCP.

  > **Note**
  >
  > L'option `domain-name-servers` autorise jusqu'à quatre valeurs, mais votre instance de base de données Amazon RDS utilise uniquement la première valeur.

- Assurez-vous que votre serveur DNS peut résoudre toutes les requêtes de recherche, notamment les noms DNS publics, les noms DNS privés Amazon EC2 et les noms DNS spécifiés par le client. Si le trafic réseau sortant contient une recherche DNS que votre serveur DNS ne peut pas gérer, votre serveur DNS doit avoir des fournisseurs DNS en amont appropriés, configurés.
- Configurez votre serveur DNS pour produire des réponses UDP (User Datagram Protocol) de 512 octets ou moins.
- Configurez votre serveur DNS pour produire des réponses TCP (Transmission Control Protocol) de 1024 octets ou moins.
- Configurez votre serveur DNS pour permettre le trafic entrant à partir de vos instances de bases de données Amazon RDS sur le port 53. Si votre serveur DNS est dans un Amazon VPC, le VPC doit avoir un groupe de sécurité qui contient des règles entrantes permettant le trafic UDP et TCP sur le port 53. Si votre serveur DNS n'est pas dans un Amazon VPC, il doit avoir une liste blanche des pare-feux appropriés pour permettre le trafic UDP et TCP sur le port 53.

  Pour de plus amples informations, veuillez consulter Groupes de sécurité pour votre VPC et Ajout et suppression de règles.
- Configurez le VPC de votre instance de base de données Amazon RDS pour permettre le trafic sortant via le port 53. Votre serveur VPC doit avoir un groupe de sécurité qui contient des règles sortantes permettant le trafic UDP et TCP sur le port 53.

  Pour de plus amples informations, veuillez consulter Groupes de sécurité pour votre VPC et Ajout et suppression de règles.
- Le chemin d'acheminement entre l'instance de base de données Amazon RDS et le serveur DNS doit être configuré correctement pour permettre un trafic DNS.
  - Si l'instance de base de données Amazon RDS et le serveur DNS ne sont pas dans le même VPC, une connexion d'appairage doit être configurée entre les deux. Pour de plus amples informations, veuillez consulter Qu'est-ce que l'appairage de VPC ?

Tâches de base de données DBA courantes pour les instances de base de données Oracle

Vous trouverez ci-dessous des informations sur la façon d'effectuer certaines tâches DBA courantes liées aux bases de données sur vos instances de base de données Amazon RDS exécutant Oracle. Pour offrir une expérience de service géré, Amazon RDS ne fournit pas l'accès shell aux instances de base de données. Amazon RDS limite également l'accès à certaines tables et procédures système qui requièrent des privilèges avancés.

Rubriques

- Modification du nom global d'une base de données (p. 1115)
- Création et dimensionnement des espaces de table (p. 1116)
- Définition de l'espace de table par défaut (p. 1116)
- Définition de l'espace de table temporaire par défaut (p. 1117)
- Création d'un point de contrôle de base de données (p. 1117)
- Définition d'une récupération distribuée (p. 1117)
- Définition du fuseau horaire de la base de données (p. 1117)
- Utilisation de tables externes Oracle (p. 1118)
- Génération de rapports de performance avec AWR (Automatic Workload Repository) (p. 1119)
- Réglage des liens de base de données pour une utilisation avec les instances de base de données dans un VPC (p. 1123)
- Définition de l'édition par défaut d'une instance de base de données (p. 1123)
- Activation de l'audit pour la table SYS.AUD$ (p. 1124)
- Désactivation de l'audit pour la table SYS.AUD$ (p. 1124)
- Nettoyage de builds d'index en ligne interrompues (p. 1125)
- Ignorer les blocs corrompus (p. 1126)
- Redimensionnement de l'espace de table temporaire dans un réplica en lecture (p. 1128)
- Purge de la corbeille (p. 1129)

Modification du nom global d'une base de données

Pour modifier le nom global d'une base de données, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.rename_global_name`. La procédure `rename_global_name` comporte les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`p_new_global_name`	varchar2	—	Oui	Nouveau nom global de la base de données.

La base de données doit être ouverte pour que la modification du nom puisse se produire. Pour plus d'informations sur la modification du nom global d'une base de données, consultez ALTER DATABASE (MODIFIER BASE DE DONNÉES) dans la documentation Oracle.

L'exemple suivant remplace le nom global de la base de données par `new_global_name`.

```
exec rdsadmin.rdsadmin_util.rename_global_name(p_new_global_name => 'new_global_name');
```

Création et dimensionnement des espaces de table

Amazon RDS ne prend en charge qu'Oracle Managed Files (OMF) pour les fichiers de données, les fichiers journaux et les fichiers de contrôle. Lorsque vous créez des fichiers de données et des fichiers journaux, vous ne pouvez pas spécifier les noms de fichiers physiques.

Par défaut, les espaces de table sont créés avec l'option auto extend activée et aucune restriction de taille maximum. A cause de ces paramètres par défaut, les espaces de table peuvent se développer pour utiliser l'ensemble du stockage alloué. Nous vous recommandons de spécifier une taille maximum appropriée sur les espaces de table permanents et temporaires, et de surveiller attentivement l'utilisation de l'espace.

L'exemple suivant crée un espace de table nommé `users2` avec une taille comprise entre 1 et 10 gigaoctets maximum :

```
CREATE TABLESPACE users2 DATAFILE SIZE 1G AUTOEXTEND ON MAXSIZE 10G;
```

L'exemple suivant crée un espace de table temporaire nommé `temp01` :

```
CREATE TEMPORARY TABLESPACE temp01;
```

Nous vous recommandons de ne pas utiliser d'espaces de table smallfile, car vous ne pouvez pas redimensionner les espaces de table smallfile avec Amazon RDS for Oracle. Toutefois, vous pouvez ajouter un fichier de données à un espace de table smallfile.

Vous pouvez redimensionner un espace de table bigfile en utilisant `ALTER TABLESPACE`. Vous pouvez spécifier la taille en kilo-octets (Ko), mégaoctets (Mo), gigaoctets (Go) ou téraoctets (To).

L'exemple suivant redimensionne un espace de table bigfile nommé `users2` pour qu'il fasse 200 Mo.

```
ALTER TABLESPACE users2 RESIZE 200M;
```

L'exemple suivant ajoute un fichier de données à un espace de table smallfile nommé **`users2`**.

```
ALTER TABLESPACE users2 ADD DATAFILE SIZE 100000M AUTOEXTEND ON NEXT 250m
 MAXSIZE UNLIMITED;
```

Définition de l'espace de table par défaut

Pour définir l'espace de table par défaut, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.alter_default_tablespace`. La procédure `alter_default_tablespace` comporte les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`tablespace_name`	varchar	—	Oui	Nom de l'espace de table par défaut.

L'exemple suivant définit le tablespace par défaut sur *`users2`* :

```
exec rdsadmin.rdsadmin_util.alter_default_tablespace(tablespace_name => 'users2');
```

Définition de l'espace de table temporaire par défaut

Pour définir l'espace de table temporaire par défaut, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.alter_default_temp_tablespace`. La procédure `alter_default_temp_tablespace` comporte les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`tablespace_name`	varchar	—	Oui	Nom de l'espace de table temporaire par défaut.

L'exemple suivant définit l'espace de table temporaire par défaut sur *`temp01`*.

```
exec rdsadmin.rdsadmin_util.alter_default_temp_tablespace(tablespace_name => 'temp01');
```

Création d'un point de contrôle de base de données

Pour créer un point de contrôle sur la base de données, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.checkpoint`. La procédure `checkpoint` ne comporte aucun paramètre.

L'exemple suivant crée un point de contrôle sur la base de données.

```
exec rdsadmin.rdsadmin_util.checkpoint;
```

Définition d'une récupération distribuée

Pour définir une récupération distribuée, utilisez les procédures Amazon RDS `rdsadmin.rdsadmin_util.enable_distr_recovery` et `disable_distr_recovery`. Ces procédures ne comportent aucun paramètre.

L'exemple suivant active la récupération distribuée.

```
exec rdsadmin.rdsadmin_util.enable_distr_recovery;
```

L'exemple suivant désactive la récupération distribuée.

```
exec rdsadmin.rdsadmin_util.disable_distr_recovery;
```

Définition du fuseau horaire de la base de données

Vous pouvez définir le fuseau horaire de votre base de données Oracle Amazon RDS des manières suivantes :

- L'option `Timezone`

  L'option `Timezone` modifie le fuseau horaire au niveau de l'hôte et impacte toutes les valeurs et colonnes date, telles que `SYSDATE`. Pour de plus amples informations, veuillez consulter Fuseau horaire Oracle (p. 1088).
- La procédure Amazon RDS `rdsadmin.rdsadmin_util.alter_db_time_zone`

  La procédure `alter_db_time_zone` modifie le fuseau horaire uniquement pour certains types de données, et ne change pas `SYSDATE`. Il existe des restrictions supplémentaires sur la définition du fuseau horaire, répertoriées dans la documentation Oracle.

> **Note**
>
> Vous pouvez également définir le fuseau horaire par défaut pour Oracle Scheduler. Pour plus d'informations, consultez Définition du fuseau horaire pour les tâches d'Oracle Scheduler (p. 1155).

La procédure `alter_db_time_zone` possède les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`p_new_tz`	varchar2	—	Oui	Nouveau fuseau horaire correspondant à une région nommée ou à un décalage absolu par rapport à l'heure UTC (Coordinated Universal Time). Les décalages valides s'étendent de -12h00 à +14h00.

L'exemple suivant remplace le fuseau horaire par l'heure UTC plus trois heures.

```
exec rdsadmin.rdsadmin_util.alter_db_time_zone(p_new_tz => '+3:00');
```

L'exemple suivant remplace le fuseau horaire par celui de la région Africa/Algiers.

```
exec rdsadmin.rdsadmin_util.alter_db_time_zone(p_new_tz => 'Africa/Algiers');
```

Après avoir modifié le fuseau horaire grâce à la procédure `alter_db_time_zone`, redémarrez l'instance de base de données pour que la modification prenne effet. Pour plus d'informations, consultez Redémarrage d'une instance de base de données (p. 272). Pour de plus amples informations sur la mise à niveau des fuseaux horaires, veuillez consulter Considérations relatives au fuseau horaire (p. 980)

Utilisation de tables externes Oracle

Les tables externes Oracle sont des tables contenant des données ne figurant pas dans la base de données. À la place, les données se trouvent dans des fichiers externes auxquels la base de données peut accéder. L'utilisation de tables externes vous permet d'accéder aux données sans les charger dans la base de données. Pour de plus amples informations sur les tables externes, veuillez consulter Managing External Tables dans la documentation Oracle.

Avec Amazon RDS, vous pouvez stocker des fichiers de table externe dans des objets de répertoire. Vous pouvez créer un objet de répertoire ou vous pouvez en utiliser un qui est prédéfini dans la base de données Oracle, comme le répertoire DATA_PUMP_DIR. Pour plus d'informations sur la création d'objets de répertoire, consultez Création et suppression de répertoires dans l'espace de stockage de données principal (p. 1164). Vous pouvez interroger la vue ALL_DIRECTORIES pour répertorier tous les objets de répertoire de votre instance de base de données Amazon RDS Oracle.

> **Note**
>
> Les objets de répertoire pointent vers le même espace de stockage de données (volume Amazon EBS) utilisé par votre instance. L'espace utilisé—ainsi que les fichiers de données, journaux redo, d'audit, de suivi et autres—sont déduits du stockage alloué.

Vous pouvez déplacer un fichier de données externes d'une base de données Oracle à une autre à l'aide du package DBMS_FILE_TRANSFER ou du package UTL_FILE. Le fichier de données externes est

déplacé d'un répertoire de la base de données source vers le répertoire spécifié sur la base de données de destination. Pour plus d'informations sur l'utilisation de DBMS_FILE_TRANSFER, consultez Importation à l'aide d'Oracle Data Pump (p. 991).

Après avoir déplacé le fichier de données externe, celui-ci peut vous permettre de créer une table externe. L'exemple suivant crée une table externe qui utilise le fichier `emp_xt_file1.txt` dans le répertoire USER_DIR1.

```
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;
```

Supposons que vous souhaitiez déplacer des données se trouvant dans une instance de base de données Amazon RDS Oracle vers un fichier de données externe. Dans ce as, vous pouvez remplir le fichier de données externe en créant une table externe et en sélectionnant les données de la table de la base de données. Par exemple, l'instruction SQL suivante crée la table externe `orders_xt` en interrogeant la table `orders` de la base de données.

```
CREATE TABLE orders_xt
  ORGANIZATION EXTERNAL
   (
     TYPE ORACLE_DATAPUMP
     DEFAULT DIRECTORY DATA_PUMP_DIR
     LOCATION ('orders_xt.dmp')
   )
   AS SELECT * FROM orders;
```

Dans cet exemple, les données sont renseignées dans le fichier `orders_xt.dmp` du répertoire DATA_PUMP_DIR.

Génération de rapports de performance avec AWR (Automatic Workload Repository)

Pour collecter des données de performance et générer des rapports, Oracle recommande AWR (Automatic Workload Repository). AWR nécessite Oracle Database Enterprise Edition et une licence pour les packs Diagnostics et Tuning. Pour activer AWR, définissez le paramètre d'initialisation `CONTROL_MANAGEMENT_PACK_ACCESS` sur `DIAGNOSTIC` ou `DIAGNOSTIC+TUNING`.

Utilisation des rapports AWR dans RDS

Pour générer des rapports AWR, vous pouvez exécuter des scripts tels que `awrrpt.sql`. Ces scripts sont installés sur le serveur hôte de base de données. Dans Amazon RDS, vous n'avez pas d'accès direct à

l'hôte. Toutefois, vous pouvez obtenir des copies de scripts SQL à partir d'une autre installation d'Oracle Database.

Vous pouvez également utiliser AWR en exécutant des procédures dans le package PL/SQL `SYS.DBMS_WORKLOAD_REPOSITORY`. Vous pouvez utiliser ce package pour gérer les références et les instantanés, mais aussi pour afficher les rapports ASH et AWR. Par exemple, pour générer un rapport AWR au format texte, exécutez la procédure `DBMS_WORKLOAD_REPOSITORY.AWR_REPORT_TEXT`. Toutefois, vous ne pouvez pas accéder à ces rapports AWR à partir d'AWS Management Console.

Lorsque vous travaillez avec AWR, nous vous recommandons d'utiliser les procédures `rdsadmin.rdsadmin_diagnostic_util`. Vous pouvez utiliser ces procédures pour générer les éléments suivants :

- Rapports AWR
- Rapports ASH (Active Session History)
- Rapports ADDM (Automatic Database Diagnostic Monitor)
- Fichiers de vidage Oracle Data Pump Export des données AWR

Les procédures `rdsadmin_diagnostic_util` enregistrent les rapports dans le système de fichiers de l'instance de base de données. Vous pouvez accéder à ces rapports à partir de la console. Vous pouvez également accéder aux rapports à l'aide des procédures `rdsadmin.rds_file_util`. Vous pouvez accéder aux rapports copiés dans Amazon S3 à l'aide de l'option S3 Integration. Pour de plus amples informations, veuillez consulter Lecture de fichiers dans un répertoire d'instance de base de données (p. 1166) et Intégration Amazon S3 (p. 1014).

Vous pouvez utiliser les procédures `rdsadmin_diagnostic_util` pour les versions suivantes du moteur de base de données Amazon RDS for Oracle :

- 11.2.0.4.v24 ou versions 11.2 ultérieures
- 12.1.0.2.v20 ou versions 12.1 ultérieures
- 12.2.0.1.ru-2020-04.rur-2020-04.r1 ou versions 12.2 ultérieures
- 18.0.0.0.ru-2020-04.rur-2020-04.r1 ou versions 18c ultérieures
- 19.0.0.0.ru-2020-04.rur-2020-04.r1 ou versions 19c ultérieures

Paramètres communs pour le package d'utilitaires de diagnostic

Vous utilisez généralement les paramètres suivants lors de la gestion d'AWR et d'ADDM avec le package rdsadmin_diagnostic_util.

Paramètre	Type de données	Par défaut	Obligat	Description
`begin_snap_id`	`NUMBER`	—	Oui	ID de l'instantané de début.
`end_snap_id`	`NUMBER`	—	Oui	ID de l'instantané de fin.
`dump_directory`	`VARCHAR2`	`BDUMP`	Non	Répertoire dans lequel le rapport ou le fichier d'exportation sera écrit. Si vous spécifiez un répertoire autre que le répertoire par défaut, l'utilisateur qui exécute les procédures `rdsadmin_diagnostic_util` doit disposer des autorisations en écriture pour le répertoire.
`report_type`	`VARCHAR2`	`HTML`	Non	Format du rapport. Les valeurs valides sont `TEXT` et `HTML`.

Paramètre	Type de données	Par défaut	Obligat	Description
`dbid`	`NUMBER`	—	Non	Identifiant de base de données valide (DBID) affiché dans la vue `DBA_HIST_DATABASE_INSTANCE` pour Oracle. Si ce paramètre n'est pas spécifié, RDS utilise le DBID actuel, qui est affiché dans la vue `V$DATABASE.DBID`.

Vous utilisez généralement les paramètres suivants lors de la gestion d'ASH avec le package rdsadmin_diagnostic_util.

Paramètre	Type de données	Par défaut	Obligato	Description
`begin_time`	`DATE`	—	Oui	Heure de début de l'analyse ASH.
`end_time`	`DATE`	—	Oui	Heure de fin de l'analyse ASH.
`slot_width`	`NUMBER`	`0`	Non	Durée des emplacements (en secondes) utilisés dans la section « Top Activity (Activité principale) » du rapport ASH. Si ce paramètre n'est pas spécifié, l'intervalle de temps entre `begin_time` et `end_time` n'utilise pas plus de 10 emplacements.
`sid`	`NUMBER`	Null	Non	ID de session.
`sql_id`	`VARCHAR2`	Null	Non	ID SQL.
`wait_class`	`VARCHAR2`	Null	Non	Nom de la classe d'attente.
`service_hash`	`NUMBER`	Null	Non	Hachage du nom de service.
`module_name`	`VARCHAR2`	Null	Non	Nom du module.
`action_name`	`VARCHAR2`	Null	Non	Nom de l'action.
`client_id`	`VARCHAR2`	Null	Non	ID spécifique à l'application de la session de base de données.
`plsql_entry`	`VARCHAR2`	Null	Non	Point d'entrée PL/SQL.

Génération d'un rapport AWR

Pour générer un rapport AWR, utilisez la procédure `rdsadmin.rdsadmin_diagnostic_util.awr_report`.

L'exemple suivant génère un rapport AWR pour la plage d'instantanés comprise entre 101 et 106. Le fichier texte en sortie est nommé `awrrpt_101_106.txt`. Vous pouvez accéder à ce rapport à partir d'AWS Management Console.

```
exec rdsadmin.rdsadmin_diagnostic_util.awr_report(101,106,'TEXT');
```

L'exemple suivant génère un rapport HTML pour la plage d'instantanés comprise entre 63 et 65. Le fichier HTML en sortie est nommé `awrrpt_63_65.html`. La procédure écrit le rapport dans un répertoire de base de données autre que le répertoire par défaut et nommé `AWR_RPT_DUMP`.

```
exec rdsadmin.rdsadmin_diagnostic_util.awr_report(63,65,'HTML','AWR_RPT_DUMP');
```

Extraction de données AWR dans un fichier de vidage

Pour extraire des données AWR dans un fichier de vidage, utilisez la procédure `rdsadmin.rdsadmin_diagnostic_util.awr_extract`.

L'exemple suivant extrait la plage d'instantanés comprise entre 101 et 106. Le fichier de vidage en sortie est nommé `awrextract_101_106.dmp`. Vous pouvez accéder à ce fichier via la console.

```
exec rdsadmin.rdsadmin_diagnostic_util.awr_extract(101,106);
```

L'exemple suivant extrait la plage d'instantanés comprise entre 63 et 65. Le fichier de vidage en sortie est nommé `awrextract_63_65.dmp`. Le fichier est stocké dans un répertoire de base de données autre que le répertoire par défaut et nommé `AWR_RPT_DUMP`.

```
exec rdsadmin.rdsadmin_diagnostic_util.awr_extract(63,65,'AWR_RPT_DUMP');
```

Génération d'un rapport ADDM

Pour générer un rapport ADDM, utilisez la procédure `rdsadmin.rdsadmin_diagnostic_util.addm_report`.

L'exemple suivant génère un rapport HTML pour la plage d'instantanés comprise entre 101 et 106. Le fichier texte en sortie est nommé `addmrpt_101_106.txt`. Vous pouvez accéder au rapport via la console.

```
exec rdsadmin.rdsadmin_diagnostic_util.addm_report(101,106);
```

L'exemple suivant génère un rapport ADDM pour la plage d'instantanés comprise entre 63 et 65. Le fichier texte en sortie est nommé `addmrpt_63_65.txt`. Le fichier est stocké dans un répertoire de base de données autre que le répertoire par défaut et nommé `ADDM_RPT_DUMP`.

```
exec rdsadmin.rdsadmin_diagnostic_util.addm_report(63,65,'ADDM_RPT_DUMP');
```

Génération d'un rapport ASH

Pour générer un rapport ASH, utilisez la procédure `rdsadmin.rdsadmin_diagnostic_util.ash_report`.

L'exemple suivant génère un rapport ASH qui inclut les données des 14 dernières minutes. Le nom du fichier en sortie utilise le format `ashrpt`*`begin_timeend_time`*`.txt`, où *`begin_time`* et *`end_time`* utilisent le format `YYYYMMDDHH24MISS`. Vous pouvez accéder au fichier via la console.

```
BEGIN
    rdsadmin.rdsadmin_diagnostic_util.ash_report(
        begin_time     =>     SYSDATE-14/1440,
        end_time       =>     SYSDATE,
        report_type    =>     'TEXT');
END;
/
```

L'exemple suivant génère un rapport ASH qui inclut les données depuis le 18 novembre 2019 à 18h07 jusqu'au 18 novembre 2019 à 18h15. Le nom du rapport HTML en sortie est `ashrpt_20190918180700_20190918181500.html`. Le rapport est stocké dans un répertoire de base de données autre que le répertoire par défaut et nommé `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;
/
```

Accès aux rapports AWR à partir de la console ou de l'interface de ligne de commande

Pour accéder aux rapports AWR ou exporter des fichiers de vidage, vous pouvez utiliser AWS Management Console ou l'AWS CLI. Pour de plus amples informations, veuillez consulter Téléchargement d'un fichier journal de base de données (p. 491).

Réglage des liens de base de données pour une utilisation avec les instances de base de données dans un VPC

Pour utiliser les liens de base de données Oracle avec des instances de base de données Amazon RDS au sein du même VPC (cloud privé virtuel) ou de VPC appairés, un itinéraire valide doit exister entre les deux instances de base de données. Vérifiez l'itinéraire valide entre les instances de bases de données à l'aide de vos tables de routage VPC et la liste de contrôle d'accès (ACL) réseau.

Le groupe de sécurité de chaque instance de base de données doit autoriser le trafic entrant dans l'autre instance de base de données et le trafic sortant de cette instance. Les règles entrantes et sortantes peuvent faire référence à des groupes de sécurité à partir du même VPC ou d'un VPC appairé. Pour de plus amples informations, veuillez consulter Mise à jour de vos groupes de sécurité pour référencer des groupes de sécurité du VPC appairé.

Si vous avez configuré un serveur DNS personnalisé grâce aux jeux d'options DHCP de votre VPC, votre serveur DNS personnalisé doit pouvoir résoudre le nom de la cible du lien de la base de données. Pour plus d'informations, consultez Configuration d'un serveur DNS personnalisé (p. 1114).

Pour plus d'informations sur l'utilisation des liens de base de données avec Oracle Data Pump, consultez Importation à l'aide d'Oracle Data Pump (p. 991).

Définition de l'édition par défaut d'une instance de base de données

Vous pouvez redéfinir les objets de base de données dans un environnement privé appelé une édition. Vous pouvez utiliser la redéfinition basée sur l'édition pour mettre à niveau les objets de base de données d'une application avec un temps d'arrêt minimal.

Vous pouvez définir l'édition par défaut d'une instance de bases de données Amazon RDS Oracle à l'aide de la procédure Amazon RDS `rdsadmin.rdsadmin_util.alter_default_edition`.

L'exemple suivant définit l'édition par défaut de l'instance de bases de données Amazon RDS Oracle sur `RELEASE_V1`.

```
exec rdsadmin.rdsadmin_util.alter_default_edition('RELEASE_V1');
```

L'exemple suivant redéfinit l'édition par défaut de l'instance de base de données Amazon RDS Oracle sur la valeur par défaut d'Oracle.

```
exec rdsadmin.rdsadmin_util.alter_default_edition('ORA$BASE');
```

Pour de plus amples informations concernant la redéfinition basée sur l'édition d'Oracle, veuillez consulter About Editions and Edition-Based Redefinition dans la documentation Oracle.

Activation de l'audit pour la table SYS.AUD$

Pour activer l'audit sur la table de suivi d'audit de base de données `SYS.AUD$`, utilisez la procédure Amazon RDS`rdsadmin.rdsadmin_master_util.audit_all_sys_aud_table`. La seule propriété d'audit prise en charge est `ALL`. Vous ne pouvez pas auditer ou ne pas auditer des instructions ou des opérations individuelles.

L'activation de l'audit est prise en charge pour les instances de base de données Oracle qui exécutent les versions suivantes :

- 11.2.0.4.v18 et versions 11.2 ultérieures
- 12.1.0.2.v14 et versions 12.1 ultérieures
- Toutes les versions 12.2.0.1
- Toutes les versions 18.0.0.0
- Toutes les versions 19.0.0.0

La procédure `audit_all_sys_aud_table` comporte les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`p_by_access`	booléen	true	Non	Définissez ce paramètre sur `true` pour auditer `BY ACCESS`. Définissez ce paramètre sur `false` pour auditer `BY SESSION`.

La requête suivante retourne la configuration d'audit actuelle de `SYS.AUD$` pour une base de données.

```
SELECT * FROM DBA_OBJ_AUDIT_OPTS WHERE OWNER='SYS' AND OBJECT_NAME='AUD$';
```

Les commandes suivantes activent l'audit de `ALL` sur `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);
```

La commande suivante active l'audit de `ALL` sur `SYS.AUD$ BY SESSION`.

```
exec rdsadmin.rdsadmin_master_util.audit_all_sys_aud_table(p_by_access => false);
```

Pour de plus amples informations, veuillez consulter AUDIT (Traditional Auditing) dans la documentation Oracle.

Désactivation de l'audit pour la table SYS.AUD$

Pour désactiver l'audit sur la table de suivi d'audit de base de données `SYS.AUD$`, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_master_util.noaudit_all_sys_aud_table`. Cette procédure ne prend aucun paramètre.

La requête suivante retourne la configuration d'audit actuelle pour `SYS.AUD$`, pour une base de données :

```
SELECT * FROM DBA_OBJ_AUDIT_OPTS WHERE OWNER='SYS' AND OBJECT_NAME='AUD$';
```

La commande suivante désactive l'audit de `ALL` sur `SYS.AUD$`.

```
exec rdsadmin.rdsadmin_master_util.noaudit_all_sys_aud_table;
```

Pour de plus amples informations, veuillez consulter NOAUDIT (Traditional Auditing) dans la documentation Oracle.

Nettoyage de builds d'index en ligne interrompues

Pour nettoyer des builds d'index en ligne qui ont échoué, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_dbms_repair.online_index_clean`.

La procédure `online_index_clean` possède les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`object_id`	binary_integer	`ALL_INDEX_ID`	Non	ID d'objet de l'index. En général, vous pouvez utiliser l'ID d'objet du texte d'erreur ORA-08104.
`wait_for_lock`	binary_integer	`rdsadmin.rdsadmin_dbms_repair.lock_wait`	Non	Spécifiez `rdsadmin.rdsadmin_dbms_repair.lo` la valeur par défaut pour tenter de verrouiller l'objet sous-jacent et réessayer jusqu'à ce qu'une limite interne soit atteinte si le verrouillage échoue. Spécifiez `rdsadmin.rdsadmin_dbms_repair.lo` pour essayer d'obtenir un verrouillage sur l'objet sous-jacent, sans réessayer si le verouillage échoue.

L'exemple suivant nettoie une build d'index en ligne ayant échoué.

```
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;
 /
```

Pour de plus amples informations, veuillez consulter ONLINE_INDEX_CLEAN Function dans la documentation d'Oracle.

Ignorer les blocs corrompus

Pour ignorer les blocs corrompus pendant les analyses d'index et de table, utilisez le package `rdsadmin.rdsadmin_dbms_repair`.

Les procédures suivantes encapsulent la fonctionnalité de la procédure `sys.dbms_repair.admin_table` et ne prennent aucun paramètre :

- `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`

Les procédures suivantes prennent les mêmes paramètres que leurs homologues du package `DBMS_REPAIR` pour les bases de données Oracle :

- `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`

Pour de plus amples informations sur la gestion de la corruption de base de données, veuillez consulter DBMS_REPAIR dans la documentation Oracle.

Example Réponse aux blocs corrompus

Cet exemple présente le flux de travail de base pour répondre aux blocs corrompus. Vos étapes dépendront de l'emplacement et de la nature de votre corruption de bloc.

> **Important**
>
> Avant de tenter de réparer les blocs corrompus, consultez attentivement la documentation DBMS_REPAIR.

Pour ignorer les blocs corrompus pendant les analyses d'index et de table

1. Exécutez les procédures suivantes pour créer des tables de réparation si elles n'existent pas déjà.

```
exec rdsadmin.rdsadmin_dbms_repair.create_repair_table;
exec rdsadmin.rdsadmin_dbms_repair.create_orphan_keys_table;
```

2. Exécutez les procédures suivantes pour vérifier s'il existe des enregistrements et les purger si nécessaire.

```
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. Exécutez la procédure suivante pour rechercher les blocs corrompus.

```
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. Utilisez la procédure `skip_corrupt_blocks` pour activer ou désactiver l'ignorance de corruption pour les tables affectées. Selon la situation, vous devrez peut-être également extraire des données dans une nouvelle table, puis supprimer la table contenant le bloc corrompu.

   Exécutez la procédure suivante pour permettre d'ignorer la corruption pour les tables affectées.

```
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';
```

   Exécutez la procédure suivante pour ne pas ignorer la corruption.

```
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. Une fois tous les travaux de réparation terminés, exécutez les procédures suivantes pour supprimer les tables de réparation.

```
exec rdsadmin.rdsadmin_dbms_repair.drop_repair_table;
```

```
exec rdsadmin.rdsadmin_dbms_repair.drop_orphan_keys_table;
```

Redimensionnement de l'espace de table temporaire dans un réplica en lecture

Par défaut, les espaces de table Oracle sont créés avec l'option « auto extend » activée et sans aucune restriction de taille maximum. À cause de ces paramètres par défaut, les espaces de table peuvent parfois trop se développer. Nous vous recommandons de spécifier une taille maximum appropriée sur les espaces de table permanents et temporaires, et de surveiller attentivement l'utilisation de l'espace.

Pour redimensionner l'espace temporaire dans un réplica en lecture pour une instance de base de données Oracle, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.resize_temp_tablespace` ou `rdsadmin.rdsadmin_util.resize_tempfile`.

La procédure `resize_temp_tablespace` possède les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`temp_tbs`	varchar2	—	Oui	Nom de l'espace de table temporaire à redimensionner.
`size`	varchar2	—	Oui	Vous pouvez spécifier la taille en octets (par défaut), kilooctets (Ko), mégaoctets (Mo) ou gigaoctets (Go).

La procédure `resize_tempfile` possède les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`file_id`	binary_integer	—	Oui	Identifiant de fichier de l'espace de table temporaire à redimensionner.
`size`	varchar2	—	Oui	Vous pouvez spécifier la taille en octets (par défaut), kilooctets (Ko), mégaoctets (Mo) ou gigaoctets (Go).

Les exemples suivants redimensionnent un espace de table temporaire nommé `TEMP` pour qu'il fasse 4 Go sur un réplica en lecture.

```
exec rdsadmin.rdsadmin_util.resize_temp_tablespace('TEMP','4G');
```

```
exec rdsadmin.rdsadmin_util.resize_temp_tablespace('TEMP','4096000000');
```

L'exemple suivant redimensionne un espace de table temporaire basé sur le fichier temporaire avec l'identifiant de fichier `1` pour qu'il fasse 2 Mo sur un réplica en lecture.

```
exec rdsadmin.rdsadmin_util.resize_tempfile(1,'2M');
```

Pour de plus amples informations sur les réplicas en lecture pour les instances de base de données Oracle, veuillez consulter Utilisation des réplicas Oracle pour Amazon RDS (p. 1003).

Purge de la corbeille

Lorsque vous supprimez une table, votre base de données Oracle ne supprime pas immédiatement son espace de stockage. La base de données renomme la table et la place, ainsi que les objets associés, dans une corbeille. La purge de la corbeille supprime ces éléments et libère leur espace de stockage.

Pour purger l'intégralité de la corbeille, suivez la procédure Amazon RDS `rdsadmin.rdsadmin_util.purge_dba_recyclebin`. Toutefois, cette procédure ne peut pas purger la corbeille des objets `SYS` et `RDSADMIN`. Si vous devez purger ces objets, contactez AWS Support.

L'exemple suivant purge l'ensemble de la corbeille.

```
exec rdsadmin.rdsadmin_util.purge_dba_recyclebin;
```

Tâches de journal DBA courantes pour les instances de base de données Oracle

Vous trouverez ci-dessous des informations sur la façon d'effectuer certaines tâches DBA courantes liées à la journalisation sur vos instances de base de données Amazon RDS exécutant Oracle. Pour offrir une expérience de service géré, Amazon RDS ne fournit pas l'accès shell aux instances de base de données et limite l'accès à certaines tables et procédures système qui requièrent des privilèges avancés.

Pour plus d'informations, consultez Fichiers journaux de base de données Oracle (p. 515).

Rubriques

- Configuration du mode FORCE LOGGING (p. 1129)
- Configuration d'une journalisation supplémentaire (p. 1130)
- Changement de fichiers journaux en ligne (p. 1131)
- Ajout de journaux redo en ligne (p. 1131)
- Suppression de journaux redo en ligne (p. 1132)
- Redimensionnement de journaux redo en ligne (p. 1132)
- Conservation des journaux redo archivés (p. 1134)
- Accès aux journaux de transactions (p. 1135)

Configuration du mode FORCE LOGGING

En mode FORCE LOGGING, Oracle enregistre toutes les modifications apportées à la base de données, à l'exception de celles apportées aux espaces de table temporaires et aux segments temporaires (`NOLOGGING` des clauses sont ignorées). Pour de plus amples informations, veuillez consulter Specifying FORCE LOGGING Mode dans la documentation Oracle.

Pour définir le mode FORCE LOGGING, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.force_logging`. La procédure `force_logging` comporte les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Oui	Description
`p_enable`	booléen	true	Non	Définissez ce paramètre sur `true` pour mettre la base de données en mode FORCE LOGGING ou sur `false` pour sortir la base de données de ce mode.

L'exemple suivant met la base de données en mode FORCE LOGGING.

```
exec rdsadmin.rdsadmin_util.force_logging(p_enable => true);
```

Configuration d'une journalisation supplémentaire

Si vous activez la journalisation supplémentaire, LogMiner dispose des informations nécessaires pour prendre en charge les lignes chaînées et les tables en cluster. Pour de plus amples informations, veuillez consulter journalisation supplémentaire dans la documentation Oracle.

Oracle Database n'active pas la journalisation supplémentaire par défaut. Pour activer et désactiver la journalisation supplémentaire, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.alter_supplemental_logging`. Pour plus d'informations sur la façon dont Amazon RDS gère la conservation des journaux redo archivés pour les instances de base de données Oracle, consultez Conservation des journaux redo archivés (p. 1134).

La procédure `alter_supplemental_logging` possède les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`p_action`	varchar2	—	Oui	`'ADD'` pour ajouter la journalisation supplémentaire, `'DROP'` pour la supprimer.
`p_type`	varchar2	null	Non	Type de journalisation supplémentaire. Les valeurs valides sont `'ALL'`, `'FOREIGN KEY'`, `'PRIMARY KEY'`, `'UNIQUE'` et `PROCEDURAL`.

L'exemple suivant active la journalisation supplémentaire.

```
begin
    rdsadmin.rdsadmin_util.alter_supplemental_logging(
        p_action => 'ADD');
end;
/
```

L'exemple suivant active la journalisation supplémentaire pour toutes les colonnes de taille maximale et de longueur fixe.

```
begin
    rdsadmin.rdsadmin_util.alter_supplemental_logging(
        p_action => 'ADD',
        p_type   => 'ALL');
end;
/
```

L'exemple suivant active la journalisation supplémentaire pour les colonnes de clés primaires.

```
begin
    rdsadmin.rdsadmin_util.alter_supplemental_logging(
        p_action => 'ADD',
        p_type   => 'PRIMARY KEY');
end;
/
```

Changement de fichiers journaux en ligne

Pour changer des fichiers journaux, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.switch_logfile`. La procédure `switch_logfile` ne comporte aucun paramètre.

L'exemple suivant change des fichiers journaux.

```
exec rdsadmin.rdsadmin_util.switch_logfile;
```

Ajout de journaux redo en ligne

Une instance de base de données Amazon RDS exécutant Oracle démarre avec quatre journaux redo en ligne de 128 Mo chacun. Pour ajouter des journaux redo supplémentaires, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.add_logfile`.

La procédure `add_logfile` comporte les paramètres suivants.

> **Note**
>
> Les paramètres s'excluent mutuellement.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`bytes`	positives	null	Non	Taille du fichier journal en octets.
`p_size`	varchar2	—	Oui	Taille du fichier journal. Vous pouvez spécifier la taille en kilo-octets (Ko), mégaoctets (Mo) ou gigaoctets (Go).

La commande suivante ajoute un fichier journal de 100 Mo.

```
exec rdsadmin.rdsadmin_util.add_logfile(p_size => '100M');
```

Suppression de journaux redo en ligne

Pour supprimer des journaux redo, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.drop_logfile`. La procédure `drop_logfile` comporte les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`grp`	positives	—	Oui	Numéro de groupe du journal.

L'exemple suivant supprime le journal doté du numéro de groupe 3.

```
exec rdsadmin.rdsadmin_util.drop_logfile(grp => 3);
```

Vous pouvez uniquement supprimer des journaux dont le statut est inutilisé ou inactif. L'exemple suivant permet d'obtenir les statuts des journaux.

```
SELECT GROUP#, STATUS FROM V$LOG;

GROUP#     STATUS
---------- ----------------
1          CURRENT
2          INACTIVE
3          INACTIVE
4          UNUSED
```

Redimensionnement de journaux redo en ligne

Une instance de base de données Amazon RDS exécutant Oracle démarre avec quatre journaux redo en ligne de 128 Mo chacun. L'exemple suivant montre comment vous pouvez utiliser les procédures Amazon RDS pour redimensionner vos journaux en remplaçant leur taille de 128 Mo par 512 Mo.

```
/* 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
```

Conservation des journaux redo archivés

Vous pouvez conserver localement les journaux redo archivés sur votre instance de base de données pour les utiliser avec des produits comme Oracle LogMiner (DBMS_LOGMNR). Une fois que vous avez conservé les journaux redo, vous pouvez utiliser LogMiner pour analyser les journaux. Pour de plus amples informations, veuillez consulter Using LogMiner to Analyze Redo Log Files dans la documentation Oracle.

Pour conserver les journaux redo archivés, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.set_configuration`. La procédure `set_configuration` comporte les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`name`	varchar	—	Oui	Nom de la configuration à mettre à jour.
`value`	varchar	—	Oui	Valeur pour la configuration.

L'exemple suivant conserve les journaux redo pendant 24 heures.

```
begin
    rdsadmin.rdsadmin_util.set_configuration(
        name  => 'archivelog retention hours',
        value => '24');
end;
/
commit;
```

> **Note**
>
> La validation est obligatoire pour que la modification prenne effet.

Pour voir combien de temps les journaux redo archivés sont conservés pour votre instance de base de données, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.show_configuration`.

L'exemple suivant affiche la durée de conservation des journaux.

```
set serveroutput on
exec rdsadmin.rdsadmin_util.show_configuration;
```

La sortie affiche le paramètre actuel pour `archivelog retention hours`. La sortie suivante montre que les journaux redo archivés sont conservés pendant 48 heures.

```
NAME:archivelog retention hours
VALUE:48
DESCRIPTION:ArchiveLog expiration specifies the duration in hours before archive/redo log
 files are automatically deleted.
```

Étant donné que les journaux redo archivés sont conservés sur votre instance de base de données, vérifiez que votre instance de base de données dispose d'un stockage alloué suffisant pour les journaux conservés. Pour déterminer la quantité d'espace que votre instance de base de données a utilisée au cours des X dernières heures, vous pouvez exécuter la requête suivante en remplaçant X par le nombre d'heures.

```
select sum(BLOCKS * BLOCK_SIZE) bytes
  from V$ARCHIVED_LOG
 where FIRST_TIME >= SYSDATE-(X/24) and DEST_ID=1;
```

Les journaux redo archivés sont générés uniquement si la période de conservation des sauvegardes de votre instance de base de données est supérieure à zéro. Par défaut, la période de conservation des sauvegardes est supérieure à zéro. Par conséquent, à moins que vous ayez explicitement mis la vôtre à zéro, les journaux redo archivés sont générés pour votre instance de base de données.

Vous ne pouvez pas retélécharger les journaux redo archivés dans votre instance de base de données après qu'ils aient été supprimés de celle-ci. Amazon RDS conserve les journaux redo archivés en dehors de votre instance de base de données pour supporter la restitution de cette dernière à un moment dans le temps. Amazon RDS conserve les journaux redo archivés en dehors de votre instance de base de données selon la période de rétention des sauvegardes configurée dans votre instance de base de données. Pour modifier la période de rétention des sauvegardes pour votre instance de base de données, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

> **Note**
>
> Dans certains cas, vous pouvez utiliser JDBC sur Linux pour télécharger les journaux redo archivés et connaître des temps de latence élevés et des réinitalisations de connexion. Dans ces cas, les problèmes peuvent être causés par le paramétrage du générateur de nombres aléatoires sur votre client Java. Nous vous recommandons de définir vos pilotes JDBC pour l'utilisation d'un générateur de nombres aléatoires sans blocage.

Accès aux journaux de transactions

L'accès aux journaux de transactions est pris en charge pour Oracle version 11.2.0.4.v11 et ultérieures, Oracle version 12.1.0.2.v7 et ultérieures, toutes les versions 12.2.0.1, toutes les versions 18.0.0.0 et toutes les versions 19.0.0.

Vous pouvez accéder à vos fichiers journaux redo en ligne et archivés pour les exploiter avec des outils externes comme GoldenGate, Attunity, Informatica, entre autres. Pour accéder à vos fichiers de journalisation Redo en ligne et archivés, vous devez d'abord créer des objets de répertoire qui fournissent un accès en lecture seule aux chemins d'accès physiques.

Le code suivant crée des répertoires qui fournissent un accès en lecture seule à vos fichiers de journalisation Redo en ligne et archivés :

> **Important**
>
> Ce code retire également le privilège `DROP ANY DIRECTORY`.

```
exec rdsadmin.rdsadmin_master_util.create_archivelog_dir;
exec rdsadmin.rdsadmin_master_util.create_onlinelog_dir;
```

Une fois que vous avez créé des objets de répertoire pour vos fichiers de journalisation Redo en ligne et archivés, vous pouvez lire les fichiers à l'aide de PL/SQL. Pour de plus amples informations sur la lecture de fichiers à partir d'objets de répertoire, veuillez consulter Établissement de la liste des fichiers situés dans un répertoire d'instance de base de données (p. 1165) et Lecture de fichiers dans un répertoire d'instance de base de données (p. 1166).

Le code suivant supprime les répertoires pour vos fichiers journaux redo en ligne et archivés.

```
exec rdsadmin.rdsadmin_master_util.drop_archivelog_dir;
exec rdsadmin.rdsadmin_master_util.drop_onlinelog_dir;
```

Le code suivant accorde et révoque le privilège `DROP ANY DIRECTORY`.

```
exec rdsadmin.rdsadmin_master_util.revoke_drop_any_directory;
exec rdsadmin.rdsadmin_master_util.grant_drop_any_directory;
```

Tâches Recovery Manager (RMAN) DBA courantes pour les instances base de données Oracle

Dans la section suivante, vous trouverez comment effectuer les tâches DBA Oracle Recovery Manager (RMAN) sur vos instances de base de données Amazon RDS exécutant Oracle. Pour offrir une expérience de service géré, Amazon RDS ne fournit pas l'accès shell aux instances de base de données. Il restreint également l'accès à certaines procédures système et tables qui requièrent des privilèges avancés.

Vous pouvez utiliser le package Amazon RDS `rdsadmin.rdsadmin_rman_util` pour effectuer les sauvegardes RMAN de votre base de données Amazon RDS for Oracle sur disque. Le package `rdsadmin.rdsadmin_rman_util` prend en charge les sauvegardes de fichiers de base de données complètes et incrémentielles, les sauvegardes d'espace de table et les sauvegardes de journal d'archives.

Les sauvegardes RMAN consomment un espace de stockage sur l'hôte d'instance de base de données Amazon RDS. Lorsque vous effectuez une sauvegarde, vous spécifiez un objet de répertoire Oracle en tant que paramètre dans l'appel de procédure. Les fichiers de sauvegarde sont placés dans le répertoire spécifié. Vous pouvez utiliser les répertoires par défaut, tels que `DATA_PUMP_DIR`, ou créer un répertoire. Pour de plus amples informations, veuillez consulter Création et suppression de répertoires dans l'espace de stockage de données principal (p. 1164).

Une fois qu'une sauvegarde RMAN est terminée, vous pouvez copier les fichiers de sauvegarde hors de l'hôte d'instance de base de données Amazon RDS for Oracle. Vous pouvez faire cela en vue d'une restauration vers un hôte non-RDS ou pour le stockage à long terme des sauvegardes. Par exemple, vous pouvez copier les fichiers de sauvegarde dans un compartiment Amazon S3. Pour de plus amples informations, reportez-vous à l'utilisation d'Intégration Amazon S3 (p. 1014).

Les fichiers de sauvegarde RMAN restent sur l'hôte d'instance de base de données Amazon RDS jusqu'à ce que vous les supprimiez manuellement. Vous pouvez utiliser la procédure Oracle `UTL_FILE.FREMOVE` pour supprimer les fichiers d'un répertoire. Pour de plus amples informations, veuillez consulter FREMOVE Procedure dans la documentation Oracle.

Lorsque vous sauvegardez les journaux redo archivés ou effectuez une sauvegarde complète ou incrémentielle incluant des journaux redo archivés, la conservation des journaux redo doit être définie sur une valeur non nulle. Pour de plus amples informations, veuillez consulter Conservation des journaux redo archivés (p. 1134).

> **Note**
>
> Pour une sauvegarde et une restauration vers une autre instance de base de données Amazon RDS for Oracle, vous pouvez continuer à utiliser les fonctions Amazon RDS de sauvegarde et de restauration. Pour de plus amples informations, veuillez consulter Sauvegarde et restauration d'une instance de base de données Amazon RDS (p. 317)
> Actuellement, la restauration RMAN n'est pas prise en charge pour les instances de base de données Amazon RDS for Oracle.

Rubriques

- Paramètres communs pour les procédures RMAN (p. 1137)
- Validation des fichiers d'instance de base de données (p. 1140)
- Activation et désactivation du suivi des modifications de bloc (p. 1143)
- Recoupement des journaux redo archivés (p. 1144)
- Sauvegarde des journaux redo archivés (p. 1145)
- Réalisation d'une sauvegarde complète de base de données (p. 1150)
- Réalisation d'une sauvegarde incrémentielle de base de données (p. 1151)
- Réalisation d'une sauvegarde d'espace de table (p. 1152)

Paramètres communs pour les procédures RMAN

Vous pouvez utiliser des procédures dans le package Amazon RDS `rdsadmin.rdsadmin_rman_util` pour effectuer des tâches avec RMAN. Plusieurs paramètres sont communs aux procédures figurant dans le package. Le package possède les paramètres communs suivants.

Nom du paramètre	Type de données	Valeurs valides	Par défaut	Obligatoire	Description
`p_owner`	varchar2	Propriétaire valide du répertoire spécifié dans `p_directory_name`.	—	Oui	Propriétaire du répertoire devant contenir les fichiers de sauvegarde.
`p_directory_name`	varchar2	Nom de répertoire de base de données valide.	–	Oui	Nom du répertoire devant contenir les fichiers de sauvegarde.
`p_label`	varchar2	`a-z`, `A-Z`, `0-9`, `'_'`, `'-'`, `'.'`	—	Non	Chaîne unique incluse dans les noms de fichiers de sauvegarde. **Note** La limite est de 30 caractères.

Nom du paramètre	Type de données	Valeurs valides	Par défaut	Obligatoire	Description
`p_compress`	booléen	`TRUE`, `FALSE`	`FALSE`	Non	Spécifiez `TRUE` pour activer la compression de sauvegarde DE BASE. Spécifiez `FALSE` pour désactiver la compression de sauvegarde DE BASE.
`p_include_archive_logs`	booléen	`TRUE`, `FALSE`	`FALSE`	Non	Spécifiez `TRUE` pour inclure les journaux redo archivés dans la sauvegarde. Spécifiez `FALSE` pour exclure les journaux redo archivés de la sauvegarde. Si vous incluez les journaux redo archivés dans la sauvegarde, définissez la conservation sur une heure ou plus à l'aide de la procédure `rdsadmin.rdsadmin_util.set_co` De plus, appelez la procédure `rdsadmin.rdsadmin_rman_util.c` immédiatement avant d'exécuter la sauvegarde. Dans le cas contraire, la sauvegarde peut échouer en raison de fichiers journaux redo archivés manquants qui ont été supprimés par les procédures de gestion Amazon RDS.
`p_include_controlfile`	booléen	`TRUE`, `FALSE`	`FALSE`	Non	Spécifiez `TRUE` pour inclure le fichier de contrôle dans la sauvegarde. Spécifiez `FALSE` pour exclure le fichier de contrôle de la sauvegarde.

Nom du paramètre	Type de données	Valeurs valides	Par défaut	Obligatoire	Description
`p_optimize`	booléen	`TRUE`, `FALSE`	`TRUE`	Non	Spécifiez `TRUE` pour activer l'optimisation de la sauvegarde, si des journaux redo archivés sont inclus, afin de réduire la taille de la sauvegarde. Spécifiez `FALSE` pour désactiver l'optimisation de la sauvegarde.
`p_parallel`	nombre	Entier valide compris entre `1` et `254` pour Oracle Database Enterprise Edition (EE) `1` pour d'autres éditions d'Oracle Database	`1`	Non	Nombre de canaux.
`p_rman_to_dbms_output`	booléen	`TRUE`, `FALSE`	`FALSE`	Non	Lorsque la valeur est `TRUE`, la sortie RMAN est envoyée au package `DBMS_OUTPUT` ainsi qu'à un fichier du répertoire `BDUMP`. Dans SQL*Plus, utilisez `SET SERVEROUTPUT ON` pour voir la sortie. Lorsque la valeur est `FALSE`, la sortie RMAN est envoyée uniquement à un fichier dans le répertoire `BDUMP`.

Nom du paramètre	Type de données	Valeurs valides	Par défaut	Obligatoire	Description
`p_section_size_mb`	nombre	Entier valide	`NULL`	Non	Taille de la section en mégaoctets (Mo). Valide en parallèle en divisant chaque fichier dans la taille de section spécifiée. Lorsque la valeur est `NULL`, le paramètre est ignoré.
`p_validation_type`	varchar2	`'PHYSICAL'` `'PHYSICAL+LOGICAL'`	`'PHYSICAL'`	Non	Niveau de détection de la corruption. Spécifiez `'PHYSICAL'` pour rechercher de la corruption physique. Par exemple, la corruption physique peut être un bloc dont l'en-tête et le pied de page ne correspondent pas. Spécifiez `'PHYSICAL+LOGICAL'` pour rechercher les incohérences logiques en plus de la corruption physique. Un bloc corrompu est un exemple de corruption logique.

Validation des fichiers d'instance de base de données

Vous pouvez utiliser le package Amazon RDS `rdsadmin.rdsadmin_rman_util` pour valider des fichiers d'instance de base de données Amazon RDS for Oracle, notamment des fichiers de données, des espaces de table, des fichiers de contrôle ou des fichiers de paramètres de serveur (SPFILE).

Pour de plus amples informations sur la validation RMAN, veuillez consulter Validating Database Files and Backups et VALIDATE dans la documentation Oracle.

Rubriques

- Validation d'une instance de base de données (p. 1141)
- Validation d'un espace de table (p. 1141)
- Validation d'un fichier de contrôle (p. 1142)
- Validation d'un fichier SPFILE (p. 1142)
- Validation d'un fichier de données (p. 1142)

Validation d'une instance de base de données

Pour valider tous les fichiers pertinents utilisés par une instance de base de données Amazon RDS Oracle, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_rman_util.validate_database`.

Cette procédure utilise les paramètres courants suivants pour les tâches RMAN :

- `p_validation_type`
- `p_parallel`
- `p_section_size_mb`
- `p_rman_to_dbms_output`

Pour de plus amples informations, veuillez consulter Paramètres communs pour les procédures RMAN (p. 1137).

L'exemple suivant valide l'instance de base de données à l'aide des valeurs par défaut pour les paramètres.

```
exec rdsadmin.rdsadmin_rman_util.validate_database;
```

L'exemple suivant valide l'instance de base de données à l'aide des valeurs spécifiées pour les paramètres.

```
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;
/
```

Lorsque le paramètre `p_rman_to_dbms_output` est défini sur `FALSE`, la sortie RMAN est écrite dans un fichier, dans le répertoire `BDUMP`.

Pour afficher les fichiers dans le répertoire `BDUMP`, exécutez l'instruction `SELECT` suivante.

```
SELECT * FROM table(rdsadmin.rds_file_util.listdir('BDUMP')) order by mtime;
```

Pour afficher le contenu d'un fichier dans le répertoire `BDUMP`, exécutez l'instruction `SELECT` suivante.

```
SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP','rds-rman-
validate-nnn.txt'));
```

Remplacez le nom du fichier par celui du fichier que vous souhaitez afficher.

Validation d'un espace de table

Pour valider les fichiers associés à un espace de table, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_rman_util.validate_tablespace`.

Cette procédure utilise les paramètres courants suivants pour les tâches RMAN :

- `p_validation_type`

- `p_parallel`
- `p_section_size_mb`
- `p_rman_to_dbms_output`

Pour de plus amples informations, veuillez consulter Paramètres communs pour les procédures RMAN (p. 1137).

Cette procédure utilise également le paramètre supplémentaire suivant.

Nom du paramètre	Type de données	Valeurs valides	Par défaut	Obligatoire	Description
`p_tablespace_name`	varchar2	Nom d'espace de table valide	—	Oui	Nom de l'espace de table.

Validation d'un fichier de contrôle

Pour valider uniquement le fichier de contrôle utilisé par une instance de base de données Amazon RDS Oracle, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_rman_util.validate_current_controlfile`.

Cette procédure utilise le paramètre courant suivant pour les tâches RMAN :

- `p_validation_type`
- `p_rman_to_dbms_output`

Pour de plus amples informations, veuillez consulter Paramètres communs pour les procédures RMAN (p. 1137).

Validation d'un fichier SPFILE

Pour valider uniquement le fichier de paramètres serveur (SPFILE) utilisé par une instance de base de données Amazon RDS Oracle, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_rman_util.validate_spfile`.

Cette procédure utilise le paramètre courant suivant pour les tâches RMAN :

- `p_validation_type`
- `p_rman_to_dbms_output`

Pour plus d'informations, consultez Paramètres communs pour les procédures RMAN (p. 1137).

Validation d'un fichier de données

Pour valider un fichier de données, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_rman_util.validate_datafile`.

Cette procédure utilise les paramètres courants suivants pour les tâches RMAN :

- `p_validation_type`
- `p_parallel`
- `p_section_size_mb`

- `p_rman_to_dbms_output`

Pour de plus amples informations, veuillez consulter Paramètres communs pour les procédures RMAN (p. 1137).

Cette procédure utilise également les paramètres supplémentaires suivants.

Nom du paramètre	Type de données	Valeurs valides	Par défaut	Obligatoire	Description
`p_datafile`	varchar2	Numéro d'ID de fichier de données valide ou nom de fichier de données valide comprenant le chemin complet	—	Oui	Numéro d'ID de fichier de données (issu de `v$datafile.file#`) ou nom de fichier de données complet comprenant le chemin (issu de `v$datafile.name`).
`p_from_block`	nombre	Entier valide	`NULL`	Non	Numéro du bloc par lequel la validation commence à l'intérieur du fichier de données. Lorsqu'il est `NULL`, `1` est utilisé.
`p_to_block`	nombre	Entier valide	`NULL`	Non	Numéro du bloc par lequel la validation finit à l'intérieur du fichier de données. Lorsqu'il est `NULL`, le bloc le plus grand du fichier de données est utilisé.

Activation et désactivation du suivi des modifications de bloc

Vous pouvez activer le suivi des modifications de bloc pour une instance de base de données à l'aide de la procédure Amazon RDS `rdsadmin.rdsadmin_rman_util.enable_block_change_tracking`.

Vous pouvez désactiver le suivi des modifications de bloc pour une instance de base de données à l'aide de la procédure Amazon RDS `rdsadmin.rdsadmin_rman_util.disable_block_change_tracking`.

Ces procédures ne prennent aucun paramètre. L'activation du suivi des modifications de bloc peut améliorer les performances des sauvegardes incrémentielles.

Ces procédures sont prises en charge pour les versions suivantes du moteur de base de données Amazon RDS for Oracle :

- 11.2.0.4.v19 ou versions 11.2 supérieures
- 12.1.0.2.v15 ou versions 12.1 supérieures
- 12.2.0.1.ru-2019-01.rur-2019-01.r1 ou versions 12.2 supérieures

- Toutes les versions 18.0.0.0
- Toutes les versions 19.0.0.0

Pour déterminer si le suivi des modifications de bloc est activé pour votre instance de base de données, exécutez la requête suivante.

```
SELECT status, filename FROM V$BLOCK_CHANGE_TRACKING;
```

L'exemple suivant active le suivi des modifications de bloc pour une instance de base de données.

```
exec rdsadmin.rdsadmin_rman_util.enable_block_change_tracking;
```

L'exemple suivant désactive le suivi des modifications de bloc pour une instance de base de données.

```
exec rdsadmin.rdsadmin_rman_util.disable_block_change_tracking;
```

Recoupement des journaux redo archivés

Vous pouvez recouper les journaux redo archivés en utilisant la procédure Amazon RDS `rdsadmin.rdsadmin_rman_util.crosscheck_archivelog`.

Vous pouvez utiliser cette procédure pour recouper les journaux redo archivés inscrits dans le fichier de contrôle et supprimer éventuellement les enregistrements de journaux ayant expiré. Quand RMAN effectue une sauvegarde, il crée un enregistrement dans le fichier de contrôle. Au fil du temps, ces enregistrements augmentent la taille du fichier de contrôle. Nous vous recommandons de supprimer périodiquement les enregistrements expirés.

> **Note**
>
> Les sauvegardes Amazon RDS standard n'utilisent pas RMAN et ne créent donc pas d'enregistrement dans le fichier de contrôle.

Cette procédure utilise le paramètre courant `p_rman_to_dbms_output` pour les tâches RMAN.

Pour de plus amples informations, veuillez consulter Paramètres communs pour les procédures RMAN (p. 1137).

Cette procédure utilise également le paramètre supplémentaire suivant.

Nom du paramètre	Type de données	Valeurs valides	Par défaut	Obligatoire	Description
`p_delete_expired`	booléen	`TRUE`, `FALSE`	`TRUE`	Non	Lorsque la valeur est `TRUE`, supprimez les enregistrements de journaux redo archivés expirés du fichier de contrôle. Lorsque la valeur est `FALSE`, conservez les enregistrements de journaux redo archivés expirés dans le fichier de contrôle.

Cette procédure est prise en charge pour les versions suivantes du moteur de base de données Amazon RDS for Oracle :

- 11.2.0.4.v19 ou versions 11.2 supérieures
- 12.1.0.2.v15 ou versions 12.1 supérieures
- 12.2.0.1.ru-2019-01.rur-2019-01.r1 ou versions 12.2 supérieures
- Toutes les versions 18.0.0.0
- Toutes les versions 19.0.0.0

L'exemple suivant marque les enregistrements de journaux redo archivés dans le fichier de contrôle comme ayant expiré, mais ne les supprime pas.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.crosscheck_archivelog(
        p_delete_expired      => FALSE,
        p_rman_to_dbms_output => FALSE);
END;
/
```

L'exemple suivant supprime les enregistrements de journaux redo archivés expirés du fichier de contrôle.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.crosscheck_archivelog(
        p_delete_expired      => TRUE,
        p_rman_to_dbms_output => FALSE);
END;
/
```

Sauvegarde des journaux redo archivés

Vous pouvez utiliser le package Amazon RDS `rdsadmin.rdsadmin_rman_util` pour sauvegarder les journaux redo archivés pour une instance de base de données Oracle Amazon RDS.

Les procédures de sauvegarde des journaux redo archivés sont prises en charge pour les versions suivantes du moteur de base de données Amazon RDS for Oracle :

- 11.2.0.4.v19 ou versions 11.2 supérieures
- 12.1.0.2.v15 ou versions 12.1 supérieures
- 12.2.0.1.ru-2019-01.rur-2019-01.r1 ou versions 12.2 supérieures
- Toutes les versions 18.0.0.0
- Toutes les versions 19.0.0.0

Rubriques

- Sauvegarde de tous les journaux redo archivés (p. 1145)
- Sauvegarde d'un journal redo archivé à partir d'une plage de dates (p. 1146)
- Sauvegarde d'un journal redo archivé à partir d'une plage de numéros SCN (p. 1148)
- Sauvegarde d'un journal redo archivé à partir d'une plage de numéros de séquence (p. 1149)

Sauvegarde de tous les journaux redo archivés

Pour sauvegarder tous les journaux redo archivés pour une instance de base de données Amazon RDS Oracle, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_rman_util.backup_archivelog_all`.

Cette procédure utilise les paramètres courants suivants pour les tâches RMAN :

- `p_owner`
- `p_directory_name`
- `p_label`
- `p_parallel`
- `p_compress`
- `p_rman_to_dbms_output`

Pour de plus amples informations, veuillez consulter Paramètres communs pour les procédures RMAN (p. 1137).

L'exemple suivant sauvegarde tous les journaux redo archivés pour l'instance de base de données.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.backup_archivelog_all(
        p_owner               => 'SYS',
        p_directory_name      => 'MYDIRECTORY',
        p_parallel            => 4,
        p_rman_to_dbms_output => FALSE);
END;
/
```

Sauvegarde d'un journal redo archivé à partir d'une plage de dates

Pour sauvegarder des journaux redo archivés spécifiques pour une instance de base de données Amazon RDS Oracle, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_rman_util.backup_archivelog_date`. La plage de dates indique quels journaux redo archivés sauvegarder.

Cette procédure utilise les paramètres courants suivants pour les tâches RMAN :

- `p_owner`
- `p_directory_name`
- `p_label`
- `p_parallel`
- `p_compress`
- `p_rman_to_dbms_output`

Pour de plus amples informations, veuillez consulter Paramètres communs pour les procédures RMAN (p. 1137).

Cette procédure utilise également les paramètres supplémentaires suivants.

Nom du paramètre	Type de données	Valeurs valides	Par défaut	Obligatoire	Description
`p_from_date`	date	Date comprise entre	—	Oui	Date de début des sauvegardes des journaux archivés.

Nom du paramètre	Type de données	Valeurs valides	Par défaut	Obligatoire	Description
		`start_date` et `next_date` d'un journal redo archivé qui existe sur le disque. Cette valeur doit être inférieure ou égale à la valeur spécifiée pour `p_to_date`.			
`p_to_date`	date	Date comprise entre `start_date` et `next_date` d'un journal redo archivé qui existe sur le disque. Cette valeur doit être supérieure ou égale à la valeur spécifiée pour `p_from_date`.	—	Oui	Date de fin des sauvegardes des journaux archivés.

L'exemple suivant sauvegarde les journaux redo archivés dans la plage de dates pour l'instance de base de données.

```
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_rman_to_dbms_output => FALSE);
END;
/
```

Sauvegarde d'un journal redo archivé à partir d'une plage de numéros SCN

Pour sauvegarder des journaux redo archivés spécifiques pour une instance de base de données Amazon RDS Oracle, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_rman_util.backup_archivelog_scn`. La plage de numéros SCN indique quels journaux redo archivés sauvegarder.

Cette procédure utilise les paramètres courants suivants pour les tâches RMAN :

- `p_owner`
- `p_directory_name`
- `p_label`
- `p_parallel`
- `p_compress`
- `p_rman_to_dbms_output`

Pour de plus amples informations, veuillez consulter Paramètres communs pour les procédures RMAN (p. 1137).

Cette procédure utilise également les paramètres supplémentaires suivants.

Nom du paramètre	Type de données	Valeurs valides	Par défaut	Obligatoire	Description
`p_from_scn`	nombre	Numéro SCN d'un journal redo archivé qui existe sur le disque. Cette valeur doit être inférieure ou égale à la valeur spécifiée pour `p_to_scn`.	—	Oui	Numéro SCN de début des sauvegardes des journaux archivés.
`p_to_scn`	nombre	Numéro SCN d'un journal redo archivé qui existe sur le disque. Cette valeur doit être supérieure ou égale	—	Oui	Numéro SCN de fin des sauvegardes des journaux archivés.

Nom du paramètre	Type de données	Valeurs valides	Par défaut	Obligatoire	Description
		à la valeur spécifiée pour `p_from_scn`.			

L'exemple suivant sauvegarde les journaux redo archivés dans la plage de numéros SCN pour l'instance de base de données.

```
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_rman_to_dbms_output => FALSE);
END;
/
```

Sauvegarde d'un journal redo archivé à partir d'une plage de numéros de séquence

Pour sauvegarder des journaux redo archivés spécifiques pour une instance de base de données Amazon RDS Oracle, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_rman_util.backup_archivelog_sequence`. La plage de numéros de séquence indique quels journaux redo archivés sauvegarder.

Cette procédure utilise les paramètres courants suivants pour les tâches RMAN :

- `p_owner`
- `p_directory_name`
- `p_label`
- `p_parallel`
- `p_compress`
- `p_rman_to_dbms_output`

Pour de plus amples informations, veuillez consulter Paramètres communs pour les procédures RMAN (p. 1137).

Cette procédure utilise également les paramètres supplémentaires suivants.

Nom du paramètre	Type de données	Valeurs valides	Par défaut	Obligatoire	Description
`p_from_sequence`	nombre	Numéro de séquence d'un journal redo archivé qui	—	Oui	Numéro de séquence de début des sauvegardes des journaux archivés.

Nom du paramètre	Type de données	Valeurs valides	Par défaut	Obligatoire	Description
		existe sur le disque. Cette valeur doit être inférieure ou égale à la valeur spécifiée pour `p_to_sequence`.			
`p_to_sequence`	nombre	Numéro de séquence d'un journal redo archivé qui existe sur le disque. Cette valeur doit être supérieure ou égale à la valeur spécifiée pour `p_from_sequence`.	—	Oui	Numéro de séquence de fin des sauvegardes des journaux archivés.

L'exemple suivant sauvegarde les journaux redo archivés dans la plage de numéros de séquence pour l'instance de base de données.

```
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_rman_to_dbms_output => FALSE);
END;
/
```

Réalisation d'une sauvegarde complète de base de données

Vous pouvez effectuer une sauvegarde de tous les blocs de fichiers de données inclus dans la sauvegarde en utilisant la procédure Amazon RDS `rdsadmin.rdsadmin_rman_util.backup_database_full`.

Cette procédure utilise les paramètres courants suivants pour les tâches RMAN :

- `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`

Pour de plus amples informations, veuillez consulter Paramètres communs pour les procédures RMAN (p. 1137).

Cette procédure est prise en charge pour les versions suivantes du moteur de base de données Amazon RDS for Oracle :

- 11.2.0.4.v19 ou versions 11.2 supérieures
- 12.1.0.2.v15 ou versions 12.1 supérieures
- 12.2.0.1.ru-2019-01.rur-2019-01.r1 ou versions 12.2 supérieures
- Toutes les versions 18.0.0.0
- Toutes les versions 19.0.0.0

L'exemple suivant effectue une sauvegarde complète de l'instance de base de données à l'aide des valeurs spécifiées pour les paramètres.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.backup_database_full(
        p_owner               => 'SYS',
        p_directory_name      => 'MYDIRECTORY',
        p_parallel            => 4,
        p_section_size_mb     => 10,
        p_rman_to_dbms_output => FALSE);
END;
/
```

Réalisation d'une sauvegarde incrémentielle de base de données

Vous pouvez effectuer une sauvegarde incrémentielle de votre instance de base de données en utilisant la procédure Amazon RDS `rdsadmin.rdsadmin_rman_util.backup_database_incremental`.

Pour de plus amples informations sur les sauvegardes incrémentielles, veuillez consulter Incremental Backups dans la documentation Oracle.

Cette procédure utilise les paramètres courants suivants pour les tâches RMAN :

- `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`

Pour de plus amples informations, veuillez consulter Paramètres communs pour les procédures RMAN (p. 1137).

Cette procédure est prise en charge pour les versions suivantes du moteur de base de données Amazon RDS for Oracle :

- 11.2.0.4.v19 ou versions 11.2 supérieures
- 12.1.0.2.v15 ou versions 12.1 supérieures
- 12.2.0.1.ru-2019-01.rur-2019-01.r1 ou versions 12.2 supérieures
- Toutes les versions 18.0.0.0
- Toutes les versions 19.0.0.0

Cette procédure utilise également le paramètre supplémentaire suivant.

Nom du paramètre	Type de données	Valeurs valides	Par défaut	Obligatoire	Description
`p_level`	nombre	`0`, `1`	`0`	Non	Spécifiez `0` pour activer une sauvegarde incrémentielle complète. Spécifiez `1` pour activer une sauvegarde incrémentielle non cumulative.

L'exemple suivant effectue une sauvegarde incrémentielle de l'instance de base de données à l'aide des valeurs spécifiées pour les paramètres.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.backup_database_incremental(
        p_owner               => 'SYS',
        p_directory_name      => 'MYDIRECTORY',
        p_level               => 1,
        p_parallel            => 4,
        p_section_size_mb     => 10,
        p_rman_to_dbms_output => FALSE);
END;
/
```

Réalisation d'une sauvegarde d'espace de table

Vous pouvez effectuer la sauvegarde de l'espace de table d'une instance de base de données en utilisant la procédure Amazon RDS `rdsadmin.rdsadmin_rman_util.backup_tablespace`.

Cette procédure utilise les paramètres courants suivants pour les tâches RMAN :

- `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`

Pour de plus amples informations, veuillez consulter Paramètres communs pour les procédures RMAN (p. 1137).

Cette procédure utilise également le paramètre supplémentaire suivant.

Nom du paramètre	Type de données	Valeurs valides	Par défaut	Obligatoire	Description
`p_tablespace_name`	varchar2	Nom d'espace de table valide.	—	Oui	Nom de l'espace de table à sauvegarder.

Cette procédure est prise en charge pour les versions suivantes du moteur de base de données Amazon RDS for Oracle :

- 11.2.0.4.v19 ou versions 11.2 supérieures
- 12.1.0.2.v15 ou versions 12.1 supérieures
- 12.2.0.1.ru-2019-01.rur-2019-01.r1 ou versions 12.2 supérieures
- Toutes les versions 18.0.0.0
- Toutes les versions 19.0.0.0

L'exemple suivant effectue une sauvegarde d'espace de table à l'aide des valeurs spécifiées pour les paramètres.

```
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_rman_to_dbms_output => FALSE);
END;
/
```

Tâches Oracle Scheduler communes de DBA pour les instances de base de données Oracle

Certains travaux du planificateur relevant de SYS pouvant interférer avec les opérations de base de données normales, le Support Oracle recommande de les désactiver ou de modifier la planification de ces travaux. Vous pouvez utiliser le package Amazon RDS `rdsadmin.rdsadmin_dbms_scheduler` pour effectuer des tâches pour les travaux Oracle Scheduler relevant de SYS.

Ces procédures sont prises en charge pour les versions suivantes du moteur de base de données Amazon RDS for Oracle :

- 19c
- 18c
- 12.2.0.2.ru-2019-07.rur-2019-07.r1 ou versions 12.2 supérieures
- 12.1.0.2.v17 ou versions 12.1 supérieures
- 11.2.0.4.v21 ou versions 11.2 supérieures

Paramètres communs pour les procédures d'Oracle Scheduler

Pour effectuer des tâches avec Oracle Scheduler, utilisez les procédures du package Amazon RDS `rdsadmin.rdsadmin_dbms_scheduler`. Plusieurs paramètres sont communs aux procédures du package. Le package possède les paramètres communs suivants.

Nom du paramètre	Type de données	Valeurs valides	Par défaut	Obligatoire	Description
`name`	varchar2	`'SYS.BSLN_MAINTAIN_STATS_JOB'`, `'SYS.CLEANUP_ONLINE_IND_BUILD`	–	Oui	Nom du travail à modifier. Note Pour l'heure, vous pouvez modifier uniquement les travaux `SYS.CLEANUP_ONLINE_IND_BUI` et `SYS.BSLN_MAINTAIN_STATS_JO`
`attribute`	varchar2	`'REPEAT_INTERVAL'`,`'SCHEDULE_NAME'`	–	Oui	Attribut à modifier. Pour modifier l'intervalle de répétition du travail, spécifiez `'REPEAT_INTERVAL'`. Pour modifier le nom de planification du travail, spécifiez `'SCHEDULE_NAME'`.
`value`	varchar2	Intervalle ou nom de planification valide, selon l'attribut utilisé.	–	Oui	Nouvelle valeur de l'attribut.

Modification des travaux DBMS_SCHEDULER

Vous pouvez utiliser la procédure Oracle `dbms_scheduler.set_attribute` pour modifier certains composants d'Oracle Scheduler. Pour de plus amples informations, veuillez consulter DBMS_SCHEDULER et la procédure SET_ATTRIBUTE dans la documentation Oracle.

Lorsque vous utilisez des instances de base de données Amazon RDS, ajoutez le nom du schéma `SYS` au début du nom de l'objet. L'exemple suivant définit l'attribut du plan de la ressource pour l'objet monday window.

```
begin
    dbms_scheduler.set_attribute(
        name      => 'SYS.MONDAY_WINDOW',
        attribute => 'RESOURCE_PLAN',
        value     => 'resource_plan_1');
end;
/
```

> **Note**
>
> Certains travaux Oracle Scheduler relevant de SYS peuvent interférer avec les opérations de base de données normales. Le Support Oracle recommande de désactiver ces travaux ou de modifier leur planification. Amazon RDS pour Oracle ne fournit pas les privilèges permettant de modifier les travaux Oracle Scheduler relevant de SYS à l'aide du package `DBMS_SCHEDULER`. À la place, vous pouvez utiliser les procédures du package Amazon RDS `rdsadmin.rdsadmin_dbms_scheduler` pour effectuer des tâches pour les travaux Oracle Scheduler relevant de SYS. Pour obtenir des informations sur l'utilisation de ces paramètres, consultez Tâches Oracle Scheduler communes de DBA pour les instances de base de données Oracle (p. 1153).

Définition du fuseau horaire pour les tâches d'Oracle Scheduler

Pour modifier le fuseau horaire d'Oracle Scheduler, vous pouvez utiliser la procédure Oracle `dbms_scheduler.set_scheduler_attribute`. Pour de plus amples informations sur le package `dbms_scheduler`, veuillez consulter DBMS_SCHLENDER et SET_SCHENDER_ATTRIBUTE dans la documentation Oracle.

Pour modifier le paramètre de fuseau horaire actuel

1. Connectez-vous à la base de données à l'aide d'un client tel que SQL Developer. Pour plus d'informations, consultez Connexion à votre instance de base de données à l'aide d'Oracle SQL Developer (p. 963).
2. Définissez le fuseau horaire par défaut comme suit, en remplaçant votre fuseau horaire par *`time_zone_name`*.

```
begin
  dbms_scheduler.set_scheduler_attribute(
    attribute => 'default_timezone',
    value => 'time_zone_name'
  );
end;
/
```

Dans l'exemple suivant, vous changez le fuseau horaire pour Asia/Shanghai.

Commencez par interroger le fuseau horaire actuel, comme indiqué ci-dessous.

```
SELECT VALUE FROM DBA_SCHEDULER_GLOBAL_ATTRIBUTE WHERE ATTRIBUTE_NAME='DEFAULT_TIMEZONE';
```

La sortie indique que le fuseau horaire actuel est ETC/UTC.

```
VALUE
```

```
-------
Etc/UTC
```

Ensuite, vous définissez le fuseau horaire sur Asia/Shanghai.

```
begin
  dbms_scheduler.set_scheduler_attribute(
    attribute => 'default_timezone',
    value => 'Asia/Shanghai'
  );
end;
/
```

Pour plus d'informations sur la modification du fuseau horaire système, consultez Fuseau horaire Oracle (p. 1088).

Désactivation de travaux Oracle Scheduler relevant de SYS

Pour désactiver un travail Oracle Scheduler relevant de SYS, utilisez la procédure `rdsadmin.rdsadmin_dbms_scheduler.disable`.

Cette procédure utilise le paramètre commun `name` pour les tâches Oracle Scheduler. Pour plus d'informations, consultez Paramètres communs pour les procédures d'Oracle Scheduler (p. 1154).

L'exemple suivant désactive le travail Oracle Scheduler `SYS.CLEANUP_ONLINE_IND_BUILD`.

```
BEGIN
   rdsadmin.rdsadmin_dbms_scheduler.disable('SYS.CLEANUP_ONLINE_IND_BUILD');
END;
/
```

Activation de travaux Oracle Scheduler relevant de SYS

Pour activer un travail Oracle Scheduler relevant de SYS, utilisez la procédure `rdsadmin.rdsadmin_dbms_scheduler.disable`.

Cette procédure utilise le paramètre commun `name` pour les tâches Oracle Scheduler. Pour plus d'informations, consultez Paramètres communs pour les procédures d'Oracle Scheduler (p. 1154).

L'exemple suivant active le travail Oracle Scheduler `SYS.CLEANUP_ONLINE_IND_BUILD`.

```
BEGIN
   rdsadmin.rdsadmin_dbms_scheduler.enable('SYS.CLEANUP_ONLINE_IND_BUILD');
END;
/
```

Modification de l'intervalle de répétition pour des travaux de type CALENDAR

Pour modifier l'intervalle de répétition d'un travail Oracle Scheduler relevant de SYS de type `CALENDAR`, utilisez la procédure `rdsadmin.rdsadmin_dbms_scheduler.disable`.

Cette procédure utilise les paramètres communs suivants pour les tâches Oracle Scheduler :

- `name`

- `attribute`
- `value`

Pour plus d'informations, consultez Paramètres communs pour les procédures d'Oracle Scheduler (p. 1154).

L'exemple suivant modifier l'intervalle de répétition du travail Oracle Scheduler `SYS.CLEANUP_ONLINE_IND_BUILD`.

```
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;
/
```

Modification de l'intervalle de répétition pour des travaux de type NAMED

Certains travaux Oracle Scheduler utilisent non pas un intervalle, mais un nom de planification. Pour ce type de travaux, vous devez créer une planification nommée dans le schéma d'utilisateur principal. Pour cela, utilisez la procédure Oracle standard `sys.dbms_scheduler.create_schedule`. De même, utilisez `rdsadmin.rdsadmin_dbms_scheduler.set_attribute procedure` pour affecter la nouvelle planification nommée au travail.

Cette procédure utilise le paramètre commun suivant pour les tâches Oracle Scheduler :

- `name`
- `attribute`
- `value`

Pour plus d'informations, consultez Paramètres communs pour les procédures d'Oracle Scheduler (p. 1154).

L'exemple suivant modifie l'intervalle de répétition du travail Oracle Scheduler `SYS.BSLN_MAINTAIN_STATS_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;
```

/

Tâches de diagnostic DBA courantes pour les instances de base de données Oracle

Oracle Database inclut une infrastructure de diagnostic des pannes que vous pouvez utiliser pour analyser les problèmes de base de données. Dans la terminologie Oracle, un problème est une erreur critique, par exemple, un bogue de code ou une corruption de données. Un incident est la survenue d'un problème. Si la même erreur se produit trois fois, l'infrastructure affiche trois incidents de ce problème. Pour de plus amples informations, veuillez consulter Diagnostic et résolution de problèmes dans la documentation Oracle Database.

L'utilitaire ADRCI (Automatic Diagnostic Repository Command Interpreter) est un outil de ligne de commande Oracle qui vous permet de gérer les données de diagnostic. Par exemple, vous pouvez utiliser cet outil pour analyser les problèmes et regrouper les données de diagnostic. Un package d'incidents inclut les données de diagnostic d'un incident ou de tous les incidents qui se rapportent à un problème spécifique. Vous pouvez charger un package d'incidents, qui est implémenté en tant que fichier .zip, vers le support Oracle.

Pour offrir une expérience de service géré, Amazon RDS ne fournit pas l'accès shell à ADRCI. Pour effectuer des tâches de diagnostic pour votre instance Oracle, utilisez plutôt le package Amazon RDS `rdsadmin.rdsadmin_adrci_util`.

Grâce aux fonctions incluses dans `rdsadmin_adrci_util`, vous pouvez répertorier et regrouper les problèmes et les incidents, et également afficher les fichiers de trace. Toutes les fonctions renvoient un ID de tâche. Cet ID fait partie du nom du fichier journal qui contient la sortie ADRCI, comme dans `dbtask-`*`task_id`*`.log`. Le fichier journal réside dans le répertoire BDUMP.

Paramètres courants pour les procédures de diagnostic

Pour effectuer des tâches de diagnostic, utilisez les fonctions du package Amazon RDS `rdsadmin.rdsadmin_adrci_util`. Le package possède les paramètres communs suivants.

Nom du paramètre	Type de données	Valeurs valides	Par défaut	Obligatoire	Description
`incident_id`	nombre	Un ID d'incident valide ou null	Null	Non	Si la valeur est null, la fonction affiche tous les incidents. Si la valeur n'est pas null et représente un ID d'incident valide, la fonction affiche l'incident spécifié.
`problem_id`	nombre	Un ID de problème valide ou null	Null	Non	Si la valeur est null, la fonction affiche tous les problèmes. Si la valeur n'est pas null et représente un ID de problème valide, la fonction affiche le problème spécifié.
`last`	nombre	Un entier valide	Null	Non	Si la valeur est null, la fonction affiche au

Nom du paramètre	Type de données	Valeurs valides	Par défaut	Obligatoire	Description
		supérieur à 0 ou null			maximum 50 éléments. Si la valeur n'est pas null, la fonction affiche le nombre spécifié.

Répertorier les incidents

Pour répertorier les incidents de diagnostic pour Oracle, utilisez la fonction Amazon RDS `rdsadmin.rdsadmin_adrci_util.list_adrci_incidents`. Vous pouvez répertorier les incidents en mode basique ou détaillé. Par défaut, la fonction répertorie les 50 incidents les plus récents.

Cette fonction utilise les paramètres communs suivants :

- `incident_id`
- `problem_id`

Si vous spécifiez les deux paramètres précédents, `incident_id` remplace `problem_id`. Pour de plus amples informations, veuillez consulter Paramètres courants pour les procédures de diagnostic (p. 1158).

Cette fonction utilise le paramètre supplémentaire suivant.

Nom du paramètre	Type de données	Valeurs valides	Par défaut	Obligatoire	Description
`detail`	booléen	`TRUE` ou `FALSE`	`FALSE`	Non	Si `TRUE`, la fonction répertorie les incidents en mode détail. Si `FALSE`, la fonction répertorie les incidents en mode basique.

Pour répertorier tous les incidents, appelez la fonction `rdsadmin.rdsadmin_adrci_util.list_adrci_incidents` sans aucun argument. Vous pouvez stocker la sortie dans une variable client SQL.

```
SQL> VAR task_id VARCHAR2(80);
SQL> exec :task_id := rdsadmin.rdsadmin_adrci_util.list_adrci_incidents;

PL/SQL procedure successfully completed.
```

Pour obtenir l'ID de tâche, spécifiez la variable dans une requête de la table `dual`.

```
SQL> SELECT :task_id FROM DUAL;

:TASK_ID
------------------
1590786706158-3126
```

Pour lire le fichier journal, appelez la procédure Amazon RDS `rdsadmin.rds_file_util.read_text_file`. Indiquez l'ID de tâche dans le nom du fichier. La sortie suivante montre trois incidents : 53523, 53522 et 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.
```

Pour répertorier un incident particulier, spécifiez son ID à l'aide du paramètre `incident_id`. Dans l'exemple suivant, vous interroger le fichier journal pour l'incident 53523 uniquement.

```
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.
```

Répertorier les problèmes

Pour répertorier les problèmes de diagnostic pour Oracle, utilisez la fonction Amazon RDS `rdsadmin.rdsadmin_adrci_util.list_adrci_problems`.

Par défaut, la fonction répertorie les 50 problèmes les plus récents.

Cette fonction utilise le paramètre courant `problem_id`. Pour de plus amples informations, veuillez consulter Paramètres courants pour les procédures de diagnostic (p. 1158).

Pour obtenir l'ID de tâche pour tous les problèmes, appelez la fonction `rdsadmin.rdsadmin_adrci_util.list_adrci_problems` sans argument et stockez la sortie dans une variable client SQL.

```
SQL> exec :task_id := rdsadmin.rdsadmin_adrci_util.list_adrci_problems;

PL/SQL procedure successfully completed.
```

Pour lire le fichier journal, appelez la fonction `rdsadmin.rds_file_util.read_text_file`, en fournissant l'ID de tâche dans le nom du fichier. Dans la sortie suivante, le fichier journal présente trois problèmes : 1, 2 et 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.
```

Dans l'exemple suivant, vous répertoriez uniquement le problème 3.

```
SQL> exec :task_id := rdsadmin.rdsadmin_adrci_util.list_adrci_problems(problem_id=>3);

PL/SQL procedure successfully completed.
```

Pour lire le fichier journal du problème 3, appelez `rdsadmin.rds_file_util.read_text_file`. Indiquez l'ID de tâche dans le nom du fichier.

```
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.
```

Création de packages d'incidents

Vous pouvez créer des packages d'incident à l'aide de la fonction Amazon RDS `rdsadmin.rdsadmin_adrci_util.create_adrci_package`. La sortie est un fichier .zip que vous pouvez fournir au support Oracle.

Cette fonction utilise les paramètres communs suivants :

- `problem_id`
- `incident_id`

Assurez-vous de spécifier l'un des paramètres précédents. Si vous spécifiez les deux paramètres, `incident_id` remplace `problem_id`. Pour de plus amples informations, veuillez consulter Paramètres courants pour les procédures de diagnostic (p. 1158).

Pour créer un package pour un incident spécifique, appelez la fonction Amazon RDS `rdsadmin.rdsadmin_adrci_util.create_adrci_package` avec le paramètre `incident_id`. L'exemple suivant crée un package pour l'incident 53523.

```
SQL> exec :task_id :=
 rdsadmin.rdsadmin_adrci_util.create_adrci_package(incident_id=>53523);

PL/SQL procedure successfully completed.
```

Pour lire le fichier journal, appelez le fichier `rdsadmin.rds_file_util.read_text_file`. Vous pouvez fournir l'ID de tâche dans le nom du fichier. La sortie indique que vous avez généré le package d'incidents `ORA700EVE_20200529212043_COM_1.zip`.

```
SSQL> 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.
```

Pour regrouper les données de diagnostic concernant un problème particulier, spécifiez son ID à l'aide du paramètre `problem_id`. Dans l'exemple suivant, vous regrouper les données pour le problème 3 uniquement.

```
SQL> exec :task_id := rdsadmin.rdsadmin_adrci_util.create_adrci_package(problem_id=>3);

PL/SQL procedure successfully completed.
```

Pour lire la sortie de la tâche, appelez `rdsadmin.rds_file_util.read_text_file`, en fournissant l'ID de la tâche dans le nom du fichier. La sortie indique que vous avez généré le package d'incidents `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.
```

Affichage des fichiers de trace

Vous pouvez afficher les fichiers de trace à l'aide de la fonction Amazon RDS `rdsadmin.rdsadmin_adrci_util.show_adrci_tracefile`.

Cette fonction utilise le paramètre suivant.

Nom du paramètre	Type de données	Valeurs valides	Par défaut	Obligatoire	Description
`filename`	varchar2	Un nom de fichier de trace valide	Null	Non	Si la valeur est null, la fonction affiche tous les fichiers de trace. Si elle n'est pas null, la fonction affiche le fichier spécifié.

Pour afficher le fichier trace, appelez la fonction Amazon RDS `rdsadmin.rdsadmin_adrci_util.show_adrci_tracefile` avec le paramètre `incident_id`.

```
SQL> exec :task_id := rdsadmin.rdsadmin_adrci_util.show_adrci_tracefile;

PL/SQL procedure successfully completed.
```

Pour répertorier les noms des fichiers de trace, appelez la procédure Amazon RDS `rdsadmin.rds_file_util.read_text_file`, en fournissant l'ID de tâche dans le nom du fichier.

```
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.
```

Dans l'exemple suivant, vous générez la sortie pour 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.
```

Pour lire le fichier journal, appelez `rdsadmin.rds_file_util.read_text_file`. Indiquez l'ID de tâche dans le nom du fichier. La sortie affiche les 10 premières lignes d'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_hbl2qgmh_.log
Fri May 29 00:04:10 2020

10 rows selected.
```

Autres tâches DBA courantes pour les instances de bases de données Oracle

Vous trouverez ci-dessous des informations sur la façon d'effectuer diverses tâches DBA sur vos instances de base de données Amazon RDS exécutant Oracle. Pour offrir une expérience de service géré, Amazon RDS ne fournit pas l'accès shell aux instances de base de données et limite l'accès à certaines tables et procédures système qui requièrent des privilèges avancés.

Rubriques

- Création et suppression de répertoires dans l'espace de stockage de données principal (p. 1164)
- Établissement de la liste des fichiers situés dans un répertoire d'instance de base de données (p. 1165)
- Lecture de fichiers dans un répertoire d'instance de base de données (p. 1166)
- Accès aux fichiers Opatch (p. 1166)

Création et suppression de répertoires dans l'espace de stockage de données principal

Pour créer des répertoires, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.create_directory`. Vous pouvez créer jusqu'à 10 000 répertoires, tous situés dans votre espace principal de stockage des données. Pour supprimer des répertoires, utilisez la procédure Amazon RDS `rdsadmin.rdsadmin_util.drop_directory`.

Les procédures `drop_directory` et `create_directory` ont le paramètre requis suivant.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`p_directory_name`	varchar2	—	Oui	Nom du répertoire.

L'exemple suivant crée un répertoire nommé `PRODUCT_DESCRIPTIONS`.

```
exec rdsadmin.rdsadmin_util.create_directory(p_directory_name => 'product_descriptions');
```

Le dictionnaire de données stocke le nom du répertoire en majuscules. Vous pouvez lister les répertoires en interrogeant `DBA_DIRECTORIES`. Le système choisit le nom du chemin réel de l'hôte automatiquement. L'exemple suivant récupère le chemin du répertoire nommé `PRODUCT_DESCRIPTIONS` :

```
SELECT DIRECTORY_PATH
  FROM DBA_DIRECTORIES
 WHERE DIRECTORY_NAME='PRODUCT_DESCRIPTIONS';

DIRECTORY_PATH
--------------------------------------
/rdsdbdata/userdirs/01
```

Le nom d'utilisateur maître de l'instance de base de données possède des privilèges de lecture et d'écriture dans le nouveau répertoire et peut accorder l'accès à d'autres utilisateurs. Les privilèges `EXECUTE` ne sont pas disponibles pour les répertoires sur une instance de base de données. Les répertoires sont créés dans votre espace principal de stockage des données et consomment de l'espace, ainsi que de la bande passante d'I/O.

L'exemple suivant supprime le répertoire nommé `PRODUCT_DESCRIPTIONS`.

```
exec rdsadmin.rdsadmin_util.drop_directory(p_directory_name => 'product_descriptions');
```

> **Note**
>
> Vous pouvez également supprimer un répertoire à l'aide de la commande SQL Oracle `DROP DIRECTORY`.

La suppression d'un répertoire ne supprime pas son contenu. Étant donné que la procédure `rdsadmin.rdsadmin_util.create_directory` peut réutiliser les noms de chemin, les fichiers figurant dans les répertoires supprimés peuvent apparaître dans un répertoire nouvellement créé. Avant de supprimer un répertoire, nous vous recommandons d'utiliser `UTL_FILE.FREMOVE` pour supprimer les fichiers du répertoire. Pour de plus amples informations, veuillez consulter FREMOVE Procedure dans la documentation Oracle.

Établissement de la liste des fichiers situés dans un répertoire d'instance de base de données

Pour lister les fichiers contenus dans un répertoire, utilisez la procédure Amazon RDS `rdsadmin.rds_file_util.listdir`. La procédure `listdir` comporte les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`p_directory`	varchar2	—	Oui	Nom du répertoire à lister.

L'exemple suivant répertorie les fichiers figurant dans le répertoire nommé `PRODUCT_DESCRIPTIONS`.

```
SELECT * FROM TABLE(rdsadmin.rds_file_util.listdir(p_directory => 'PRODUCT_DESCRIPTIONS'));
```

Lecture de fichiers dans un répertoire d'instance de base de données

Pour lire un fichier texte, utilisez la procédure Amazon RDS `rdsadmin.rds_file_util.read_text_file`. La procédure `read_text_file` comporte les paramètres suivants.

Nom du paramètre	Type de données	Par défaut	Obligatoire	Description
`p_directory`	varchar2	—	Oui	Nom du répertoire qui contient le fichier.
`p_filename`	varchar2	—	Oui	Nom du fichier à lire.

L'exemple suivant lit le fichier `rice.txt` dans le répertoire `PRODUCT_DESCRIPTIONS`.

```
declare
  fh sys.utl_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;
/
```

L'exemple suivant lit le fichier `rice.txt` figurant dans le répertoire `PRODUCT_DESCRIPTIONS`.

```
SELECT * FROM TABLE
    (rdsadmin.rds_file_util.read_text_file(
        p_directory => 'PRODUCT_DESCRIPTIONS',
        p_filename  => 'rice.txt'));
```

Accès aux fichiers Opatch

Opatch est un utilitaire Oracle qui permet l'application et la restauration de correctifs sur le logiciel Oracle. Le mécanisme Oracle permettant de déterminer les correctifs ayant été appliqués à une base de données est la commande `opatch lsinventory`. Pour ouvrir des demandes de service pour les clients Bring Your Own Licence (BYOL), le support Oracle demande le fichier `lsinventory` et parfois le fichier `lsinventory_detail` généré par Opatch.

Pour offrir une expérience de service géré, Amazon RDS ne fournit pas l'accès shell à Opatch. Au lieu de cela, l'instance de base de données Oracle crée automatiquement les fichiers d'inventaire toutes les heures dans le répertoire BDUMP. Vous avez accès en lecture et en écriture sur ce répertoire. Si vous ne voyez pas vos fichiers dans BDUMP, ou si les fichiers ne sont pas à jour, attendez une heure et faites une nouvelle tentative.

> **Note**
>
> Les exemples de cette section supposent que le répertoire BDUMP est nommé `BDUMP`. Sur un réplica en lecture, le nom du répertoire BDUMP est différent. Pour savoir comment obtenir le

nom BDUMP en interrogeant `V$DATABASE.DB_UNIQUE_NAME` sur un réplica en lecture, veuillez consulter Liste de fichiers (p. 516).

Les fichiers d'inventaire utilisent la convention de dénomination Amazon RDS `lsinventory-dbv.txt` et `lsinventory_detail-dbv.txt`, où *dbv* est le nom complet de votre version de base de données. Le fichier `lsinventory-dbv.txt` est disponible sur toutes les versions de base de données. Le fichier de détails correspondant est disponible sur les versions de base de données suivantes :

- 19.0.0.0, ru-2020-01.rur-2020-01.r1 ou version ultérieure
- 18.0.0.0, ru-2020-01.rur-2020-01.r1 ou version ultérieure
- 12.2.0.1, ru-2020-01.rur-2020-01.r1 ou version ultérieure
- 12.1.0.2, v19 ou ultérieure
- 11.2.0.4, v23 ou ultérieure

Par exemple, si votre version de base de données est 19.0.0.0.ru-2020-04.rur-2020-04.r1, vos fichiers d'inventaire portent les noms suivants.

```
lsinventory-19.0.0.0.ru-2020-04.rur-2020-04.r1.txt
lsinventory_detail-19.0.0.0.ru-2020-04.rur-2020-04.r1.txt
```

Assurez-vous de télécharger les fichiers qui correspondent à la version actuelle de votre moteur de base de données.

Console

Pour télécharger un fichier d'inventaire à l'aide de la console

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez le nom de l'instance de base de données qui contient le fichier journal que vous voulez consulter.
4. Choisissez l'onglet Logs & events (Journaux et événements).
5. Faites défiler jusqu'à la section Journaux.
6. Dans la section Logs (Journaux) recherchez `lsinventory`.
7. Sélectionnez le fichier auquel vous souhaitez accéder, puis choisissez Download (Télécharger).

SQL

Pour lire le fichier `lsinventory-dbv.txt` dans un client SQL, vous pouvez utiliser une instruction `SELECT`. Pour cette technique, utilisez l'une des fonctions `rdsadmin` suivantes : `rdsadmin.rds_file_util.read_text_file` ou `rdsadmin.tracefile_listing`.

Dans l'exemple de requête suivant, remplacez *dbv* par votre version de base de données Oracle. Par exemple, la version de votre base de données peut être 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

Pour lire le fichier `lsinventory-dbv.txt` dans un client SQL, vous pouvez écrire un programme PL/SQL. Ce programme utilise `utl_file` pour lire le fichier et `dbms_output` pour l'imprimer. Ce sont des packages fournis par Oracle.

Dans l'exemple de programme suivant, remplacez *dbv* par la version de votre base de données Oracle. Par exemple, la version de votre base de données peut être 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;
/
```

Ou interrogez `rdsadmin.tracefile_listing` et spoulez la sortie vers un fichier. L'exemple suivant spoule la sortie vers `/tmp/tracefile.txt`.

```
SPOOL /tmp/tracefile.txt
SELECT *
FROM   rdsadmin.tracefile_listing
WHERE  FILENAME LIKE 'lsinventory%';
SPOOL OFF;
```

Utilisation de l'authentification Kerberos avec Amazon RDS for Oracle

Vous pouvez désormais utiliser l'authentification Kerberos pour authentifier les utilisateurs lorsqu'ils se connectent à votre instance de base de données Amazon RDS qui exécute Oracle. Dans ce cas, l'nstance de base de données utilise AWS Directory Service for Microsoft Active Directory (Enterprise Edition), également appelé AWS Managed Microsoft AD, pour activer l'authentification Windows. Lorsque les utilisateurs s'authentifient avec une instance de base de données Oracle jointe au domaine d'approbation, les demandes d'authentification sont transmises à l'annuaire de domaine que vous créez avec AWS Directory Service.

Vous pouvez gagner du temps et de l'argent en conservant toutes les informations d'identification dans le même annuaire. Vous avez un endroit centralisé de stockage et de gestion des informations d'identification pour plusieurs instances de base de données. L'utilisation d'un annuaire peut également améliorer votre profil de sécurité global.

Amazon RDS prend en charge l'authentification Kerberos pour les instances de base de données Oracle dans les régions AWS suivantes :

- USA Est (Ohio)
- USA Est (Virginie du Nord)
- USA Ouest (Californie du Nord)
- USA Ouest (Oregon)

- Asie-Pacifique (Mumbai)
- Asie-Pacifique (Séoul)
- Asie-Pacifique (Singapour)
- Asie-Pacifique (Sydney)
- Asie-Pacifique (Tokyo)
- Canada (Centre)
- Europe (Francfort)
- Europe (Irlande)
- Europe (Londres)
- Europe (Stockholm)
- Amérique du Sud (São Paulo)
- AWS GovCloud (US-East)
- AWS GovCloud (USA Ouest)

> **Note**
>
> L'authentification Kerberos n'est pas prise en charge pour les classes d'instances de base de données qui sont obsolètes pour les instances de base de données Oracle. Pour plus d'informations, consultez Prise en charge des classes d'instance de base de données pour Oracle (p. 933).

Pour configurer l'authentification pour une instance de base de données Oracle, effectuez les étapes générales suivantes, décrites plus en détails par la suite :

1. Utilisez AWS Managed Microsoft AD pour créer un annuaire AWS Managed Microsoft AD. Vous pouvez utiliser AWS Management Console, AWS CLI ou l'API AWS Directory Service pour créer l'annuaire.
2. Créez un rôle AWS Identity and Access Management (IAM) qui utilise la stratégie IAM `AmazonRDSDirectoryServiceAccess` gérée. Le rôle autorise Amazon RDS à effectuer des appels vers votre annuaire.

   Pour que le rôle autorise l'accès, le point de terminaison AWS Security Token Service (AWS STS) doit être activé dans la région AWS correcte pour votre compte AWS. Les points de terminaison AWS STS sont actifs par défaut dans toutes les régions AWS et vous pouvez les utiliser sans qu'aucune autre action soit nécessaire. Pour de plus amples informations, veuillez consulter Activation et désactivation d'AWS STS dans une région AWS dans le Guide de l'utilisateur IAM.
3. Créez et configurez les utilisateurs dans l'annuaire AWS Managed Microsoft AD à l'aide des outils Microsoft Active Directory. Pour de plus amples informations sur la création des utilisateurs dans votre Microsoft Active Directory, veuillez consulter Gérer les utilisateurs et les groupes dans Microsoft AD géré par AWS dans le Guide d'administration AWS Directory Service.
4. Si vous avez l'intention de rechercher l'annuaire et l'instance de base de données dans des comptes AWS ou des VPC (Virtual Private Cloud) différents, configurez l'appairage des VPC. Pour de plus amples informations, veuillez consulter Qu'est-ce que l'appairage de VPC ? dans le Amazon VPC Peering Guide.
5. Créez ou modifiez une instance de base de données Oracle depuis la console, l'interface de ligne de commande ou l'API RDS à l'aide de l'une des méthodes suivantes :
   - Création d'une instance de base de données Amazon RDS (p. 146)
   - Modification d'une instance de base de données Amazon RDS (p. 243)
   - Restauration à partir d'un instantané de base de données (p. 329)
   - Restauration d'une instance de base de données à une date spécifiée (p. 365)

   Lorsque vous créez ou modifiez l'instance de base de données, fournissez l'identifiant de domaine (identifiant `d-*`) qui a été généré lors de la création de votre annuaire et le nom du rôle que vous avez

créé. Vous pouvez rechercher l'instance de base de données dans le même Amazon Virtual Private Cloud (VPC) que le répertoire ou dans un compte AWS ou un VPC différent.

6. Utilisez les informations d'identification de l'utilisateur principal Amazon RDS pour vous connecter à l'instance de base de données Oracle. Créez l'utilisateur dans Oracle en vue d'une identification externe. Les utilisateurs identifiés en externe peuvent se connecter à l'instance de base de données Oracle à l'aide de l'authentification Kerberos.

Pour obtenir l'authentification Kerberos à l'aide d'un compte Microsoft Active Directory sur site ou auto-géré, créez une approbation de forêt ou une approbation externe. L'approbation peut être unidirectionnelle ou bidirectionnelle. Pour de plus amples informations sur la configuration des approbations de forêt avec AWS Directory Service, veuillez consulter Quand créer une relation d'approbation dans le Guide d'administration AWS Directory Service.

Rubriques

- Configuration de l'authentification Kerberos pour les instances de base de données Oracle (p. 1170)
- Gestion d'une instance de base de données dans un domaine (p. 1179)
- Connexion à Oracle avec l'authentification Kerberos (p. 1181)

Configuration de l'authentification Kerberos pour les instances de base de données Oracle

Vous utilisez AWS Directory Service for Microsoft Active Directory (Enterprise Edition), également appelé AWS Managed Microsoft AD, pour configurer l'authentification Kerberos pour une instance de base de données Oracle. Pour configurer l'authentification Kerberos, procédez comme suit :

- Étape 1 : Créer un annuaire à l'aide d'AWS Managed Microsoft AD (p. 1170)
- Étape 2 : Créer une approbation (p. 1174)
- Étape 3 : Créer un rôle IAM pour une utilisation par Amazon RDS (p. 1174)
- Étape 4 : Créer et configurer des utilisateurs (p. 1175)
- Étape 5 : Activer le trafic entre VPC entre le répertoire et l'instance de base de données (p. 1176)
- Étape 6 : Créer ou modifier une instance de base de données Oracle (p. 1176)
- Étape 7 : Créer les connexions Oracle d'authentification Kerberos (p. 1178)
- Étape 8 : Configurer un client Oracle (p. 1178)

Étape 1 : Créer un annuaire à l'aide d'AWS Managed Microsoft AD

AWS Directory Service crée un annuaire Active Directory totalement géré dans le Cloud AWS. Lorsque vous créez un annuaire AWS Managed Microsoft AD, AWS Directory Service crée deux contrôleurs de domaine et serveurs de système de noms de domaine (DNS) en votre nom. Les serveurs de répertoire sont créés dans des sous-réseaux différents d'un VPC. Cette redondance permet de s'assurer que votre annuaire reste accessible, y compris en cas de défaillance.

Lorsque vous créez un annuaire AWS Managed Microsoft AD, AWS Directory Service effectue les tâches suivantes en votre nom :

- Configuration d'un annuaire Active Directory dans le VPC.
- Création d'un compte d'administrateur d'annuaire avec le nom d'utilisateur Admin et le mot de passe spécifié. Ce compte est utilisé pour gérer votre annuaire.

Note

Assurez-vous d'enregistrer ce mot de passe, car AWS Directory Service ne le stocke pas. Vous pouvez le réinitialiser, mais vous ne pouvez pas le récupérer.

- Création d'un groupe de sécurité pour les contrôleurs de l'annuaire.

Lorsque vous lancez un AWS Managed Microsoft AD, AWS crée une unité d'organisation (UO) qui contient tous les objets de votre annuaire. Cette unité d'organisation, qui porte le nom NetBIOS que vous avez saisi lorsque vous avez créé votre annuaire, est située dans la racine du domaine. La racine du domaine appartient à AWS, qui la gère.

Le compte Admin qui a été créé avec votre annuaire AWS Managed Microsoft AD dispose des autorisations nécessaires pour les activités administratives les plus courantes pour votre unité d'organisation :

- Création, mise à jour et suppression des utilisateurs
- Ajouter des ressources à votre domaine, comme des serveurs de fichiers ou d'impression, puis attribuer des autorisations pour ces ressources aux utilisateurs dans votre unité d'organisation
- Créer des unités d'organisation et des conteneurs supplémentaires
- Déléguer des autorités
- Restaurer des objets supprimés de la corbeille Active Directory
- Exécuter des modules AD et DNS Windows PowerShell sur le service Web Active Directory

Le compte Admin dispose également de droits pour exécuter les activités suivantes au niveau du domaine :

- Gérer les configurations DNS (ajouter, supprimer ou mettre à jour des enregistrements, des zones et des redirecteurs)
- Afficher les journaux d'événements DNS
- Afficher les journaux d'événements de sécurité

Pour créer un annuaire avec AWS Managed Microsoft AD

1. Connectez-vous à la AWS Management Console et ouvrez la console AWS Directory Service à l'adresse https://console.aws.amazon.com/directoryservicev2/.
2. Dans le panneau de navigation, choisissez Annuaires, puis Configurer un annuaire.
3. Choisissez AWS Managed Microsoft AD. AWS Managed Microsoft AD est la seule option que vous pouvez utiliser actuellement avec Amazon RDS.
4. Entrez les informations suivantes :

   Nom de DNS de l'annuaire

   Nom complet de l'annuaire, par exemple **`corp.example.com`**.

   Nom NetBIOS de l'annuaire

   Nom court de l'annuaire, par exemple **`CORP`**.

   Description de l'annuaire

   (Facultatif) Une description de l'annuaire.

   Mot de passe administrateur

   Mot de passe de l'administrateur de l'annuaire. Le processus de création d'un annuaire crée un compte d'administrateur avec le nom d'utilisateur Admin et ce mot de passe.

Le mot de passe de l'administrateur de l'annuaire ne peut pas contenir le terme « admin ». Le mot de passe est sensible à la casse et doit comporter entre 8 et 64 caractères. Il doit également contenir au moins un caractère de trois des quatre catégories suivantes :

- Lettres minuscules (a–z)
- Lettres majuscules (A–Z)
- Chiffres (0–9)
- Caractères non alphanumériques (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Confirmer le mot de passe

Saisissez à nouveau le mot de passe de l'administrateur.

5. Choisissez Suivant.
6. Entrez les informations suivantes dans la section Mise en réseau, puis choisissez Suivant :

   VPC

   VPC de l'annuaire. Créez l'instance de base de données Oracle dans ce même VPC.

   Sous-réseaux

   Sous-réseaux pour les serveurs d'annuaires. Les deux sous-réseaux doivent être dans des zones de disponibilité différentes.
7. Vérifiez les informations concernant l'annuaire et effectuez les modifications nécessaires. Lorsque les informations sont correctes, choisissez Create directory (Créer l'annuaire).

La création de l'annuaire prend plusieurs minutes. Lorsqu'il est créé, la valeur du champ Statut devient Actif.

Pour consulter les informations relatives à votre annuaire, choisissez le nom de l'annuaire dans la liste. Notez la valeur ID de l'annuaire, car vous avez besoin de cette valeur lorsque vous créez ou modifiez votre instance de base de données Oracle.

Étape 2 : Créer une approbation

Si vous envisagez d'utiliser uniquement AWS Managed Microsoft AD, passez à Étape 3 : Créer un rôle IAM pour une utilisation par Amazon RDS (p. 1174).

Pour obtenir l'authentification Kerberos à l'aide d'un compte Microsoft Active Directory sur site ou auto-géré, créez une approbation de forêt ou une approbation externe. L'approbation peut être unidirectionnelle ou bidirectionnelle. Pour de plus amples informations sur la configuration des approbations de forêts avec AWS Directory Service, veuillez consulter Quand créer une relation d'approbation ? dans le Guide d'administration AWS Directory Service.

Étape 3 : Créer un rôle IAM pour une utilisation par Amazon RDS

Pour qu'Amazon RDS appelle AWS Directory Service pour vous, il est nécessaire de disposer d'un rôle IAM qui utilise la stratégie IAM gérée `AmazonRDSDirectoryServiceAccess`. Ce rôle permet à Amazon RDS d'effectuer des appels vers AWS Directory Service.

Lorsqu'une instance de base de données est créée à l'aide de l'AWS Management Console et que l'utilisateur de la console dispose de l'autorisation `iam:CreateRole`, la console crée ce rôle automatiquement. Dans ce cas, le nom du rôle est `rds-directoryservice-kerberos-access-role`. Sinon, vous devez créer le rôle IAM manuellement. Lorsque vous créez ce rôle IAM, choisissez `Directory Service` et attachez-lui la stratégie gérée AWS `AmazonRDSDirectoryServiceAccess`.

Pour de plus amples informations sur la création de rôles IAM pour un service, veuillez consulter Création d'un rôle pour déléguer des autorisations à un service AWS dans le IAM Guide de l'utilisateur.

> **Note**
>
> Le rôle IAM utilisé pour l'authentification Windows pour RDS pour Microsoft SQL Server ne peut pas être utilisé pour RDS pour Oracle.

Vous pouvez également créer des stratégies avec les autorisations obligatoires au lieu d'utiliser la stratégie gérée IAM `AmazonRDSDirectoryServiceAccess`. Dans ce cas, le rôle IAM doit avoir la stratégie d'approbation IAM suivante :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "directoryservice.rds.amazonaws.com",
          "rds.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Le rôle doit également avoir la stratégie de rôle IAM suivante.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
    "Effect": "Allow",
    "Resource": "*"
    }
  ]
}
```

Étape 4 : Créer et configurer des utilisateurs

Vous pouvez créer des utilisateurs à l'aide de l'outil Active Directory Users and Computers, qui fait partie des outils Active Directory Domain Services et Active Directory Lightweight Directory Services. Dans ce cas, les utilisateurs sont des personnes ou des entités qui ont accès à votre annuaire.

Pour créer des utilisateurs dans un annuaire AWS Directory Service, vous devez être connecté à une instance Amazon EC2 Windows qui est membre de l'annuaire AWS Directory Service. Parallèlement, vous devez être connecté en tant qu'utilisateur disposant de privilèges pour créer des utilisateurs. Pour de plus amples informations, veuillez consulter Créer un utilisateur dans le Guide d'administration AWS Directory Service.

Étape 5 : Activer le trafic entre VPC entre le répertoire et l'instance de base de données

Si vous avez l'intention de rechercher l'annuaire et l'instance de base de données dans le même VPC, ignorez cette étape et passez à Étape 6 : Créer ou modifier une instance de base de données Oracle (p. 1176).

Si vous avez l'intention de rechercher l'annuaire et l'instance de base de données dans des VPC différents, configurez le trafic entre VPC à l'aide de l'appairage de VPC ou à l'aide de AWS Transit Gateway.

La procédure suivante active le trafic entre les VPC à l'aide de l'appairage de VPC. Suivez les instructions de Qu'est-ce que l'appairage de VPC ? dans le Guide de l'appairage Amazon Virtual Private Cloud.

Pour activer le trafic entre VPC à l'aide de l'appairage de VPC

1. Configurez les règles de routage de VPC appropriées afin de veiller à ce que le trafic réseau puisse être acheminé dans les deux sens.
2. Assurez-vous que le groupe de sécurité de l'instance de base de données puisse recevoir le trafic entrant depuis le groupe de sécurité de cet annuaire.
3. Assurez-vous qu'il n'existe aucune règle de liste de contrôle d'accès (ACL) pour bloquer le trafic.

Si un autre compte AWS possède l'annuaire, vous devez le partager.

Pour partager l'annuaire entre des comptes AWS

1. Commencez le partage de l'annuaire avec le compte AWS dans lequel l'instance de base de données sera créée en suivant les instructions du Didacticiel : Partage de votre annuaire AWS Managed Microsoft AD pour la jonction de domaines EC2 en toute transparence dans le Guide d'administration AWS Directory Service.
2. Connectez-vous à la console AWS Directory Service à l'aide du compte pour l'instance de base de données et assurez-vous que l'état du domaine est `SHARED` avant de poursuivre.
3. Lorsque vous êtes connecté à la console AWS Directory Service avec le compte de l'instance de base de données, notez la valeur de ID de l'annuaire. Vous utilisez cet ID pour joindre l'instance de base de données au domaine.

Étape 6 : Créer ou modifier une instance de base de données Oracle

Créez ou modifiez une instance de base de données Oracle en vue de son utilisation avec votre annuaire. Vous pouvez utiliser la console, l'interface de ligne de commande ou l'API RDS pour associer une instance de base de données à un annuaire. Vous pouvez effectuer cette opération de différentes manières :

- Créez une instance de base de données Oracle à l'aide de la console, de l'interface de ligne de commande create-db-instance ou de l'opération d'API RDS CreateDBInstance.

  Pour obtenir des instructions, consultez Création d'une instance de base de données Amazon RDS (p. 146).
- Créez une instance de base de données Oracle à l'aide de la console, de l'interface de ligne de commande modify-db-instance ou de l'opération d'API RDS ModifyDBInstance.

  Pour obtenir des instructions, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

- Restaurez une instance de base de données Oracle à partir d'un instantané de base de données à l'aide de la console, de la commande d'interface de ligne de commande restore-db-instance-from-db-snapshot ou de l'opération d'API RDS RestoreDBInstanceFromDBSnapshot.

  Pour obtenir des instructions, consultez Restauration à partir d'un instantané de base de données (p. 329).
- Restaurez une instance de base de données Oracle à un moment donné en utilisant la console, la commande d'interface de ligne de commande restore-db-instance-to-point-in-time ou l'opération d'API RDS RestoreDBInstanceToPointInTime.

  Pour obtenir des instructions, consultez Restauration d'une instance de base de données à une date spécifiée (p. 365).

L'authentification Kerberos est uniquement prise en charge pour les instances de base de données Oracle dans un VPC. L'instance de base de données peut être dans le même VPC que l'annuaire ou dans un VPC différent. L'instance de base de données doit utiliser un groupe de sécurité qui accepte les sorties du VPC, afin que l'instance de base de données puisse communiquer avec l'annuaire.

Lorsque vous utilisez la console pour créer une instance de base de données, choisissez Mot de passe et authentification Kerberos dans la section Authentification de base de données. Choisissez Parcourir les annuaires, puis sélectionnez l'annuaire, ou choisissez Créer un nouvel annuaire.

Lorsque vous utilisez la console pour modifier ou restaurer une instance de base de données, choisissez l'annuaire dans la section Authentification Kerberos ou choisissez Créer un nouvel annuaire.

Lorsque vous utilisez AWS CLI, les paramètres suivants sont obligatoires pour que l'instance de base de données puisse utiliser l'annuaire que vous avez créé :

- Pour le paramètre `--domain`, vous devez indiquer l'identifiant du domaine (identifiant « d-* ») généré lors de la création de l'annuaire.
- Pour le paramètre `--domain-iam-role-name`, utilisez le rôle que vous avez créé qui utilise la stratégie IAM gérée `AmazonRDSDirectoryServiceAccess`.

Par exemple, la commande d'interface de ligne de commande suivante modifie une instance de base de données de façon à utiliser un annuaire.

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --domain d-ID \
    --domain-iam-role-name role-name
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --domain d-ID ^
    --domain-iam-role-name role-name
```

> **Important**
>
> Si vous modifiez une instance de base de données de façon à activer l'authentification Kerberos, redémarrez l'instance de base de données après avoir effectué la modification.

Étape 7 : Créer les connexions Oracle d'authentification Kerberos

Utilisez les informations d'identification de l'utilisateur principal Amazon RDS pour vous connecter à l'instance de base de données Oracle comme vous le faites pour n'importe quelle instance de base de données. L'instance de base de données est jointe au domaine AWS Managed Microsoft AD. Vous pouvez ainsi mettre en service les connexions et utilisateurs Oracle depuis les utilisateurs et groupes Microsoft Active Directory de votre domaine. Pour gérer les autorisations de base de données, vous pouvez octroyer et annuler les autorisations Oracle standard pour ces connexions.

Pour autoriser un utilisateur Microsoft Active Directory à s'authentifier avec Oracle, utilisez les informations d'identification de l'utilisateur principal Amazon RDS. Vous utilisez les informations d'identification pour vous connecter à l'instance de base de données Oracle de la même manière que pour vous connecter à n'importe quelle instance de base de données. Après vous être connecté, créez un utilisateur authentifié en externe dans Oracle.

```
CREATE USER "KRBUSER@CORP.EXAMPLE.COM" IDENTIFIED EXTERNALLY;
GRANT CREATE SESSION TO "KRBUSER@CORP.EXAMPLE.COM";
```

Remplacez *KRBUSER@CORP.EXAMPLE.COM* par le nom d'utilisateur et le nom de domaine. Les utilisateurs (personnes et applications) de votre domaine peuvent désormais se connecter à l'instance Oracle RDS à partir d'un ordinateur client joint au domaine à l'aide de l'authentification Kerberos.

Étape 8 : Configurer un client Oracle

Pour configurer un client Oracle, vous devez vous conformer aux exigences suivantes :

- Créez un fichier krb5.conf (ou équivalent) pointant vers le domaine. Configurez le client Oracle pour utiliser le fichier krb5.conf.

- Vérifiez que le trafic peut circuler entre l'hôte du client et AWS Directory Service via le port 53 DNS et les ports Kerberos (88 et 464 pour AWS Directory Service géré) via TCP/UDP.
- Vérifiez que le trafic peut circuler entre l'hôte du client et l'instance de base de données via le port de la base de données.

Vous trouverez ci-après un exemple de contenu krb5.conf pour AWS Managed Microsoft AD :

```
[libdefaults]
 default_realm = EXAMPLE.COM
 default_ccache_name = /tmp/kerbcache
[realms]
 EXAMPLE.COM = {
  kdc = example.com
  admin_server = example.com
 }
[domain_realm]
 .example.com = EXAMPLE.COM
 example.com = EXAMPLE.COM
```

Vous trouverez ci-après un exemple de contenu krb5.conf pour Microsoft AD sur site :

```
[libdefaults]
 default_realm = EXAMPLE.COM
 default_ccache_name = /tmp/kerbcache
[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
```

Vous trouverez ci-après un exemple de contenu sqlnet.ora pour une configuration SQL*Plus :

```
SQLNET.AUTHENTICATION_SERVICES=(KERBEROS5PRE,KERBEROS5)
SQLNET.KERBEROS5_CONF=path_to_krb5.conf_file
```

Pour obtenir un exemple de configuration SQL Developer, veuillez consulter Document 1609359.1 sur le support Oracle.

Gestion d'une instance de base de données dans un domaine

Vous pouvez utiliser la console, l'interface de ligne de commande ou l'API RDS pour gérer votre instance de base de données et sa relation avec votre Microsoft Active Directory. Par exemple, vous pouvez associer un Microsoft Active Directory de façon à activer l'authentification Kerberos. Vous pouvez également annuler l'association d'un Microsoft Active Directory pour désactiver l'authentification Kerberos. Vous pouvez également transférer une instance de base de données vers une autre afin qu'elle soit authentifiée en externe par un Microsoft Active Directory.

Par exemple, l'interface de ligne de commande vous permet d'effectuer les actions suivantes :

- Pour retenter l'activation de l'authentification Kerberos en cas d'échec d'appartenance, utilisez la commande d'interface de ligne de commande modify-db-instance et spécifiez l'ID d'annuaire d'appartenance actuelle pour l'option `--domain`.
- Pour désactiver l'authentification Kerberos sur une instance de base de données, utilisez la commande d'interface de ligne de commande modify-db-instance et spécifiez `none` pour l'option `--domain`.
- Pour transférer une instance de base de données d'un domaine vers un autre, utilisez la commande d'interface de ligne de commande modify-db-instance et spécifiez l'identifiant du nouveau domaine pour l'option `--domain`.

Adhésion au domaine

Après la création ou la modification de votre instance de base de données, cette dernière devient un membre du domaine. Vous pouvez consulter le statut de l'appartenance au domaine pour l'instance de base de données dans la console ou en exécutant la commande d'interface de ligne de commande describe-db-instances. Le statut de l'instance de base de données peut avoir les valeurs suivantes :

- `kerberos-enabled` – L'instance de base de données a l'authentification Kerberos activée.
- `enabling-kerberos` – AWS est en train d'activer l'authentification Kerberos sur cette instance de base de données.
- `pending-enable-kerberos` – L'activation de l'authentification Kerberos est en attente sur cette instance de base de données.
- `pending-maintenance-enable-kerberos` – AWS tentera d'activer l'authentification Kerberos sur cette instance de base de données lors de la prochaine fenêtre de maintenance planifiée.
- `pending-disable-kerberos` – La désactivation de l'authentification Kerberos est en attente sur cette instance de base de données.
- `pending-maintenance-disable-kerberos` – AWS tentera de désactiver l'authentification Kerberos sur cette instance de base de données lors de la prochaine fenêtre de maintenance planifiée.
- `enable-kerberos-failed` – Un problème de configuration a empêché AWS d'activer l'authentification Kerberos sur l'instance de base de données. Corrigez le problème de configuration avant de réémettre la commande de modification de l'instance de base de données.
- `disabling-kerberos` – AWS est en train de désactiver l'authentification Kerberos sur cette instance de base de données.

Une demande d'activation de l'authentification Kerberos peut échouer à cause d'un problème de connectivité réseau ou d'un rôle IAM incorrect. Si la tentative d'activation de l'authentification Kerberos échoue lorsque vous créez ou modifiez une instance de base de données, vérifiez d'abord que vous utilisez le rôle IAM correct. Ensuite, modifiez l'instance de base de données pour rejoindre le domaine.

> **Note**
>
> Seule l'authentification Kerberos avec Amazon RDS for Oracle envoie le trafic aux serveurs DNS du domaine. Toutes les autres demandes DNS sont traitées comme un accès réseau sortant sur vos instances de bases de données exécutant Oracle. Pour de plus amples informations sur l'accès réseau sortant avec Amazon RDS for Oracle, veuillez consulter Configuration d'un serveur DNS personnalisé (p. 1114).

Clés Kerberos à rotation forcée

Une clé secrète est partagée entre un AWS Managed Microsoft AD et une instance de base de données Amazon RDS pour Oracle. Cette clé subit une rotation automatique tous les 45 jours. Vous pouvez utiliser la procédure Amazon RDS suivante pour forcer la rotation de cette clé.

```
SELECT rdsadmin.rdsadmin_kerberos_auth_tasks.rotate_kerberos_keytab AS TASK_ID FROM DUAL;
```

> **Note**
>
> Dans une configuration de réplica en lecture, cette procédure est uniquement disponible sur l'instance de base de données source et non sur le réplica en lecture.

L'instruction `SELECT` renvoie l'ID de la tâche dans un type de données `VARCHAR2`. Vous pouvez consulter le statut d'une tâche en cours dans un fichier bdump. Les fichiers bdump se trouvent dans le répertoire `/rdsdbdata/log/trace`. Chaque nom de fichier bdump a le format suivant.

```
dbtask-task-id.log
```

Vous pouvez afficher le résultat en affichant le fichier de sortie de la tâche.

```
SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP','dbtask-task-
id.log'));
```

Remplacez *`task-id`* par l'ID de tâche renvoyé par la procédure.

> **Note**
>
> Les tâches sont exécutées de manière asynchrone.

Connexion à Oracle avec l'authentification Kerberos

Cette section suppose que vous avez configuré votre client Oracle comme décrit dans Étape 8 : Configurer un client Oracle (p. 1178). Pour vous connecter à la base de données Oracle avec l'authentification Kerberos, connectez-vous à l'aide du type d'authentification Kerberos. Par exemple, après avoir lancé Oracle SQL Developer, choisissez Authentification Kerberos comme type d'authentification, comme indiqué ci-après.

Pour vous connecter à Oracle avec l'authentification Kerberos avec SQL*Plus :

1. A partir d'une invite de commande, exécutez la commande suivante :

```
kinit username
```

Remplacez `username` par le nom d'utilisateur puis, à l'invite, entrez le mot de passe stocké dans le Microsoft Active Directory pour l'utilisateur.

2. Ouvrez SQL*Plus et connectez-vous à l'aide du nom et du numéro de port DNS pour l'instance de base de données Oracle.

   Pour de plus amples informations sur la connexion à l'instance de base de données Oracle dans SQL*Plus, veuillez consulter Connexion à votre instance de base de données à l'aide de SQL*Plus (p. 966).

Outils et des logiciels tiers pour les instances de base de données Oracle

Cette section fournit des informations sur les outils et les logiciels tiers pour les instances de bases de données Oracle sur Amazon RDS.

Rubriques

- Configuration de Amazon RDS pour héberger des outils et des logiciels tiers pour Oracle (p. 1182)
- Utilisation d'Oracle GoldenGate avec Amazon RDS (p. 1188)
- Utilisation de l'utilitaire Oracle Repository Creation Utility sur Amazon RDS pour Oracle (p. 1200)
- Installation d'une base de données Siebel sur Oracle sur Amazon RDS (p. 1205)

Configuration de Amazon RDS pour héberger des outils et des logiciels tiers pour Oracle

Vous pouvez utiliser Amazon RDS pour héberger une instance de base de données Oracle qui prend en charge des logiciels et des composants tels que les éléments suivants :

- Gestion des relations client Siebel (CRM)
- Oracle Fusion Middleware Metadata, installé par le Repository Creation Utility (RCU)

Les procédures suivantes vous permettent de créer une instance de base de données Oracle sur Amazon RDS que vous pouvez utiliser pour héberger des logiciels et des composants supplémentaires pour Oracle.

Création d'une instance &VPC à utiliser avec une base de données Oracle

Au cours de la procédure suivante, vous créez un Virtual Private Cloud (VPC) basé sur le service Amazon VPC, un sous-réseau privé et un groupe de sécurité. Votre instance de base de données Amazon RDS doit être disponible seulement pour vos composants intermédiaires et non pour l'internet public. Par conséquent, votre instance de base de données Amazon RDS est hébergée dans un sous-réseau privé, offrant une sécurité supérieure.

Pour créer un VPC basé sur Amazon VPC

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le coin supérieur droit d'AWS Management Console, choisissez la région AWS pour votre VPC. Cet exemple utilise la région USA Ouest (Oregon).

3. Dans le coin supérieur gauche, choisissez VPC Dashboard (Tableau de bord VPC), puis Start VPC Wizard (Démarrer l'assistant VPC).
4. Sur la page Step 1: Select a VPC Configuration (Étape 1 : Sélectionner une configuration de VPC), choisissez VPC with Public and Private Subnets (VPC avec sous-réseaux publics et privés), puis Select (Sélectionner).
5. Sur la page Step 2: VPC with Public and Private Subnets (Étape 2 : VPC avec sous-réseaux publics et privés), illustrée ci-après, définissez les valeurs suivantes :

Option	Value
Bloc d'adresse CIDR IPv4	`10.0.0.0/16` Pour plus d'informations sur la sélection de blocs d'adresses CIDR pour votre VPC, consultez la page Dimensionnement VPC.
Bloc d'adresse CIDR IPv6	Pas de bloc d'adresse CIDR IPv6
VPC name	Le nom de votre VPC, par exemple **`vpc-1`**.
CIDR de sous-réseau public IPv4	`10.0.0.0/24` Pour plus d'informations sur le dimensionnement de sous-réseau, consultez la page Dimensionnement de sous-réseau.
Zone de disponibilité	Zone de disponibilité pour votre région AWS.
Nom de sous-réseau public	Nom de votre sous-réseau public, par exemple **`subnet-public-1`**.
CIDR de sous-réseau privé IPv4	`10.0.1.0/24` Pour plus d'informations sur le dimensionnement de sous-réseau, consultez la page Dimensionnement de sous-réseau.
Zone de disponibilité	Zone de disponibilité pour votre région AWS.
Nom de sous-réseau privé	Nom de votre sous-réseau privé, par exemple **`subnet-private-1`**.
Type d'instance	Type d'instance pour votre instance NAT, par exemple `t2.small`. Note Si la zone Type d'instance n'apparaît pas dans la console, choisissez Use a NAT instance instead (Utiliser plutôt une instance NAT).
Nom de la paire de clés	`No key pair`
Points de terminaison de service	`None`
Enable DNS hostnames	`Yes`
Hardware tenancy	`Default`

6. Sélectionnez Create VPC (Créer un VPC).

Une instance de base de données Amazon RDS dans un VPC nécessite au moins deux sous-réseaux privés ou au moins deux sous-réseaux publics, pour prendre en charge le déploiement Multi-AZ. Pour plus d'informations sur l'utilisation de plusieurs zones de disponibilité, consultez Régions, zones de disponibilité et zones locales (p. 39). Étant donné que votre base de données est privée, ajoutez un second sous-réseau privé à votre VPC.

Pour créer un sous-réseau supplémentaire

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le coin supérieur droit de la AWS Management Console, confirmez que vous êtes dans la région AWS correcte pour votre VPC.

3. Dans le coin supérieur gauche, sélectionnez VPC Dashboard (Tableau de bord VPC), choisissez Sous-réseaux, puis Créer sous-réseau.
4. Sur la page Create Subnet (Créer le sous-réseau), définissez les valeurs suivantes.

Option	Valeur
Name tag	Nom de votre deuxième sous-réseau privé, par exemple **`subnet-private-2`**.
VPC	Votre VPC, par exemple **`vpc-1`**.
Zone de disponibilité	Zone de disponibilité pour votre région AWS. Note Choisissez une zone de disponibilité différente de celle que vous avez choisie pour le premier sous-réseau privé.
CIDR block	`10.0.2.0/24`

5. Choisissez Yes, Create.

Les deux sous-réseaux privés doivent utiliser la même table de routage. Dans la procédure suivante, vérifiez que les tables de routage correspondent, et si non, vous modifiez l'une d'entre elles.

Pour s'assurer que les sous-réseaux utilisent la même table de routage.

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le coin supérieur droit de la AWS Management Console, confirmez que vous êtes dans la région AWS correcte pour votre VPC.
3. Dans le coin supérieur gauche, sélectionnez VPC Dashboard (Tableau de bord VPC), choisissez Sous-réseaux, puis choisissez votre premier sous-réseau privé, par exemple **`subnet-private-1`**.
4. Au bas de la console, sélectionnez l'onglet Route Table (Tableau de routage), illustré ci-dessous.

5. Prenez note de la table de routage, par exemple `rtb-0d9fc668`.
6. Dans la liste des sous-réseaux, sélectionnez le second sous-réseau privé, par exemple **`subnet-private-2`**.
7. En bas de la console, sélectionnez l'onglet Route Table (Tableau de routage).
8. Si la table de routage du second sous-réseau n'est pas la même que la table de routage du premier sous-réseau, modifiez-la pour qu'elle corresponde :

a. Choisissez Edit.
b. Pour Change to (Remplacer par), sélectionnez la table de routage qui correspond à votre premier sous-réseau.
c. Choisissez Save (Enregistrer).

Un groupe de sécurité agit en tant que pare-feu virtuel pour votre instance de base de données afin de contrôler le trafic entrant et sortant. Dans la procédure suivante, vous créez un groupe de sécurité pour votre instance de base de données. Pour plus d'informations sur les groupes de sécurité, consultez la page Groupes de sécurité pour votre VPC.

Pour créer un groupe de sécurité VPC pour une instance de base de données Amazon RDS privée

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le coin supérieur droit de la AWS Management Console, confirmez que vous êtes dans la région AWS correcte pour votre VPC.
3. Dans le coin supérieur gauche, choisissez successivement VPC Dashboard (Tableau de bord VPC), Security Groups (Groupes de sécurité) et Create Security Group (Créer groupe de sécurité).
4. Sur la page Create Security Group (Créer un groupe de sécurité), définissez les valeurs suivantes.

Option	Valeur
Name tag	Nom de votre groupe de sécurité, par exemple **`sgdb-1`**.
Nom du groupe	Nom de votre groupe de sécurité, par exemple **`sgdb-1`**.
Description	Description de votre groupe de sécurité.
VPC	Votre VPC, par exemple **`vpc-1`**.

5. Choisissez Yes, Create.

Dans la procédure suivante, vous ajoutez des règles à votre groupe de sécurité pour contrôler le trafic entrant vers votre instance de base de données. Pour plus d'informations sur la modification de règles entrantes, consultez Règles des groupes de sécurité.

Pour ajouter des règles entrantes au groupe de sécurité

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le coin supérieur droit de la AWS Management Console, confirmez que vous êtes dans la région AWS correcte pour votre VPC.
3. Dans le coin supérieur gauche, sélectionnez VPC Dashboard (Tableau de bord VPC), choisissez Security Groups (Groupes de sécurité), puis choisissez votre groupe de sécurité, par exemple **`sgdb-1`**.
4. En bas de la console, sélectionnez l'onglet Inbound Rules (Règles entrantes), puis Modifier.
5. Définissez ces valeurs, comme illustré ci-après.

Option	Valeur
Type	`Oracle (1521)`

Option	Valeur
Protocole	`TCP (6)`
Plage de ports	1521
Source	Identifiant de votre groupe de sécurité. Lorsque vous choisissez la zone, vous voyez le nom de votre groupe de sécurité, par exemple **`sgdb-1`**.

6. Choisissez Enregistrer.

Création d'une instance de base de données Oracle

Vous pouvez utiliser Amazon RDS pour héberger une instance de base de données Oracle. Lorsque vous créez la nouvelle instance de base de données, spécifiez le VPC et le groupe de sécurité que vous avez crées précédemment à l'aides des instructions dans Création d'une instance &VPC à utiliser avec une base de données Oracle (p. 1182). Choisissez également Non pour Accessible publiquement.

Pour de plus amples informations sur la création d'une instance de base de données, veuillez consulter Création d'une instance de base de données Amazon RDS (p. 146).

Interfaces Amazon RDS supplémentaires

Dans les procédures précédentes, nous utilisons la AWS Management Console pour effectuer des tâches. Amazon Web Services fournit également le AWS Command Line Interface (AWS CLI) et une interface de programmation d'application. Vous pouvez utiliser l'AWS CLI ou l'API pour automatiser un grand nombre de tâches de gestion de Amazon RDS, y compris des tâches permettant de gérer une instance de base de données Oracle avec Amazon RDS.

Pour plus d'informations, consultez la Référence AWS Command Line Interface pour Amazon RDS et Amazon RDS API Reference.

Voir aussi

- Configuration pour Amazon RDS (p. 62)
- Utilisation de l'utilitaire Oracle Repository Creation Utility sur Amazon RDS pour Oracle (p. 1200)
- Installation d'une base de données Siebel sur Oracle sur Amazon RDS (p. 1205)
- Scénarios d'accès à une instance de base de données d'un VPC (p. 1613)
- Connexion à une instance de base de données Oracle (p. 961)

Utilisation d'Oracle GoldenGate avec Amazon RDS

Oracle GoldenGate (GoldenGate) permet de collecter, de répliquer et de gérer les données transactionnelles entre des bases de données. Il s'agit d'un package logiciel de réplication et de capture de données modifiées basé sur les journaux utilisé avec les bases de données Oracle pour les systèmes de traitement transactionnel en ligne (OLTP). GoldenGate crée des fichiers de suivi qui contiennent les dernières données modifiées de la base de données source, puis les publie sur la base de données cible. Vous pouvez utiliser GoldenGate avec Amazon RDS pour la réplication de base de données Active-Active, la migration et les mises à niveau sans interruption, la reprise après sinistre, la protection des données et la réplication intra-région et entre régions.

Lorsque vous travaillez avec GoldenGate sur Amazon RDS, prenez en compte les points suivants :

- Vous êtes responsable de la configuration et de la gestion de GoldenGate afin de l'utiliser avec Amazon RDS.
- Vous êtes responsable de la gestion des licences GoldenGate (BYOL, Réutilisez vos licences) afin de l'utiliser avec Amazon RDS dans toutes les régions AWS. Pour plus d'informations, consultez Options de licence Oracle (p. 930).
- Amazon RDS prend en charge GoldenGate pour Oracle Database Standard Edition Two (SE2), Standard Edition One (SE1), Standard Edition (SE) et Enterprise Edition (EE).
- Amazon RDS prend en charge GoldenGate pour les versions de base de données 11.2.0.4, 12.1.0.2, 12.2.0.1, 18.0.0.0 et 19.0.0.
- Amazon RDS prend en charge GoldenGate versions 11.2.1 et ultérieures.
- Amazon RDS prend en charge la migration et la réplication sur des bases de données Oracle à l'aide de GoldenGate. Nous ne prenons pas en charge, ni n'empêchons les migrations ou les réplications client entre des bases de données hétérogènes.
- Vous pouvez utiliser GoldenGate sur des instances de bases de données Oracle Amazon RDS qui utilisent Oracle TDE (Transparent Data Encryption). Pour préserver l'intégrité des données répliquées, vous devez configurer le chiffrement sur le hub GoldenGate à l'aide de volumes chiffrés EBS ou du chiffrement des fichiers de suivi. Vous devez également configurer le chiffrement pour les données envoyées entre le hub GoldenGate et les instances de base de données source et cible. Les instances de base de données Oracle Amazon RDS prennent en charge le chiffrement avec Oracle Secure Sockets Layer (SSL) (p. 1068) ou Oracle NNE (Native Network Encryption) (p. 1062).
- GoldenGate DDL est pris en charge avec les versions GoldenGate 12.1 et ultérieures lorsque vous utilisez le mode capture intégré.

Présentation

L'architecture GoldenGate à utiliser avec Amazon RDS se compose de trois modules découplés. La base de données source peut être au choix une base de données Oracle sur site, une base de données Oracle sur une instance Amazon EC2 ou une base de données Oracle sur une instance de base de données Amazon RDS. Vous travaillez également avec un hub GoldenGate, qui déplace les informations de transaction de la base de données source vers la base de données cible. Votre hub peut être l'un des suivants :

- Une instance Amazon EC2 sur laquelle Oracle Database et GoldenGate sont installés
- Une installation Oracle sur site.

Vous pouvez avoir plus d'un hub Amazon EC2, et nous vous recommandons d'utiliser deux hubs si vous utilisez GoldenGate pour une réplication inter-régions.

Votre base de données cible peut se trouver sur une instance de base de données Amazon RDS, une instance Amazon EC2 ou un emplacement sur site.

GoldenGate sur Amazon RDS prend en charge les scénarios courants suivants :

Scénario 1 : Une base de données source Oracle sur site et un hub GoldenGate sur site qui fournit les données à une instance de base de données Amazon RDS cible.

Scénario 2 : Une base de données Oracle sur site qui agit comme la base de données source, connectée à un hub d'instance Amazon EC2 qui fournit des données à une instance de base de données Amazon RDS cible.

Scénario 3 : Une base de données Oracle sur une instance de base de données Amazon RDS qui agit comme la base de données source, connectée à un hub d'instance Amazon EC2 qui fournit des données à une instance de base de données Amazon RDS cible.

Scénario 4 : Une base de données Oracle sur une instance Amazon EC2 qui agit comme la base de données source, connectée à un hub d'instance Amazon EC2 qui fournit des données à une instance de base de données Amazon RDS cible.

Scénario 5 : Une base de données Oracle sur une instance de base de données Amazon RDS connectée à un hub d'instance Amazon EC2 dans la même région AWS. Dans ce scénario, le hub est connecté à un hub d'instance Amazon EC2 d'une autre région AWS. Ce second hub fournit des données à l'instance de base de données cible Amazon RDS dans la même région AWS que le second hub d'instance Amazon EC2.

Note

Tout problème ayant un impact sur l'exécution de GoldenGate dans un environnement sur site aura également un impact sur l'exécution de GoldenGate sur AWS. Nous vous recommandons fortement de surveiller le hub GoldenGate afin de vous assurer que les valeurs `EXTRACT` et `REPLICAT` sont reprises en cas de basculement. Du fait que le hub GoldenGate est exécuté sur une instance Amazon EC2, Amazon RDS ne gère pas le hub GoldenGate et ne peut pas garantir qu'il soit en cours d'exécution.

Vous pouvez utiliser GoldenGate avec Amazon RDS pour mettre à niveau vers des versions majeures d'Oracle. Par exemple, vous pouvez utiliser GoldenGate avec Amazon RDS pour mettre à niveau une base de données Oracle version 8 sur site vers une base de données Oracle exécutant la version 11.2.0.4 sur une instance de base de données Amazon RDS.

Pour configurer GoldenGate en utilisant Amazon RDS, vous configurez le hub sur l'instance Amazon EC2, puis vous configurez les bases de données source et cible. Les étapes suivantes montrent comment configurer GoldenGate pour une utilisation avec Amazon RDS. Chaque étape est expliquée en détail dans les sections suivantes :

- Configuration d'un hub GoldenGate sur Amazon EC2 (p. 1191)
- Configuration d'une base de données source à utiliser avec GoldenGate sur Amazon RDS (p. 1192)
- Configuration d'une base de données cible à utiliser avec GoldenGate sur Amazon RDS (p. 1196)
- Utilisation des utilitaires EXTRACT et REPLICAT de GoldenGate (p. 1197)

Configuration d'un hub GoldenGate sur Amazon EC2

Pour créer un hub GoldenGate sur une instance Amazon EC2, vous devez suivre plusieurs étapes. Commencez par créer une instance Amazon EC2 avec une installation complète d'Oracle DBMS. Pour Oracle version 11.2.0.4, vous installez le correctif 13328193. L'instance Amazon EC2 doit également avoir le logiciel Oracle GoldenGate installé. Les versions exactes du logiciel dépendent des versions de base de données source et cible. Pour de plus amples informations sur l'installation de GoldenGate, veuillez consulter la Documentation d'Oracle.

L'instance Amazon EC2 qui sert de hub GoldenGate stocke et traite les informations de transaction de la base de données source dans des fichiers de suivi. Pour pouvoir prendre en charge ce processus,

assurez-vous que vous disposez de suffisamment de stockage alloué pour stocker les fichiers de suivi. Vérifiez également que l'instance Amazon EC2 dispose d'une puissance de traitement suffisante pour gérer la quantité de données traitées. En outre, assurez-vous que l'instance EC2 dispose de suffisamment de mémoire pour stocker les informations de transaction avant qu'elles ne soient écrites dans le fichier de suivi.

Les tâches suivantes configurent un hub GoldenGate sur une instance Amazon EC2. Chaque tâche est expliquée en détail dans cette section :

1. Créer les sous-répertoires GoldenGate.
2. Mettre à jour le fichier de paramètres GLOBALS.
3. Configurer le fichier mgr.prm et démarrer le gestionnaire.

Créez ensuite des sous-répertoires dans le répertoire GoldenGate en utilisant le shell de ligne de commande Amazon EC2 et ggsci, l'interpréteur de commandes GoldenGate. Les sous-répertoires sont créés sous le répertoire gg et incluent des répertoires pour des fichiers de point de contrôle, de rapport et de paramètres.

```
prompt$ cd /gg
prompt$ ./ggsci
  GGSCI> CREATE SUBDIRS
```

Créez un fichier de paramètres GLOBALS en utilisant l'interpréteur de ligne de commande Amazon EC2. Les paramètres qui affectent tous les processus GoldenGate sont définis dans le fichier de paramètres GLOBALS. L'exemple suivant crée le fichier nécessaire :

```
$ cd $GGHOME
$ vi GLOBALS
CheckpointTable oggadm1.oggchkpt
```

La dernière étape dans la configuration du hub GoldenGate consiste à configurer le manager (gestionnaire). Ajoutez les lignes suivantes au fichier mgr.prm, puis démarrez le manager (manager) en utilisant ggsci:

```
PORT 8199
PurgeOldExtracts ./dirdat/*, UseCheckpoints, MINKEEPDAYS 5
```

```
GGSCI>  start mgr
```

Une fois ces étapes réalisées, le hub GoldenGate est prêt à être utilisé. Vous configurez ensuite les bases de données source et cible.

Configuration d'une base de données source à utiliser avec GoldenGate sur Amazon RDS

Lorsque votre base de données source exécute la version 11.2.0.4, ou une version ultérieure, vous devez accomplir les tâches suivantes pour configurer une base de données source à utiliser avec GoldenGate :

1. Définissez le paramètre `compatible` sur 11.2.0.4, ou une version ultérieure.
2. Définissez le paramètre `ENABLE_GOLDENGATE_REPLICATION` sur True. Ce paramètre active la journalisation supplémentaire pour la base de données source. Si votre base de données source est sur une instance de base de données Amazon RDS, vérifiez que vous disposez d'un groupe de paramètres affecté à l'instance de base de données avec le paramètre `ENABLE_GOLDENGATE_REPLICATION` défini

sur true. Pour plus d'informations sur le paramètre `ENABLE_GOLDENGATE_REPLICATION`, consultez la documentation Oracle.

3. Définissez la période de conservation pour les journaux redo archivés pour la base de données source GoldenGate.
4. Créez un compte utilisateur GoldenGate sur la base de données source.
5. Accordez les privilèges nécessaires à l'utilisateur GoldenGate.
6. Ajoutez un alias TNS pour la base de données source au fichier `tnsnames.ora` sur le hub GoldenGate.

Définir COMPATIBLE sur la base de données source

Vérifiez que le paramètre d'initialisation `COMPATIBLE` de la base de données source est défini sur 11.2.0.4 ou version ultérieure. Si vous utilisez une base de données Oracle sur une instance de base de données Amazon RDS comme source, vérifiez que vous disposez d'un groupe de paramètres avec le paramètre `COMPATIBLE` défini sur 11.2.0.4 ou version ultérieure associé à l'instance de base de données. Si vous modifiez le paramètre `COMPATIBLE` dans un groupe de paramètres associé à l'instance de base de données, la modification requiert un redémarrage d'instance.

Vous pouvez utiliser les commandes d'interface de ligne de commande Amazon RDS suivantes pour créer un groupe de paramètres et définir le paramètre `COMPATIBLE`. Veillez à associer le nouveau groupe de paramètres à l'instance de base de données source.

Pour Linux, macOS ou Unix :

```
aws rds create-db-parameter-group \
    --db-parameter-group-name example-goldengate \
    --description "Parameters to allow GoldenGate" \
    --db-parameter-group-family oracle-ee-11.2

aws rds modify-db-parameter-group \
    --db-parameter-group-name example-goldengate \
    --parameters "ParameterName=compatible, ParameterValue=11.2.0.4, ApplyMethod=pending-
reboot"

aws rds modify-db-instance \
    --db-instance-identifier example-test \
    --db-parameter-group-name example-goldengate \
    --apply-immediately

aws rds reboot-db-instance \
    --db-instance-identifier example-test
```

Pour Windows :

```
aws rds create-db-parameter-group ^
    --db-parameter-group-name example-goldengate ^
    --description "Parameters to allow GoldenGate" ^
    --db-parameter-group-family oracle-ee-11.2

aws rds modify-db-parameter-group ^
    --db-parameter-group-name example-goldengate ^
    --parameters "ParameterName=compatible, ParameterValue=11.2.0.4, ApplyMethod=pending-
reboot"

aws rds modify-db-instance ^
    --db-instance-identifier example-test ^
    --db-parameter-group-name example-goldengate ^
    --apply-immediately
```

```
aws rds reboot-db-instance ^
    --db-instance-identifier example-test
```

Conservez toujours le groupe de paramètres avec le paramètre `COMPATIBLE`. Si vous restaurez une instance depuis un instantané de base de données, modifiez l'instance restaurée pour utiliser le groupe de paramètres associé à une valeur de paramètre `COMPATIBLE` correspondante ou supérieure. Faites cette modification dès que possible après l'action de restauration. Elle nécessite un redémarrage de l'instance.

Activer la journalisation supplémentaire sur la base de données source

Le paramètre `ENABLE_GOLDENGATE_REPLICATION`, lorsqu'il est défini sur True (Vrai), active la journalisation supplémentaire pour la base de données source et configure les autorisations GoldenGate requises. Si votre base de données source se trouve sur une instance de base de données Amazon RDS, vous devez avoir un groupe de paramètres affecté à l'instance de base de données avec le paramètre `ENABLE_GOLDENGATE_REPLICATION` défini sur true. Pour de plus amples informations sur `ENABLE_GOLDENGATE_REPLICATION`, veuillez consulter la documentation Oracle.

Définir la période de conservation du journal sur la base de données source

La base de données source doit également conserver les journaux redo archivés. Par exemple, définissez la période de conservation des journaux redo archivés sur 24 heures.

```
exec rdsadmin.rdsadmin_util.set_configuration('archivelog retention hours',24);
```

Spécifiez la durée de conservation des journaux en heures. Cette durée doit dépasser tout éventuel temps d'arrêt de l'instance source ou tout problème potentiel de communication ou de mise en réseau sur l'instance source. Cela permet à Oracle GoldenGate de récupérer les journaux à partir de l'instance source si nécessaire.

La valeur minimum absolue requise est d'une heure de conservation des journaux. Si la conservation des journaux n'est pas activée, ou si la valeur de conservation est trop faible, le message suivant s'affiche :

```
2014-03-06 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 1306Not able to establish initial position for begin time 2014-03-06
 06:16:55.
```

Les journaux sont conservés sur votre instance de base de données. Assurez-vous de disposer d'un espace de stockage suffisant sur votre instance pour les fichiers. Pour vérifier la quantité d'espace utilisé au cours des X dernière heures, utilisez la requête suivante, en remplaçant X par le nombre d'heures.

```
SELECT SUM(BLOCKS * BLOCK_SIZE) BYTES FROM V$ARCHIVED_LOG
   WHERE NEXT_TIME>=SYSDATE-X/24 AND DEST_ID=1;
```

Créer un compte utilisateur sur la source

GoldenGate s'exécute en tant qu'utilisateur de base de données et doit avoir les privilèges de base de données adéquats pour accéder aux journaux redo et d'archivage pour la base de données source. Pour cela, vous devez créer un compte utilisateur GoldenGate sur la base de données source. Pour plus d'informations sur les autorisations pour un compte utilisateur GoldenGate, consultez la section 4, la section 4.4 et le tableau 4.1 dans la documentation Oracle.

Les instructions suivantes créent un compte utilisateur nommé oggadm1.

```
CREATE TABLESPACE administrator;
```

```
CREATE USER oggadm1  IDENTIFIED BY "password"
   DEFAULT TABLESPACE ADMINISTRATOR TEMPORARY TABLESPACE TEMP;
```

Accorder des privilèges de compte sur la base de données source

Accordez les privilèges nécessaires au compte utilisateur GoldenGate à l'aide de la commande SQL `grant` et de la procédure `rdsadmin.rdsadmin_util grant_sys_object`. Les instructions suivantes accordent des privilèges à un utilisateur nommé 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;
```

Enfin, accordez les privilèges nécessaires à un compte utilisateur pour être administrateur GoldenGate. Le package que vous utilisez pour octroyer l'accord, `dbms_goldengate_auth` ou `rdsadmin_dbms_goldengate_auth`, dépend de la version du moteur de base de données Oracle.

- Pour les versions de base de données Oracle antérieures à Oracle 12.2, exécutez le programme PL/SQL suivant.

  ```
  exec dbms_goldengate_auth.grant_admin_privilege (grantee=>'OGGADM1',
     privilege_type=>'capture',
     grant_select_privileges=>true,
     do_grants=>TRUE);
  ```

- Pour les versions de base de données Oracle antérieures ou égales à Oracle 12.2, qui nécessitent le niveau de correctif 12.2.0.1.ru-2019-04.rur-2019-04.r1 ou ultérieur, exécutez le programme PL/SQL suivant.

  ```
  exec rdsadmin.rdsadmin_dbms_goldengate_auth.grant_admin_privilege (grantee=>'OGGADM1',
     privilege_type=>'capture',
     grant_select_privileges=>true,
     do_grants=>TRUE);
  ```

  Pour révoquer des privilèges, utilisez la procédure `revoke_admin_privilege` dans le même package.

Ajouter un alias TNS pour la base de données source

Ajoutez l'entrée suivante à `$ORACLE_HOME/network/admin/tnsnames.ora` dans le répertoire de base Oracle devant être utilisé par le processus `EXTRACT`. Pour de plus amples informations sur le fichier `tnsnames.ora`, veuillez consulter la documentation Oracle.

```
OGGSOURCE=
   (DESCRIPTION=
        (ENABLE=BROKEN)
        (ADDRESS_LIST=
            (ADDRESS=(PROTOCOL=TCP)(HOST=goldengate-source.abcdef12345.us-
west-2.rds.amazonaws.com)(PORT=8200)))
        (CONNECT_DATA=(SID=ORCL))
```

```
    )
```

Configuration d'une base de données cible à utiliser avec GoldenGate sur Amazon RDS

Les tâches suivantes configurent une instance de base de données cible à utiliser avec GoldenGate :

1. Définir le paramètre `compatible` sur 11.2.0.4, ou une version ultérieure
2. Définissez le paramètre `ENABLE_GOLDENGATE_REPLICATION` sur `TRUE`. Si votre base de données cible est sur une instance de base de données Amazon RDS, vous devez avoir un groupe de paramètres affecté à l'instance de base de données avec le paramètre `ENABLE_GOLDENGATE_REPLICATION` défini sur `TRUE`. Pour plus d'informations sur le paramètre `ENABLE_GOLDENGATE_REPLICATION`, consultez la documentation Oracle.
3. Créer et gérer un compte utilisateur GoldenGate sur la base de données cible
4. Accorder les privilèges nécessaires à l'utilisateur GoldenGate
5. Ajoutez un alias TNS pour la base de données cible à tnsnames.ora sur le hub GoldenGate.

Créer un compte d'utilisateur sur la base de données cible

GoldenGate s'exécute en tant qu'utilisateur de base de données et doit posséder les privilèges de base de données appropriés. Pour vous assurer qu'il les possède, créez un compte utilisateur GoldenGate sur la base de données cible.

Les instructions suivantes créent un utilisateur nommé oggadm1 :

```
CREATE TABLESPACE administrator;
CREATE TABLESPACE administrator_idx;
CREATE USER oggadm1  IDENTIFIED BY "password"
   DEFAULT TABLESPACE administrator
   TEMPORARY TABLESPACE temp;
ALTER USER oggadm1 QUOTA UNLIMITED ON administrator;
ALTER USER oggadm1 QUOTA UNLIMITED ON administrator_idx;
```

Accorder des privilèges de compte sur la base de données cible

Accordez les privilèges nécessaires au compte d'utilisateur GoldenGate sur la base de données cible. Dans l'exemple suivant, vous accordez des privilèges à 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;
```

Enfin, accordez les privilèges nécessaires à un compte utilisateur pour être administrateur GoldenGate. Le package que vous utilisez pour octroyer l'accord, `dbms_goldengate_auth` ou `rdsadmin_dbms_goldengate_auth`, dépend de la version du moteur de base de données Oracle.

- Pour les versions de base de données Oracle antérieures à Oracle 12.2, exécutez le programme PL/SQL suivant.

```
exec dbms_goldengate_auth.grant_admin_privilege (grantee=>'OGGADM1',
   privilege_type=>'capture',
   grant_select_privileges=>true,
   do_grants=>TRUE);
```

- Pour les versions de base de données Oracle antérieures ou égales à Oracle 12.2, qui nécessitent le niveau de correctif 12.2.0.1.ru-2019-04.rur-2019-04.r1 ou ultérieur, exécutez le programme PL/SQL suivant.

```
exec rdsadmin.rdsadmin_dbms_goldengate_auth.grant_admin_privilege (grantee=>'OGGADM1',
   privilege_type=>'capture',
   grant_select_privileges=>true,
   do_grants=>TRUE);
```

Pour révoquer des privilèges, utilisez la procédure `revoke_admin_privilege` dans le même package.

Ajouter un alias TNS pour la base de données cible

Ajoutez l'entrée suivante à `$ORACLE_HOME/network/admin/tnsnames.ora` dans le répertoire de base Oracle devant être utilisé par le processus `REPLICAT`. Pour de plus amples informations sur le fichier `tnsname.ora`, veuillez consulter la documentation Oracle.

```
OGGTARGET=
    (DESCRIPTION=
        (ENABLE=BROKEN)
        (ADDRESS_LIST=
            (ADDRESS=(PROTOCOL=TCP)(HOST=goldengate-target.abcdef12345.us-
west-2.rds.amazonaws.com)(PORT=8200)))
        (CONNECT_DATA=(SID=ORCL))
    )
```

Utilisation des utilitaires EXTRACT et REPLICAT de GoldenGate

Les utilitaires GoldenGate `EXTRACT` et `REPLICAT` s'associent pour maintenir la synchronisation des bases de données source et cible via la réplication de transaction incrémentielle en utilisant des fichiers de suivi. Toutes les modifications qui interviennent sur la base de données source sont automatiquement détectées par `EXTRACT`, puis formatées et transférées vers des fichiers de suivi sur le hub d'instance EC2 ou sur site GoldenGate. Après le chargement initial, les données sont lues depuis ces fichiers et répliquées sur la base de données cible par l'utilitaire `REPLICAT`.

Exécution de l'utilitaire GoldenGate EXTRACT

L'utilitaire `EXTRACT` récupère, convertit et fournit des données de la base de données source dans des fichiers de suivi. `EXTRACT` met en file d'attente les détails de transaction à la mémoire ou au stockage temporaire sur disque. Lorsque la transaction est validée dans la base de données source, `EXTRACT` vide tous les détails de transaction dans un fichier de suivi. Le fichier de suivi achemine ces détails vers le hub d'instances GoldenGate sur site ou EC2, puis vers la base de données cible.

Les tâches suivantes activent et démarrent l'utilitaire `EXTRACT` :

1. Configurez le fichier de paramètres `EXTRACT` sur le hub GoldenGate (instance EC2 ou sur site). La liste suivante affiche un exemple de fichier de paramètre `EXTRACT`.

```
EXTRACT EABC
SETENV (ORACLE_SID=ORCL)
SETENV (NLSLANG=AL32UTF8)

USERID oggadm1@OGGSOURCE, PASSWORD XXXXXX
EXTTRAIL /path/to/goldengate/dirdat/ab

IGNOREREPLICATES
GETAPPLOPS
TRANLOGOPTIONS EXCLUDEUSER OGGADM1

TABLE EXAMPLE.TABLE;
```

2. Sur le hub GoldenGate, lancez l'interface de ligne de commande GoldenGate (ggsci). Connectez-vous à la base de données source. L'exemple suivant illustre le format pour la connexion :

```
dblogin userid <user>@<db tnsname>
```

3. Ajoutez une table de point de contrôle pour la base de données :

```
add checkpointtable
```

4. Ajoutez transdata pour activer la journalisation supplémentaire pour la table de base de données :

```
add trandata <user>.<table>
```

   Vous pouvez sinon ajouter transdata pour activer la journalisation supplémentaire pour toutes les tables de base de données :

```
add trandata <user>.*
```

5. En utilisant la ligne de commande `ggsci`, activez l'utilitaire `EXTRACT` en utilisant les commandes suivantes :

```
add extract <extract name> tranlog, INTEGRATED tranlog, begin now
add exttrail <path-to-trail-from-the param-file>
   extract <extractname-from-paramfile>,
   MEGABYTES Xm
```

6. Enregistrez l'utilitaire `EXTRACT` avec la base de données afin que les journaux d'archivage ne soient pas supprimés. Cela vous permet de récupérer d'anciennes transactions non validées, si nécessaire. Pour enregistrer l'utilitaire `EXTRACT` avec la base de données, utilisez la commande suivante :

```
 register EXTRACT <extract process name>, DATABASE
```

7. Pour démarrer l'utilitaire `EXTRACT`, utilisez la commande suivante :

```
start <extract process name>
```

Exécution de l'utilitaire GoldenGate REPLICAT

L'utilitaire `REPLICAT` est utilisé pour « pousser » des informations de transaction dans les fichiers de suivi vers la base de données cible.

Les tâches suivantes activent et démarrent l'utilitaire `REPLICAT` :

1. Configurez le fichier de paramètres `REPLICAT` sur le hub GoldenGate (instance EC2 ou sur site). La liste suivante affiche un exemple de fichier de paramètre `REPLICAT`.

```
REPLICAT RABC
SETENV (ORACLE_SID=ORCL)
SETENV (NLSLANG=AL32UTF8)

USERID oggadm1@OGGTARGET, password XXXXXX

ASSUMETARGETDEFS
MAP EXAMPLE.TABLE, TARGET EXAMPLE.TABLE;
```

2. Lancez l'interface de ligne de commande GoldenGate (ggsci). Connectez-vous à la base de données cible. L'exemple suivant illustre le format pour la connexion.

```
dblogin userid <user>@<db tnsname>
```

3. En utilisant la ligne de commande ggsci, ajoutez un tableau de point de contrôle. L'utilisateur indiqué doit être le compte utilisateur GoldenGate, et non pas le propriétaire du schéma de table cible. L'exemple suivant crée un tableau de point de contrôle nommé gg_checkpoint.

```
add checkpointtable <user>.gg_checkpoint
```

4. Pour activer l'utilitaire `REPLICAT`, utilisez la commande suivante :

```
add replicat <replicat name> EXTTRAIL <extract trail file> CHECKPOINTTABLE
 <user>.gg_checkpoint
```

5. Pour démarrer l'utilitaire `REPLICAT`, utilisez la commande suivante :

```
start <replicat name>
```

Dépannage de problèmes lors de l'utilisation de GoldenGate avec Amazon RDS

Cette section explique les problèmes les plus courants lors de l'utilisation d'Oracle GoldenGate avec Amazon RDS.

Rubriques

- Conservation de journal (p. 1199)
- GoldenGate semble correctement configuré mais la réplication ne fonctionne pas (p. 1200)

Conservation de journal

Pour utiliser Oracle GoldenGate avec Amazon RDS, assurez-vous que la rétention des journaux est activée.

Spécifiez la durée de conservation des journaux en heures. Cette durée doit dépasser tout éventuel temps d'arrêt de l'instance source ou tout problème potentiel de communication ou de mise en réseau sur l'instance source. Cela permet à Oracle GoldenGate de récupérer les journaux à partir de l'instance source si nécessaire.

La valeur minimum absolue requise est d'une heure de conservation des journaux. Si la conservation des journaux n'est pas activée, ou si la valeur de conservation est trop faible, le message suivant s'affiche :

```
2014-03-06 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 1306Not able to establish initial position for begin time 2014-03-06
 06:16:55.
```

GoldenGate semble correctement configuré mais la réplication ne fonctionne pas

Pour les tables pré-existantes, il faut indiquer à GoldenGate à partir de quel SCN il doit travailler. Procédez comme suit pour résoudre ce problème :

1. Lancez l'interface de ligne de commande GoldenGate (ggsci). Connectez-vous à la base de données source. L'exemple suivant illustre le format pour la connexion.

   ```
   dblogin userid <user>@<db tnsname>
   ```

2. A l'aide de la ligne de commande ggsci, configurez le SCN de départ du processus `EXTRACT`. L'exemple suivant définit le SCN sur 223274 pour l'extraction :

   ```
   ALTER EXTRACT <extract process name> SCN 223274
   start <extract process name>
   ```

3. Connectez-vous à la base de données cible. L'exemple suivant illustre le format pour la connexion.

   ```
   dblogin userid <user>@<db tnsname>
   ```

4. A l'aide de la ligne de commande ggsci, configurez le SCN de départ du processus `REPLICAT`. L'exemple suivant définit le SCN sur 223274 pour `REPLICAT`.

   ```
   start <replicat process name> atcsn 223274
   ```

Utilisation de l'utilitaire Oracle Repository Creation Utility sur Amazon RDS pour Oracle

Vous pouvez utiliser Amazon RDS pour héberger une instance de base de données Oracle qui contient les schémas pour prendre en charge vos composants Fusion Middleware. Avant de pouvoir utiliser les composants Fusion Middleware, vous devez créer et remplir les schémas pour eux dans votre base de données. Vous créez et remplissez les schémas à l'aide de l'utilitaire Oracle Repository Creation Utility (RCU).

Vous pouvez stocker les schémas de tous les composants Fusion Middleware dans votre instance de base de données Amazon RDS. Voici une liste de schémas qui ont été vérifiés à installer correctement :

- 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)

Licence et Versions

Amazon RDS prend en charge l'utilitaire Oracle Repository Creation Utility (RCU) version 12c seulement. Vous pouvez utiliser le RCU dans les configurations suivantes :

- Chiffrement RCU 12c avec base de données Oracle 12.2.0.1
- RCU 12c avec Oracle Database 12.1.0.2.v4 ou version ultérieure
- RCU 12c avec Oracle Database 11.2.0.4.v8 ou version ultérieure

Avant de pouvoir utiliser RCU, vous avez besoin d'une licence pour Oracle Fusion Middleware. Vous devez également suivre les consignes sur les licences d'Oracle pour la base de données Oracle qui héberge le référentiel. Pour de plus amples informations, veuillez consulter le Manuel d'utilisateur sur les informations de licence Oracle Fusion Middleware dans la documentation Oracle.

Fusion MiddleWare prend en charge les référentiels sur Oracle Database Enterprise Edition et éditions Standard (SE, SE One ou SE Two). Oracle recommande l'Enterprise Edition pour les installations de production nécessitant un partitionnement et les installations nécessitant une reconstruction d'index en ligne.

Avant de créer votre instance de base de données Oracle, confirmez que la version de la base de données Oracle dont vous avez besoin pour prendre en charge les composants que vous souhaitez déployer. Vous pouvez utiliser la matrice de certification pour trouver les exigences pour les composants et versions de Fusion Middleware que vous souhaitez déployer. Pour de plus amples informations, veuillez consulter la page Configurations système prises en charge par Oracle Fusion Middleware dans la documentation Oracle.

Amazon RDS prend en charge les mises à niveau de version de la base de données Oracle en fonction des besoins. Pour plus d'informations, consultez Mise à niveau d'une version du moteur d'une instance de base de données (p. 267).

Avant de commencer

Avant de commencer, vous avez besoin d'une instance Amazon VPC. Étant donné que votre instance de base de données Amazon RDS doit être disponible uniquement pour vos composants Fusion Middleware et pas pour le réseau Internet public, votre instance de base de données Amazon RDS est hébergée dans un sous-réseau privé, fournissant une plus grande sécurité. Pour plus d'informations sur la création d'une instance de base de données Oracle à utiliser avec Amazon VPC, consultez Création d'une instance &VPC à utiliser avec une base de données Oracle (p. 1182).

Avant de commencer, vous avez également besoin d'une instance de base de données Oracle. Pour plus d'informations sur la création d'une instance de base de données Oracle à utiliser avec les métadonnées de Fusion Middleware, consultez Création d'une instance de base de données Oracle (p. 1187).

Recommandations

Voici quelques recommandations pour l'utilisation de votre instance de base de données dans ce scénario :

- Nous recommandons d'utiliser Multi-AZ pour les charges de travail de production. Pour plus d'informations sur l'utilisation de plusieurs zones de disponibilité, consultez Régions, zones de disponibilité et zones locales (p. 39).
- Pour une sécurité optimale, Oracle recommande que vous utilisiez Transparent Data Encryption (TDE) pour chiffrer les données au repos. Si vous avez une licence Enterprise Edition qui inclut l'option de sécurité avancée, vous pouvez activer le chiffrement au repos à l'aide de l'option TDE. Pour plus d'informations, consultez Oracle Transparent Data Encryption (p. 1091).

  Amazon RDS fournit également une option de chiffrement au repos pour toutes les éditions de la base de données. Pour plus d'informations, consultez Chiffrement des ressources Amazon RDS (p. 1522).
- Configurez vos groupes de sécurité VPC pour permettre la communication entre vos serveurs d'applications et votre instance de base de données Amazon RDS. Les serveurs d'applications qui hébergent les composants Fusion Middleware peuvent être sur Amazon EC2 ou sur site.

Utilisation de l'utilitaire Oracle Repository Creation Utility

Vous utilisez l'utilitaire Oracle Repository Creation Utility (RCU) pour créer et remplir les schémas pour prendre en charge vos composants Fusion Middleware.

Exécution de RCU à l'aide de la ligne de commande en une seule étape

Si vous n'avez besoin de modifier aucun de vos schémas avant de les remplir, vous pouvez exécuter RCU en une seule étape. Sinon, consultez la section suivante pour exécuter RCU en plusieurs étapes.

Vous pouvez exécuter le RCU en mode silencieux à l'aide du paramètre de ligne de commande `-silent`. Lorsque vous exécutez le RCU en mode silencieux, cela vous évite de taper des mots de passe sur la ligne de commande en créant un fichier texte contenant les mots de passe. Créez un fichier texte avec le mot de passe pour `dbUser` sur la première ligne et le mot de passe de chaque composant sur les lignes suivantes. Vous spécifiez le nom du fichier mot de passe en tant que dernier paramètre de la commande RCU.

Example

L'exemple suivant permet de créer et remplir les schémas pour le composant d'infrastructure SOA (et ses dépendances) en une seule étape.

Pour Linux, macOS ou 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
```

Pour de plus amples informations, veuillez consulter la page Exécution de l'utilitaire RCU dans la ligne de commande dans la documentation Oracle.

Exécution de RCU dans la ligne de commande en plusieurs étapes

Si vous devez modifier manuellement vos scripts de schéma, vous pouvez exécuter le RCU en plusieurs étapes :

1. Exécutez RCU en mode Prepare Scripts for System Load (Préparer les scripts pour le chargement système) à l'aide du paramètre de ligne de commande `-generateScript` pour créer les scripts pour vos schémas.
2. Modifiez et exécutez manuellement le script généré `script_systemLoad.sql`.
3. Exécutez RCU à nouveau en mode Perform Product Load (Exécuter la charge de produit) à l'aide du paramètre de ligne de commande `-dataLoad` pour remplir les schémas.
4. Exécutez le script de nettoyage généré `script_postDataLoad.sql`.

Vous pouvez exécuter le RCU en mode silencieux à l'aide du paramètre de ligne de commande `-silent`. Lorsque vous exécutez le RCU en mode silencieux, cela vous évite de taper des mots de passe sur la ligne de commande en créant un fichier texte contenant les mots de passe. Créez un fichier texte avec le mot de passe pour `dbUser` sur la première ligne et le mot de passe de chaque composant sur les lignes suivantes. Vous spécifiez le nom du fichier mot de passe en tant que dernier paramètre de la commande RCU.

Example

L'exemple suivant permet de créer des scripts de schéma pour le composant d'infrastructure SOA (et ses dépendances).

Pour Linux, macOS ou 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
```

Désormais, vous pouvez modifier le script généré, vous connecter à votre instance de base de données Oracle et exécuter le script. Le script généré est appelé `script_systemLoad.sql`. Pour plus d'informations sur la connexion à votre instance de base de données Oracle, consultez Connexion à votre exemple d'instance de base de données Oracle (p. 97).

L'exemple suivant permet de remplir les schémas pour le composant d'infrastructure SOA (et ses dépendances).

Pour Linux, macOS ou 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
```

Pour finir, vous vous connectez à votre instance de base de données Oracle et vous exécutez le script de nettoyage. Ce script est appelé `script_postDataLoad.sql`.

Pour de plus amples informations, veuillez consulter la page Exécution de l'utilitaire RCU dans la ligne de commande dans la documentation Oracle.

Exécution de RCU en mode interactif

Pour utiliser l'interface utilisateur graphique de RCU, vous pouvez exécuter RCU en mode interactif. Pour exécuter RCU en mode interactif, inclut le paramètre `-interactive` et omet le paramètre `-silent`. Pour de plus amples informations, veuillez consulter la page Présentation des écrans de l'utilitaire RCU dans la documentation Oracle.

Example

L'exemple suivant démarre le RCU en mode interactif et pré-remplit les informations de connexion.

Pour Linux, macOS ou 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
```

Problèmes connus

Voici quelques problèmes connus concernant l'utilisation de RCU, avec des suggestions de dépannage :

- Fichiers Oracle Managed Files (OMF) — Amazon RDS utilise les fichiers de données OMF pour simplifier la gestion du stockage. Vous pouvez personnaliser les attributs de table, telles que la taille et la gestion de l'extension. Toutefois, si vous spécifiez un nom de fichier de données lorsque vous exécutez RCU provoque l'échec du code de l'espace de table avec `ORA-20900`. Le RCU peut être utilisée avec OMF de la manière suivante :

  - Dans RCU 12.2.1.0 et version ultérieure, utilisez le paramètre de ligne de commande `-honorOMF`.
  - Dans RCU 12.1.0.3 et plus tard, utilisez plusieurs étapes et modifier le script généré. Pour plus d'informations, consultez Exécution de RCU dans la ligne de commande en plusieurs étapes (p. 1203).
- SYSDBA — Comme Amazon RDS est un service géré, vous n'avez pas un accès total SYSDBA à votre instance de base de données Oracle. Cependant, RCU 12c prend en charge les utilisateurs avec des privilèges inférieurs. Dans la plupart des cas, le privilège de l'utilisateur principal est suffisant pour créer des référentiels. Dans certains cas, le RCU peut échouer avec `ORA-01031` lors de la tentative d'accorder des privilèges objet SYS. Vous pouvez réessayer et exécuter la procédure stockée RDSADMIN_UTIL.GRANT_SYS_OBJECT(), ou contacter AWS Support.
- Transfert de service de planificateur d'entreprise — Lorsque vous utilisez le RCU pour transférer un référentiel de service de planificateur d'entreprise, le RCU peut échouer avec `Error: Component drop check failed`.

Voir aussi

- Options de licence Oracle (p. 930)

Installation d'une base de données Siebel sur Oracle sur Amazon RDS

Vous pouvez utiliser Amazon RDS pour héberger une base de données Siebel sur une instance de base de données Oracle. La base de données Siebel fait partie de l'architecture d'application Siebel Customer Relationship Management (CRM). Pour une illustration, consultez Architecture générique de Siebel Business Application.

Reportez-vous à la rubrique suivante pour configurer une base de données Siebel sur une instance de base de données Oracle sur Amazon RDS. Vous pouvez également trouver comment utiliser Amazon Web Services pour prendre en charge les autres composants requis par l'architecture d'application Siebel CRM.

> **Note**
>
> Pour installer une base de données Siebel sur Oracle sur Amazon RDS, vous devez utiliser le compte utilisateur principal. Vous n'avez pas besoin de privilège `SYSDBA` ; le privilège de l'utilisateur principal est suffisant. Pour plus d'informations, consultez Privilèges du compte utilisateur principal (p. 1605).

Licence et Versions

Pour installer une base de données Siebel sur Amazon RDS, vous devez utiliser votre propre licence d'Oracle Database et votre propre licence Siebel. Vous devez posséder la licence d'Oracle Database appropriée (avec la licence de mise à jour du logiciel et le support) pour la classe d'instance de base de données et l'édition d'Oracle Database que vous souhaitez exécuter. Pour plus d'informations, consultez Options de licence Oracle (p. 930).

Oracle Database Enterprise Edition est la seule édition certifiée par Siebel pour ce scénario. Amazon RDS prend en charge les versions 15.0 ou 16.0 de Siebel CRM. Utilisez Oracle 12c, version 12.1.0.2.0. Pour les procédures suivantes, nous utilisons la version 15.0 de Siebel CRM et Oracle 12.1.0.2 ou 12.2.0.1. Pour plus d'informations, consultez Oracle 12c avec Amazon RDS (p. 940).

Amazon RDS prend en charge les mises à niveau de la version de la base de données. Pour plus d'informations, consultez Mise à niveau d'une version du moteur d'une instance de base de données (p. 267).

Avant de commencer

Avant de commencer, vous avez besoin d'une instance Amazon VPC. Étant donné que votre instance de base de données Amazon RDS doit être disponible uniquement pour votre serveur d'entreprise Siebel et pas pour le réseau Internet public, votre instance de base de données Amazon RDS est hébergée dans un sous-réseau privé, fournissant une plus grande sécurité. Pour plus d'informations sur la création d'une instance Amazon VPC à utiliser avec Siebel CRM, consultez Création d'une instance &VPC à utiliser avec une base de données Oracle (p. 1182).

Avant de commencer, vous avez également besoin d'une instance de base de données Oracle. Pour plus d'informations sur la création d'une instance de base de données Oracle à utiliser avec Siebel CRM, consultez Création d'une instance de base de données Oracle (p. 1187).

Installation et configuration d'une base de données Siebel

Après avoir créé votre instance de base de données Oracle, vous pouvez installer votre base de données Siebel. Vous installez la base de données en créant des comptes de propriétaire et d'administrateur de table, en installant les fonctions et procédures stockées, puis en exécutant l'Assistant de configuration de base de données Siebel. Pour plus d'informations, consultez la page Installation de la base de données Siebel sur le SGBDR.

Pour exécuter l'Assistant de configuration de base de données Siebel, vous devez utiliser le compte utilisateur principal. Vous n'avez pas besoin de privilège `SYSDBA` ; le privilège de l'utilisateur principal est suffisant. Pour plus d'informations, consultez Privilèges du compte utilisateur principal (p. 1605).

Utilisation d'autres fonctions Amazon RDS avec une base de données Siebel

Après avoir créé votre instance de base de données Oracle, vous pouvez utiliser d'autres fonctions Amazon RDS pour vous aider à personnaliser votre base de données Siebel.

Collecte de statistiques avec l'Option Oracle Statspack

Vous pouvez ajouter des fonctions à votre instance de base de données grâce à l'utilisation d'options dans les groupes d'options de base de données. Lorsque vous avez créé votre instance de base de données Oracle, vous avez utilisé le groupe d'options de base de données par défaut. Si vous souhaitez ajouter des fonctions à votre base de données, vous pouvez créer un nouveau groupe d'options pour votre instance de base de données.

Si vous souhaitez collecter des statistiques de performances sur votre base de données Siebel, vous pouvez ajouter la fonction Oracle Statspack. Pour plus d'informations, consultez Oracle Statspack (p. 1085).

Certaines modifications des options sont appliquées immédiatement, et certaines modifications des options sont appliquées pendant le créneau de maintenance suivant pour l'instance de base de données. Pour plus d'informations, consultez Utilisation de groupes d'options (p. 209). Une fois que vous créez un groupe d'options personnalisé, modifiez votre instance de base de données pour l'attacher. Pour de plus amples informations, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

Réglage des performances avec les paramètres

Vous gérez la configuration de votre moteur de base de données à l'aide de paramètres dans un groupe de paramètres de base de données. Lorsque vous avez créé votre instance de base de données Oracle, vous avez utilisé le groupe de paramètres de base de données par défaut. Si vous souhaitez personnaliser votre configuration de base de données, vous pouvez créer un nouveau groupe de paramètres pour votre instance de base de données.

Lorsque vous modifiez un paramètre, en fonction du type du paramètre, les modifications sont appliquées immédiatement ou après le redémarrage manuel de l'instance de base de données. Pour plus d'informations, consultez Utilisation de groupes de paramètres de base de données (p. 225). Une fois que vous créez un groupe de paramètres personnalisé, modifiez votre instance de base de données pour l'attacher. Pour de plus amples informations, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

Afin d'optimiser votre instance de base de données Oracle pour Siebel CRM, vous pouvez personnaliser certains paramètres. Le tableau suivant illustre certains des paramètres recommandés. Pour plus d'informations sur les performances Siebel CRM, consultez le Guide de réglage des performances Siebel CRM.

Nom du paramètre	Valeur par défaut	Recommandations pour obtenir des performances optimales avec Siebel CRM
`_always_semi_join`	`CHOOSE`	`OFF`
`_b_tree_bitmap_plans`	`TRUE`	`FALSE`
`_like_with_bind_as_equality`	`FALSE`	`TRUE`
`_no_or_expansion`	`FALSE`	`FALSE`
`_optimizer_join_sel_sanity_check`	`FALSE`	`TRUE`
`_optimizer_max_permutations`	`2000`	100
`_optimizer_sortmerge_join_enabled`	`TRUE`	`FALSE`
`_partition_view_enabled`	`TRUE`	`FALSE`
`open_cursors`	`300`	Au moins **`2000`**

Création d'instantanés

Une fois que vous créez votre base de données Siebel, vous pouvez copier la base de données en utilisant les fonctions de l'instantané de Amazon RDS. Pour plus d'informations, consultez Création d'un instantané de base de données (p. 327) et Restauration à partir d'un instantané de base de données (p. 329).

Prise en charge d'autres composants Siebel CRM

En plus de votre base de données Siebel, vous pouvez également utiliser Amazon Web Services pour prendre en charge les autres composants de votre architecture d'application Siebel CRM. Vous trouverez plus d'informations sur la prise en charge fournie par Amazon AWS pour les composants Siebel CRM supplémentaires dans le tableau suivant.

Composant Siebel CRM	Amazon AWS Support
Siebel Enterprise (avec un ou plusieurs serveurs Siebel)	Vous pouvez héberger vos serveurs Siebel sur les instances Amazon Elastic Compute Cloud (Amazon EC2). Vous pouvez utiliser Amazon EC2 pour lancer autant de serveurs virtuels que vous avez besoin. A l'aide de Amazon EC2, vous pouvez effectuer facilement des mises à l'échelle ascendantes et descendantes pour gérer les modifications apportées aux conditions. Pour de plus amples informations, veuillez consulter Qu'est-ce qu'Amazon EC2 ?

Composant Siebel CRM	Amazon AWS Support
	Vous pouvez mettre vos serveurs dans le même VPC avec votre instance de base de données et utiliser le groupe de sécurité VPC pour accéder à la base de données. Pour plus d'informations, consultez Utilisation d'une instance de base de données dans un VPC (p. 1620).
Serveurs Web (avec les extensions de serveur Web Siebel)	Vous pouvez installer plusieurs serveurs Web sur plusieurs instances EC2. Vous pouvez ensuite utiliser Elastic Load Balancing pour répartir le trafic entrant entre les instances. Pour de plus amples informations, veuillez consulter la documentation relative à la présentation d'Elastic Load Balancing.
Nom du serveur Siebel Gateway	Vous pouvez héberger votre serveur de nom Siebel Gateway sur une instance EC2. Vous pouvez ensuite mettre votre serveur dans le même VPC avec l'instance de base de données et utiliser le groupe de sécurité VPC pour accéder à la base de données. Pour plus d'informations, consultez Utilisation d'une instance de base de données dans un VPC (p. 1620).

Voir aussi

- Connexion à une instance de base de données Oracle (p. 961)

Notes de mise à jour pour le moteur de base de données Oracle

Des mises à jour apportées à vos instances de bases de données Amazon RDS pour Oracle assurent que les instances restent à jour. Si vous appliquez des mises à jour, vous avez la garantie que votre instance de base de données exécute une version du logiciel de base de données testée par Oracle et par Amazon. Nous ne prenons pas en charge l'application de correctifs ponctuels à des instances de base de données individuelles.

Vous pouvez spécifier n'importe quelle version Oracle actuellement prise en charge lorsque vous créez une instance de base de données. Vous pouvez spécifier la version majeure (par exemple, Oracle 12.1), puis toute version mineure prise en charge pour la version majeure spécifiée. Si aucune version n'est spécifiée, Amazon RDS utilise par défaut une version prise en charge, généralement la plus récente. Si une version majeure est spécifiée, mais qu'une version mineure ne l'est pas, Amazon RDS utilise par défaut une version récente de la version majeure que vous avez spécifiée. Pour afficher la liste des versions prises en charge et des versions par défaut pour des instances de base de données nouvellement créées, utilisez la commande `describe-db-engine-versions` de l'AWS CLI.

Oracle versions 19.0.0, 18.0.0 et 12.2.0.1

Pour Amazon RDS pour Oracle versions 19.0.0.0, 18.0.0.0 et 12.2.0.1, Amazon RDS intègre les correctifs Oracle en utilisant les mises à jour de version (RU) et les révisions des mises à jour de version (RUR). Nous ne prenons pas en charge l'application de correctifs ponctuels à des instances de base de données individuelles.

Pour identifier les RU et RUR appliquées à Amazon RDS pour Oracle versions 19.0.0, 18.0.0.0 et 12.2.0.1, consultez le tableau ci-dessous.

RU et RUR	Version 19.0.0.0	Version 18.0.0.0	Version 12.2.0.1
Juillet 2020	19.0.0.0.ru-2020-07.rur-2020-07.r	18.0.0.0.ru-2020-07.rur-2020-07.r	12.2.0.1.ru-2020-07.rur-2020-07.r
Avril 2020	19.0.0.0.ru-2020-04.rur-2020-04.r	18.0.0.0.ru-2020-04.rur-2020-04.r	12.2.0.1.ru-2020-04.rur-2020-04.r
Janvier 2020	19.0.0.0.ru-2020-01.rur-2020-01.r	18.0.0.0.ru-2020-01.rur-2020-01.r	12.2.0.1.ru-2020-01.rur-2020-01.r
Octobre 2019	19.0.0.0.ru-2019-10.rur-2019-10.r	18.0.0.0.ru-2019-10.rur-2019-10.r	12.2.0.1.ru-2019-10.rur-2019-10.r
Juillet 2019	19.0.0.0.ru-2019-07.rur-2019-07.r	18.0.0.0.ru-2019-07.rur-2019-07.r	12.2.0.1.ru-2019-07.rur-2019-07.r
Avril 2019	—	—	12.2.0.1.ru-2019-04.rur-2019-04.r
Janvier 2019	—	—	12.2.0.1.ru-2019-01.rur-2019-01.r
Octobre 2018	—	—	12.2.0.1.ru-2018-10.rur-2018-10.r

Oracle 12.1.0.2 et 11.2.0.4

Pour Amazon RDS for Oracle versions 12.1.0.2 et 11.2.0.4, Amazon RDS intègre les correctifs d'Oracle via les mises à jour trimestrielles d'ensemble de correctifs (PSU). Si vous appliquez des mises à jour, vous avez la garantie que votre instance de base de données exécute une version du logiciel de base de données testée par Oracle et par Amazon. Nous ne prenons pas en charge l'application de correctifs ponctuels à des instances de base de données individuelles.

Pour découvrir les mises à jour d'ensemble de correctifs (PSU) Oracle appliquées à Amazon RDS pour Oracle 12.1.0.2 et 11.2.0.4, consultez le tableau ci-dessous.

PSU	Version 12.1.0.2	Version 11.2.0.4
Juillet 2020	12.1.0.2.v21 (p. 1278)	11.2.0.4.v25 (p. 1322)
Avril 2020	12.1.0.2.v20 (p. 1282)	11.2.0.4.v24 (p. 1325)
Janvier 2020	12.1.0.2.v19 (p. 1285)	11.2.0.4.v23 (p. 1327)
Octobre 2019	12.1.0.2.v18 (p. 1289)	11.2.0.4.v22 (p. 1330)
Juillet 2019	12.1.0.2.v17 (p. 1292)	11.2.0.4.v21 (p. 1332)
Avril 2019	12.1.0.2.v16 (p. 1295)	11.2.0.4.v20 (p. 1334)
Janvier 2019	12.1.0.2.v15 (p. 1297)	11.2.0.4.v19 (p. 1336)
Octobre 2018	12.1.0.2.v14 (p. 1300)	11.2.0.4.v18 (p. 1338)
Juillet 2018	12.1.0.2.v13 (p. 1302)	11.2.0.4.v17 (p. 1340)
Avril 2018	12.1.0.2.v12 (p. 1304)	11.2.0.4.v16 (p. 1341)
Janvier 2018	12.1.0.2.v11 (p. 1306)	11.2.0.4.v15 (p. 1343)
Octobre 2017	12.1.0.2.v10 (p. 1308)	11.2.0.4.v14 (p. 1345)
Juillet 2017	12.1.0.2.v9 (p. 1310)	11.2.0.4.v13 (p. 1346)
Avril 2017	12.1.0.2.v8 (p. 1312)	11.2.0.4.v12 (p. 1348)

PSU	Version 12.1.0.2	Version 11.2.0.4
Janvier 2017	12.1.0.2.v7 (p. 1314)	11.2.0.4.v11 (p. 1349)
Octobre 2016	12.1.0.2.v6 (p. 1315)	11.2.0.4.v10 (p. 1350)
Juillet 2016	12.1.0.2.v5 (p. 1316)	11.2.0.4.v9 (p. 1352)
Avril 2016	12.1.0.2.v4 (p. 1318)	11.2.0.4.v8 (p. 1353)
Janvier 2016	12.1.0.2.v3 (p. 1319)	11.2.0.4.v7 (p. 1355)
Octobre 2015	12.1.0.2.v2 (p. 1320)	11.2.0.4.v6 (p. 1356) 11.2.0.4.v5 (p. 1356)
Avril 2015	12.1.0.2.v1 (p. 1320)	11.2.0.4.v4 (p. 1357)
Octobre 2014	—	11.2.0.4.v3 (p. 1359)
Juillet 2014	—	11.2.0.4.v2 (p. 1359) (Obsolète)
Janvier 2014	—	11.2.0.4.v1 (p. 1360)

Moteur de base de données : 19.0.0.0

Les versions suivantes sont disponibles pour le moteur de base de données Oracle 19.0.0.0 :

- Version 19.0.0.0.ru-2020-07.rur-2020-07.r1 (p. 1210)
- Version 19.0.0.0.ru-2020-04.rur-2020-04.r1 (p. 1216)
- Version 19.0.0.0.ru-2020-01.rur-2020-01.r1 (p. 1222)
- Version 19.0.0.0.ru-2019-10.rur-2019-10.r1 (p. 1225)
- Version 19.0.0.0.ru-2019-07.rur-2019-07.r1 (p. 1229)

Version 19.0.0.0.ru-2020-07.rur-2020-07.r1

La version 19.0.0.0.ru-2020-07.rur-2020-07.r1 comprend ce qui suit :

- Correctif 31281355 : mise à jour 19.8.0.0.200714 de la version de base de données
- Correctif 31219897 : mise à jour 19.8.0.0.200714 de la version d'Oracle JVM
- Correctif 31335037 : DSTV35 pour RDBMS (TZDATA2020A)
- Correctif 31335142 : DSTV35 pour OJVM (TZDATA2020A)
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS
- Correctif 29213893 : DBMS_ÉCHEC DES STATS AVEC ERREUR ORA-01422 LORS DU REGROUPEMENT DES STATS POUR LA TABLE UTILIATEUR$
- Correctif 29374604 : IE ne démarre pas sur Oracle RDBMS Standard Edition 18c
- PreUpgrade Jar : preupgrade_19_cbuild_7_lf.zip
- Correctif 30417732 : ORA-00600 [KQRHASHTABLEREMOVE : X LOCK] AND INSTANCE CRASH

Correctifs combinés pour la version 19.0.0.0.ru-2020-07.rur-2020-07.r1, publiés en juillet 2020

Bogues corrigés :

```
7391838, 8476681, 14735102, 17428816, 19080742, 19697993, 20313356
21374587, 21965541, 22580355, 22729345, 23296836, 23606241, 23645975
23763462, 24596874, 24669730, 24687075, 24971456, 25030027, 25092651
25416731, 25560538, 25756945, 25804387, 25806201, 25883179, 25986062
25997810, 26001677, 26284288, 26440142, 26476244, 26611353, 26668264
26739322, 26777814, 26872233, 27036163, 27044169, 27101798, 27126122
27126938, 27166935, 27195935, 27221350, 27222128, 27244999, 27254335
27359766, 27369515, 27378053, 27392968, 27406105, 27411022, 27423500
27439716, 27453490, 27458357, 27489107, 27572040, 27582210, 27589260
27604329, 27629928, 27666312, 27692173, 27700413, 27710072, 27729678
27760043, 27801144, 27828892, 27846298, 27877830, 27880025, 27929509
27934711, 27935464, 27941110, 27957203, 27967484, 28064977, 28072567
28078186, 28092783, 28104176, 28109326, 28125947, 28129791, 28138847
28144569, 28181021, 28189466, 28204262, 28205555, 28209985, 28210681
28263142, 28271258, 28271693, 28276054, 28279456, 28294563, 28302580
28313275, 28319114, 28322973, 28326928, 28350595, 28371123, 28373960
28375383, 28379065, 28381939, 28386259, 28390273, 28395302, 28397317
28402823, 28410431, 28431445, 28435333, 28442896, 28454215, 28463226
28470673, 28475242, 28484299, 28489419, 28492006, 28498976, 28502773
28504631, 28513333, 28521330, 28530171, 28534475, 28535127, 28538439
28541606, 28542455, 28546290, 28547068, 28547926, 28558645, 28561704
28564479, 28565296, 28567417, 28567819, 28569897, 28572407, 28572533
28572544, 28572667, 28572834, 28578945, 28587723, 28589509, 28593682
28594086, 28597221, 28601957, 28605066, 28606598, 28608211, 28612239
28618343, 28620697, 28621543, 28622202, 28625862, 28627033, 28628592
28632796, 28636532, 28639299, 28642469, 28642899, 28643654, 28643718
28644549, 28645570, 28646200, 28646939, 28649388, 28655209, 28663289
28663782, 28672457, 28673945, 28681153, 28689483, 28692103, 28692275
28694639, 28694872, 28696373, 28699321, 28703812, 28705231, 28707931
28708400, 28709063, 28710385, 28710469, 28710663, 28710734, 28714461
28715655, 28715727, 28718469, 28719348, 28720204, 28720418, 28721497
28722229, 28730079, 28730253, 28734355, 28740708, 28742555, 28745367
28749853, 28752923, 28755011, 28755846, 28758722, 28760206, 28765983
28767240, 28769456, 28771947, 28772390, 28772816, 28774416, 28776431
28776811, 28777214, 28778754, 28781599, 28781754, 28785321, 28785531
28789531, 28791852, 28793062, 28795551, 28795734, 28800508, 28802734
28804517, 28805242, 28808314, 28808652, 28808656, 28810381, 28811560
28813931, 28815123, 28815355, 28815557, 28817449, 28819640, 28820669
28821847, 28824482, 28827682, 28831971, 28833912, 28835937, 28836716
28838385, 28844738, 28845346, 28846759, 28847541, 28847572, 28849776
28850084, 28852325, 28854004, 28855520, 28855922, 28857552, 28861861
28862532, 28863263, 28863432, 28863487, 28865569, 28867992, 28870496
28871040, 28872645, 28873575, 28874416, 28875089, 28876253, 28876639
28876926, 28877252, 28878865, 28881191, 28881848, 28882784, 28884931
28887305, 28888083, 28888327, 28889730, 28892794, 28897512, 28899663
28900506, 28901126, 28905390, 28905457, 28905615, 28907196, 28910498
28911140, 28912691, 28915561, 28917080, 28918429, 28919145, 28922227
28922532, 28922608, 28925250, 28925460, 28925634, 28925880, 28927452
28932914, 28933158, 28935293, 28935956, 28936114, 28937717, 28938422
28938698, 28940179, 28940281, 28940472, 28941901, 28942455, 28942694
28945421, 28945994, 28946233, 28949888, 28950868, 28951332, 28951533
28952168, 28954762, 28955606, 28955883, 28956908, 28957292, 28957723
28958088, 28959493, 28960863, 28962775, 28963036, 28965084, 28965095
28965231, 28965376, 28966444, 28968779, 28974083, 28974999, 28977322
28980448, 28981871, 28983095, 28983486, 28985478, 28986207, 28986231
28986257, 28986326, 28986481, 28988482, 28988864, 28989306, 28993295
28993353, 28994307, 28994542, 28995287, 28996376, 29000000, 29001305
29001888, 29002488, 29002784, 29002927, 29003207, 29003407, 29003617
```

```
29003738, 29006318, 29006621, 29007321, 29007353, 29007775, 29008035
29008669, 29009513, 29010126, 29011936, 29012609, 29013475, 29013832
29014076, 29015118, 29016294, 29017265, 29018655, 29018680, 29019121
29021063, 29021352, 29022986, 29024054, 29024448, 29024552, 29024732
29024876, 29026154, 29026582, 29026606, 29027456, 29027694, 29027933
29027940, 29031575, 29031600, 29032234, 29032276, 29032457, 29032607
29033052, 29033145, 29033200, 29033280, 29034587, 29036278, 29037290
29038528, 29038728, 29039089, 29039510, 29040739, 29043554, 29043651
29043725, 29044763, 29044954, 29046482, 29047127, 29047850, 29048178
29048289, 29048498, 29048605, 29048728, 29050357, 29050560, 29050765
29050886, 29051702, 29051953, 29052726, 29052850, 29053783, 29055644
29056024, 29056270, 29056560, 29056767, 29056894, 29058476, 29059011
29060216, 29061016, 29061959, 29062692, 29062848, 29062860, 29062868
29110526, 29110783, 29110790, 29110797, 29110802, 29110805, 29111598
29111631, 29112455, 29113282, 29113305, 29115857, 29117337, 29117526
29117642, 29118543, 29119077, 29120223, 29122224, 29122254, 29123297
29123432, 29123444, 29123482, 29124368, 29125036, 29125374, 29125380
29125708, 29125786, 29126345, 29127957, 29128693, 29128935, 29129450
29129476, 29129497, 29129712, 29130219, 29131539, 29131772, 29132456
29132869, 29132938, 29133470, 29134447, 29135383, 29135649, 29136111
29138641, 29139070, 29139727, 29139761, 29139956, 29141316, 29141341
29141685, 29142609, 29142667, 29143516, 29144995, 29145214, 29145730
29146157, 29146810, 29147849, 29149170, 29149829, 29150338, 29151520
29152357, 29152603, 29152752, 29154631, 29154636, 29154725, 29154829
29155099, 29157051, 29157389, 29158680, 29158899, 29159216, 29159661
29159909, 29159936, 29160174, 29160462, 29161597, 29161923, 29162095
29163073, 29163156, 29163415, 29163437, 29163524, 29163567, 29164376
29165682, 29167111, 29167342, 29167374, 29167940, 29168137, 29168219
29168433, 29169073, 29169215, 29169540, 29169739, 29170232, 29170717
29171683, 29171942, 29172618, 29172826, 29173140, 29173373, 29173618
29173817, 29174004, 29174753, 29176318, 29177466, 29177543, 29177886
29178385, 29179097, 29180313, 29180455, 29180559, 29180893, 29181078
29181153, 29181231, 29181568, 29181620, 29181743, 29181923, 29182019
29182517, 29182901, 29182920, 29183298, 29183912, 29184297, 29184666
29185193, 29186091, 29186456, 29186605, 29188255, 29189302, 29189307
29189889, 29190235, 29190474, 29190663, 29190740, 29191541, 29191827
29192419, 29192468, 29192685, 29193207, 29194205, 29194367, 29194493
29194827, 29194981, 29195279, 29195337, 29195758, 29196725, 29198092
29198913, 29199635, 29199733, 29200316, 29200700, 29201143, 29201494
29201539, 29201695, 29201787, 29202104, 29202461, 29202850, 29203122
29203166, 29203227, 29203425, 29203443, 29203604, 29205281, 29205323
29205419, 29205463, 29205767, 29205918, 29206109, 29206605, 29207073
29208260, 29208732, 29209545, 29210577, 29210610, 29210624, 29210683
29211457, 29211724, 29212012, 29212433, 29212611, 29213320, 29213351
29213613, 29213641, 29213775, 29213850, 29213879, 29213893, 29214561
29214960, 29216312, 29216723, 29216746, 29216984, 29217294, 29217472
29217828, 29217848, 29218570, 29219205, 29219273, 29219627, 29220079
29221248, 29221891, 29221942, 29222031, 29222784, 29223833, 29223859
29223967, 29224065, 29224294, 29224605, 29225076, 29225168, 29225758
29225861, 29227602, 29228869, 29229164, 29229754, 29229839, 29229844
29229955, 29230252, 29230565, 29231133, 29232117, 29232154, 29232449
29233415, 29233810, 29233953, 29234123, 29235934, 29236573, 29237538
29237575, 29237744, 29240307, 29240759, 29241345, 29241651, 29242017
29242884, 29242906, 29243749, 29243958, 29244495, 29244766, 29244968
29245063, 29245137, 29245160, 29246163, 29247415, 29247712, 29247906
29248495, 29248552, 29248723, 29248835, 29248858, 29249289, 29249412
29249583, 29249991, 29250059, 29250317, 29251259, 29251564, 29253184
29253871, 29254031, 29254623, 29254930, 29255178, 29255273, 29255431
29255435, 29255616, 29255718, 29255973, 29256426, 29259119, 29259320
29260224, 29260452, 29260956, 29261547, 29261548, 29261695, 29261906
29262512, 29262887, 29265448, 29266248, 29266899, 29267292, 29268412
29269171, 29269228, 29269825, 29270585, 29271019, 29273360, 29273539
29273570, 29273735, 29273812, 29273847, 29274428, 29274564, 29274627
29275461, 29276272, 29277317, 29278218, 29278684, 29279658, 29279751
29279854, 29281527, 29281691, 29281796, 29282090, 29282233, 29282666
29282898, 29285197, 29285453, 29285503, 29285621, 29285788, 29285956
```

```
29286037, 29286229, 29287130, 29287705, 29290110, 29290235, 29292232
29292837, 29293072, 29293574, 29293806, 29294753, 29296257, 29297863
29297915, 29298220, 29299049, 29299082, 29299830, 29299844, 29301463
29301566, 29302963, 29303918, 29304314, 29304781, 29306226, 29306713
29307090, 29307109, 29307638, 29309698, 29311336, 29311528, 29311588
29311927, 29312310, 29312672, 29312734, 29312753, 29312889, 29313347
29313417, 29313525, 29314539, 29314636, 29317756, 29318410, 29319441
29321489, 29323946, 29324568, 29324735, 29325087, 29325105, 29325257
29325765, 29325993, 29327044, 29327892, 29329042, 29329087, 29329675
29329807, 29330361, 29330791, 29331066, 29331209, 29331380, 29331493
29332292, 29332395, 29332763, 29332771, 29333500, 29336843, 29337294
29337310, 29337742, 29338315, 29338348, 29338453, 29338780, 29338913
29339101, 29339155, 29339299, 29341209, 29343086, 29343156, 29343861
29344541, 29345937, 29346057, 29346211, 29346943, 29347620, 29348176
29350052, 29350762, 29350868, 29351044, 29351386, 29351662, 29351716
29351735, 29351749, 29351771, 29352298, 29352724, 29352867, 29352947
29353271, 29353432, 29353718, 29353821, 29353960, 29355654, 29356547
29356704, 29356711, 29356752, 29356782, 29357821, 29358509, 29358828
29360252, 29360285, 29360467, 29360672, 29360775, 29360911, 29360950
29361319, 29361472, 29361801, 29362596, 29363151, 29364171, 29364177
29366406, 29366940, 29367019, 29367561, 29367971, 29368253, 29368310
29368725, 29372069, 29372541, 29373418, 29373588, 29374179, 29374604
29375355, 29375941, 29375984, 29376346, 29377804, 29377986, 29378029
29378287, 29378834, 29378913, 29379299, 29379381, 29379750, 29379978
29380527, 29381000, 29382296, 29382641, 29382784, 29382815, 29383695
29384781, 29384854, 29384864, 29385339, 29385429, 29385652, 29386502
29386557, 29386635, 29386660, 29387073, 29387274, 29387310, 29387337
29388020, 29388072, 29388094, 29388524, 29388830, 29389408, 29389889
29390011, 29390435, 29390785, 29391030, 29391237, 29391301, 29391438
29391849, 29391925, 29392554, 29392966, 29393291, 29393649, 29394014
29394140, 29394749, 29395657, 29397954, 29397996, 29398488, 29398863
29399046, 29399100, 29399121, 29399336, 29399938, 29402110, 29402131
29404483, 29405012, 29405462, 29405651, 29405996, 29407488, 29407804
29408853, 29409149, 29409455, 29410311, 29410834, 29411037, 29411469
29411931, 29412066, 29412269, 29413360, 29413382, 29413517, 29413544
29413634, 29413956, 29416688, 29416700, 29417084, 29417173, 29417719
29417884, 29418165, 29420254, 29420834, 29421059, 29423003, 29423016
29423156, 29423826, 29424999, 29426241, 29426320, 29428230, 29429017
29429087, 29429264, 29429466, 29429566, 29430524, 29430866, 29431192
29431485, 29432176, 29434301, 29434869, 29435474, 29435652, 29436454
29436514, 29436522, 29436727, 29437594, 29437712, 29438150, 29438277
29438736, 29439522, 29441196, 29442936, 29443187, 29443250, 29444072
29444282, 29444602, 29445548, 29446669, 29448498, 29449477, 29449845
29449852, 29450162, 29450193, 29450421, 29450812, 29450936, 29451386
29452251, 29452576, 29452936, 29452953, 29454978, 29455424, 29455773
29456538, 29456714, 29457312, 29457319, 29457370, 29457502, 29457807
29457978, 29460252, 29461420, 29461791, 29461971, 29462594, 29462767
29462957, 29463047, 29463528, 29463798, 29464616, 29464779, 29465047
29465177, 29466674, 29467622, 29469565, 29470291, 29471832, 29471860
29472618, 29473708, 29476473, 29481584, 29483452, 29483532, 29483626
29483672, 29483685, 29483712, 29483723, 29483771, 29485099, 29486181
29486848, 29487150, 29487189, 29488894, 29489436, 29489546, 29490256
29492127, 29492939, 29493122, 29494245, 29495057, 29495684, 29497311
29497588, 29497696, 29498198, 29500257, 29500826, 29500963, 29501218
29502561, 29503543, 29503631, 29503827, 29504492, 29504682, 29505668
29506942, 29507270, 29507616, 29508681, 29509777, 29510278, 29511064
29511611, 29511980, 29512125, 29512890, 29514479, 29515134, 29515240
29515476, 29515766, 29515834, 29516300, 29516727, 29516766, 29517168
29517883, 29519131, 29521187, 29521688, 29521748, 29521862, 29522358
29522561, 29522662, 29523055, 29523216, 29523511, 29524599, 29524985
29525366, 29525467, 29525886, 29526966, 29527595, 29527610, 29528368
29529147, 29530440, 29530515, 29530812, 29530909, 29531654, 29531836
29532532, 29536342, 29536445, 29537829, 29538631, 29540327, 29541742
29541769, 29542084, 29542449, 29542580, 29542643, 29543034, 29543956
29546817, 29547010, 29547867, 29548413, 29548427, 29548592, 29548687
29548722, 29549040, 29549071, 29549104, 29549154, 29549730, 29552773
```

```
29553141, 29554092, 29557144, 29557261, 29557336, 29557556, 29558238
29558452, 29558975, 29559187, 29559395, 29559446, 29559908, 29559981
29564592, 29564593, 29565611, 29579919, 29580394, 29580983, 29581771
29584261, 29584693, 29586143, 29587299, 29587765, 29589544, 29591343
29592011, 29592215, 29597536, 29597754, 29598039, 29598046, 29598226
29598233, 29599008, 29599300, 29601461, 29602831, 29603460, 29603884
29604002, 29604257, 29606261, 29607136, 29607797, 29608000, 29608023
29610506, 29611020, 29611991, 29614206, 29614987, 29615824, 29616244
29616414, 29618074, 29618190, 29620042, 29622936, 29623323, 29625065
29625804, 29625876, 29626154, 29626732, 29628200, 29629430, 29629650
29629681, 29629745, 29631749, 29632095, 29632265, 29632611, 29633697
29633753, 29633936, 29634643, 29635427, 29635717, 29635990, 29637362
29637526, 29637560, 29638285, 29641736, 29643721, 29644426, 29644464
29645167, 29645349, 29647176, 29648928, 29651183, 29651520, 29653132
29653246, 29655164, 29655668, 29656400, 29656819, 29656843, 29657399
29657422, 29657744, 29657960, 29658056, 29661028, 29661065, 29661722
29663191, 29663368, 29663494, 29663601, 29664087, 29664161, 29665940
29667527, 29667994, 29668005, 29669413, 29670782, 29671363, 29672507
29675446, 29676089, 29677051, 29677173, 29677733, 29677927, 29679856
29681987, 29683039, 29683211, 29684518, 29685137, 29685276, 29687214
29687220, 29687459, 29687718, 29687727, 29687763, 29688867, 29689145
29689255, 29692694, 29694869, 29695425, 29695821, 29695841, 29696310
29700125, 29700460, 29700770, 29703932, 29705793, 29707099, 29707493
29707896, 29708876, 29708915, 29710188, 29710858, 29713810, 29715220
29715703, 29716194, 29716227, 29716491, 29716602, 29716871, 29717659
29717901, 29719146, 29720133, 29721418, 29721576, 29722167, 29724658
29725476, 29725781, 29726695, 29738400, 29739576, 29741319, 29741976
29742223, 29744225, 29746962, 29747493, 29747648, 29747653, 29748285
29748336, 29748513, 29749471, 29750673, 29751094, 29753244, 29754196
29754951, 29755821, 29756274, 29756444, 29757099, 29757264, 29757651
29757687, 29758203, 29758217, 29758661, 29761678, 29761837, 29761911
29763158, 29765035, 29765393, 29766207, 29766435, 29766503, 29766679
29768899, 29770750, 29771032, 29771242, 29773197, 29773842, 29774362
29775393, 29779196, 29780140, 29782211, 29782823, 29782866, 29784106
29785239, 29785311, 29787292, 29787766, 29789911, 29791152, 29791880
29792213, 29793318, 29794174, 29794462, 29795712, 29795957, 29796378
29797726, 29802695, 29804875, 29805772, 29806390, 29807964, 29809792
29809837, 29812084, 29812489, 29813503, 29813650, 29813671, 29815341
29815713, 29817278, 29817547, 29817784, 29821582, 29822714, 29825525
29827647, 29827852, 29831196, 29834506, 29836096, 29838485, 29838773
29839715, 29840619, 29841267, 29841687, 29843277, 29843692, 29843831
29844226, 29844275, 29845530, 29846126, 29846645, 29846688, 29848084
29848849, 29849100, 29850930, 29851733, 29853485, 29856859, 29858121
29858376, 29859068, 29860994, 29861075, 29864203, 29864261, 29865188
29865590, 29865658, 29869086, 29869404, 29869887, 29869906, 29870065
29871098, 29871312, 29872401, 29872937, 29872983, 29873665, 29874090
29874761, 29875459, 29875565, 29876358, 29876989, 29877608, 29878076
29881050, 29881478, 29881575, 29881643, 29881839, 29882427, 29882454
29882729, 29884958, 29885890, 29886809, 29887111, 29888621, 29889184
29889358, 29890740, 29891075, 29891853, 29891916, 29892604, 29893132
29896510, 29897418, 29897863, 29900203, 29900824, 29901419, 29902299
29902327, 29902330, 29902659, 29903190, 29903299, 29903357, 29903454
29904002, 29906678, 29907942, 29908389, 29908777, 29909658, 29910402
29912286, 29913805, 29913966, 29914449, 29914544, 29915217, 29915848
29916975, 29919789, 29920025, 29920376, 29920804, 29921318, 29922225
29923452, 29924181, 29926466, 29927756, 29928210, 29928427, 29928564
29930457, 29932202, 29932430, 29932780, 29934052, 29937565, 29937956
29938225, 29939400, 29939795, 29940373, 29942096, 29942275, 29942554
29943670, 29943879, 29944035, 29944660, 29944963, 29945645, 29946388
29947145, 29950220, 29951620, 29951759, 29956016, 29956222, 29957412
29957493, 29958925, 29960884, 29961353, 29961609, 29961847, 29962160
29962248, 29962834, 29962927, 29962939, 29965052, 29965603, 29965888
29966768, 29967223, 29968085, 29969557, 29970081, 29970298, 29971027
29971481, 29971888, 29971936, 29971951, 29972176, 29973012, 29989783
29989845, 29991257, 29993717, 29997326, 29997553, 29997937, 30000664
30001331, 30003187, 30006159, 30006985, 30007450, 30007797, 30008125
```

```
30008198, 30008214, 30009710, 30012181, 30015070, 30017836, 30018017
30018903, 30019864, 30024618, 30025814, 30026016, 30027614, 30028599
30029519, 30029806, 30031027, 30032376, 30033040, 30033547, 30034456
30035598, 30038392, 30039800, 30039959, 30040157, 30041501, 30042490
30043398, 30043610, 30043930, 30044507, 30045389, 30045484, 30046497
30047531, 30047702, 30047765, 30047931, 30049966, 30051176, 30051783
30051804, 30052928, 30053036, 30053501, 30053748, 30054980, 30056058
30057718, 30057799, 30058149, 30058453, 30059106, 30059109, 30060267
30060330, 30062364, 30062819, 30064268, 30066352, 30067565, 30068871
30071446, 30072905, 30073314, 30073744, 30074296, 30074349, 30074469
30074472, 30074820, 30075037, 30076058, 30076197, 30076253, 30078675
30078934, 30079949, 30080266, 30081546, 30081580, 30082145, 30083100
30083216, 30083488, 30083807, 30084971, 30085897, 30086596, 30086992
30090568, 30092280, 30092859, 30095591, 30095952, 30097092, 30097115
30098251, 30099302, 30099420, 30099454, 30100354, 30101186, 30103551
30103553, 30104378, 30104555, 30106748, 30109365, 30110224, 30110370
30110518, 30114477, 30114489, 30114534, 30116085, 30116203, 30116854
30117209, 30117335, 30117593, 30118261, 30118279, 30120608, 30122583
30125765, 30126145, 30127522, 30127805, 30127904, 30128047, 30131286
30131645, 30132708, 30133841, 30134746, 30135396, 30135731, 30135942
30136346, 30139392, 30142907, 30143470, 30143593, 30146593, 30146969
30147473, 30147928, 30149035, 30149658, 30150606, 30153552, 30153885
30154633, 30155814, 30155837, 30159329, 30159511, 30159536, 30159752
30159760, 30160625, 30163243, 30164714, 30165493, 30165503, 30165897
30169254, 30170104, 30172925, 30173113, 30173556, 30174401, 30175291
30177597, 30178250, 30178839, 30178990, 30179644, 30180208, 30181756
30183696, 30183715, 30183920, 30184102, 30185852, 30186319, 30186476
30186706, 30187866, 30189516, 30190090, 30191274, 30193165, 30193505
30193736, 30194612, 30194710, 30194972, 30195667, 30195668, 30195684
30196195, 30196358, 30196629, 30198861, 30198905, 30200034, 30200132
30200237, 30200680, 30200758, 30202349, 30202388, 30203929, 30204042
30204542, 30206493, 30206675, 30207473, 30208327, 30208723, 30209736
30210884, 30213031, 30213540, 30215130, 30215302, 30215351, 30217206
30217982, 30218044, 30218317, 30219222, 30221237, 30221298, 30222512
30223712, 30223847, 30224650, 30224868, 30224950, 30225265, 30225443
30225718, 30225844, 30226244, 30228567, 30229683, 30232638, 30235919
30235979, 30236554, 30238211, 30238715, 30239480, 30240010, 30240547
30241567, 30241920, 30242120, 30242724, 30243216, 30244340, 30246053
30246179, 30247305, 30249432, 30251003, 30252005, 30252098, 30252156
30252458, 30252977, 30253035, 30253090, 30253608, 30253705, 30253835
30254206, 30254525, 30254726, 30255143, 30255528, 30256542, 30257412
30264405, 30265523, 30265608, 30265615, 30265703, 30266791, 30267155
30269428, 30269748, 30270647, 30270744, 30271114, 30272329, 30274090
30274188, 30274324, 30275548, 30275569, 30275578, 30276243, 30277120
30277451, 30277733, 30281428, 30282501, 30282591, 30283296, 30283577
30283579, 30283581, 30283932, 30284219, 30284369, 30285457, 30285843
30288343, 30288491, 30289458, 30293345, 30294267, 30294671, 30295110
30295549, 30295808, 30297905, 30299367, 30299817, 30299934, 30300030
30300538, 30305264, 30305395, 30305568, 30305880, 30307814, 30307883
30308368, 30308624, 30308772, 30308947, 30309098, 30309798, 30311826
30312094, 30312546, 30313848, 30314079, 30314198, 30314837, 30316667
30316897, 30317209, 30318638, 30318943, 30319080, 30319099, 30322980
30323658, 30323849, 30324180, 30325407, 30326882, 30327149, 30328168
30328690, 30329209, 30330123, 30331759, 30332505, 30334484, 30334563
30335127, 30335832, 30335987, 30336032, 30336742, 30339103, 30341713
30342371, 30342878, 30344614, 30345201, 30345432, 30345809, 30346330
30346867, 30349714, 30352581, 30352623, 30355490, 30357463, 30357897
30360383, 30362003, 30362850, 30363716, 30364329, 30364613, 30365745
30367193, 30368048, 30368482, 30368534, 30368668, 30371264, 30371623
30371909, 30372081, 30373550, 30374345, 30374570, 30374739, 30375109
30376986, 30377347, 30381207, 30381525, 30382982, 30383286, 30384121
30384152, 30389229, 30389414, 30389507, 30391272, 30392011, 30393110
30393653, 30394738, 30394974, 30396946, 30397100, 30398257, 30398422
30399906, 30402386, 30403763, 30403881, 30403902, 30403989, 30404117
30408515, 30408808, 30409207, 30409339, 30409590, 30412188, 30412863
30412885, 30412921, 30413137, 30414679, 30414714, 30416034, 30417648
```

```
30417732, 30419024, 30421439, 30421476, 30422487, 30423135, 30423218
30424347, 30430921, 30431274, 30431504, 30431698, 30431703, 30431717
30433177, 30437149, 30441687, 30441959, 30442749, 30442884, 30443393
30446583, 30447060, 30447589, 30448182, 30448917, 30449194, 30450787
30453442, 30454090, 30458568, 30458593, 30460922, 30461458, 30463938
30464250, 30464655, 30466081, 30469777, 30472891, 30474167, 30474774
30475115, 30476768, 30477588, 30477685, 30477691, 30477767, 30479715
30480872, 30483140, 30483521, 30484042, 30484801, 30485255, 30486436
30487387, 30490014, 30493518, 30495035, 30495133, 30495483, 30496957
30497057, 30500224, 30500297, 30500344, 30500582, 30501574, 30502415
30503943, 30505497, 30506794, 30506991, 30507032, 30509277, 30510347
30510527, 30513285, 30513848, 30515886, 30516868, 30517214, 30519188
30522285, 30522998, 30523137, 30523538, 30523601, 30523750, 30528547
30528704, 30529940, 30533132, 30534351, 30534549, 30534662, 30534827
30537405, 30537533, 30539519, 30540109, 30540407, 30544247, 30544595
30545281, 30545556, 30549637, 30549789, 30549881, 30551000, 30551123
30556581, 30556807, 30557386, 30560513, 30561590, 30564139, 30564343
30573703, 30576393, 30577071, 30579051, 30581448, 30582500, 30588738
30591028, 30592859, 30595114, 30595860, 30596488, 30598682, 30598746
30598919, 30599405, 30599407, 30600173, 30600184, 30602230, 30605215
30609799, 30612199, 30613937, 30613971, 30614411, 30619525, 30619787
30622528, 30623138, 30623142, 30624792, 30624864, 30625121, 30628899
30629643, 30629799, 30631393, 30633259, 30633938, 30635183, 30635302
30635326, 30637270, 30637319, 30641755, 30641900, 30644889, 30651231
30651621, 30651674, 30652515, 30652853, 30654558, 30657365, 30657624
30657706, 30657875, 30658702, 30661939, 30662651, 30663646, 30668407
30671813, 30674959, 30676209, 30681462, 30681516, 30686131, 30690686
30691604, 30691731, 30691857, 30692473, 30698289, 30703610, 30704826
30708735, 30710807, 30714151, 30714715, 30718862, 30719419, 30720736
30720844, 30722705, 30724679, 30724881, 30727701, 30729604, 30730026
30732711, 30734707, 30735736, 30740997, 30741263, 30749722, 30750991
30751968, 30758943, 30761878, 30763272, 30763305, 30763639, 30765486
30769312, 30773164, 30776416, 30776929, 30778855, 30781032, 30781041
30783551, 30785101, 30789904, 30790441, 30801296, 30801510, 30803210
30808869, 30812574, 30814285, 30815852, 30816938, 30823744, 30825391
30825419, 30825656, 30826474, 30828350, 30829779, 30833454, 30834110
30838605, 30847442, 30848773, 30851951, 30855101, 30857721, 30858919
30866141, 30866988, 30871716, 30871792, 30880913, 30881407, 30883877
30886188, 30887501, 30890720, 30890971, 30896620, 30904672, 30906274
30909918, 30913399, 30914272, 30914674, 30919691, 30922936, 30922996
30923517, 30923940, 30927821, 30930339, 30936831, 30937410, 30939934
30940259, 30941056, 30944643, 30945005, 30952104, 30953836, 30957739
30964194, 30968737, 30970518, 30972841, 30972966, 30973113, 30973137
30973143, 30980317, 30980733, 30987088, 30990034, 30992597, 30993198
30996991, 30998759, 30998847, 31001017, 31001455, 31001859, 31004077
31004719, 31004844, 31008240, 31010976, 31013127, 31016413, 31019249
31021157, 31022858, 31029936, 31031955, 31032904, 31039627, 31039928
31051075, 31062010, 31066265, 31077365, 31084921, 31094688, 31100172
31106577, 31113089, 31118809, 31119057, 31134430, 31153120, 31156383
31172207, 31177193, 31182793, 31193936, 31200845, 31305624, 31306261
31335037, 31335142, 31338673, 31359215, 31383396, 31393600, 31414023
31414524
```

Version 19.0.0.0.ru-2020-04.rur-2020-04.r1

La version 19.0.0.0.ru-2020-04.rur-2020-04.r1 comprend ce qui suit :

- Correctif 30869156 : Mise à jour 19.7.0.0.200414 de la version de base de données
- Correctif 30805684 : Mise à jour 19.7.0.0.200414 de la version d'Oracle JVM
- Correctif 29997937 : MISE À JOUR DSTv34 pour SGBDR (TZDATA2019B)
- Correctif 29997959 : MISE À JOUR DSTV34 pour OJVM (TZDATA2019B)

- PreUpgrade Jar : preupgrade_19_cbuild_5_lf.zip
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS
- Correctif 29213893 : DBMS_ÉCHEC DES STATS AVEC ERREUR ORA-01422 LORS DU REGROUPEMENT DES STATS POUR LA TABLE UTILIATEUR$
- Correctif 30528704 : 19C RMAN RÉCUPÉRATION DU JOURNAL REDO D'UTILISATION DE BASE DE DONNÉES AU LIEU D'ARCHIVELOG APRÈS APPLICATION DE LA MISE À JOUR DE BASE DE DONNÉES D'OCT
- Prise en charge de Purge de la corbeille (p. 1129)
- Prise en charge de Génération de rapports de performance avec AWR (Automatic Workload Repository) (p. 1119) utilisant le package `rdsadmin.rdsadmin_diagnostic_util`.

Correctifs combinés pour la version 19.0.0.0.ru-2020-04.rur-2020-04.r1, publiés en avril 2020

Bogues corrigés :

```
30533132, 30312546, 29924181, 29549154, 30937410, 29970081, 8476681
14735102, 17428816, 19080742, 19697993, 20313356, 21374587, 21965541
23296836, 23606241, 24687075, 24971456, 25756945, 25806201, 25883179
25986062, 25997810, 26284288, 26476244, 26611353, 26668264, 26739322
26777814, 26872233, 27036163, 27044169, 27101798, 27126122, 27126938
27166935, 27195935, 27244999, 27254335, 27359766, 27369515, 27378053
27406105, 27411022, 27423500, 27439716, 27453490, 27458357, 27489107
27582210, 27666312, 27710072, 27729678, 27801144, 27846298, 27880025
27929509, 27934711, 27935464, 27941110, 27957203, 27967484, 28064977
28072567, 28109326, 28125947, 28129791, 28181021, 28189466, 28204262
28205555, 28209985, 28210681, 28263142, 28271258, 28271693, 28276054
28279456, 28294563, 28313275, 28319114, 28326928, 28350595, 28371123
28373960, 28375383, 28379065, 28381939, 28386259, 28390273, 28395302
28397317, 28402823, 28410431, 28431445, 28435333, 28454215, 28463226
28475242, 28484299, 28489419, 28492006, 28498976, 28502773, 28513333
28521330, 28530171, 28534475, 28535127, 28538439, 28542455, 28546290
28547068, 28547926, 28558645, 28561704, 28564479, 28565296, 28567417
28567819, 28569897, 28572407, 28572533, 28572544, 28572667, 28572834
28578945, 28587723, 28589509, 28593682, 28594086, 28597221, 28601957
28605066, 28606598, 28608211, 28612239, 28620697, 28622202, 28625862
28627033, 28628592, 28632796, 28636532, 28639299, 28643654, 28643718
28644549, 28645570, 28646200, 28646939, 28649388, 28655209, 28663782
28672457, 28673945, 28681153, 28692103, 28692275, 28694639, 28694872
28696373, 28705231, 28707931, 28708400, 28709063, 28710385, 28710469
28710734, 28714461, 28715727, 28718469, 28719348, 28720204, 28720418
28721497, 28722229, 28730079, 28734355, 28740708, 28742555, 28749853
28752923, 28755011, 28758722, 28760206, 28765983, 28767240, 28769456
28771947, 28772390, 28774416, 28776811, 28777214, 28781754, 28785531
28789531, 28791852, 28795551, 28795734, 28802734, 28804517, 28808656
28810381, 28811560, 28815123, 28815355, 28817449, 28819640, 28820669
28821847, 28824482, 28827682, 28831971, 28833912, 28835937, 28836716
28838385, 28844738, 28845346, 28846759, 28849776, 28854004, 28855520
28855922, 28857552, 28862532, 28863263, 28863432, 28863487, 28865569
28867992, 28872645, 28873575, 28875089, 28876253, 28876639, 28876926
28878865, 28882784, 28884931, 28887305, 28888327, 28889730, 28892794
28897512, 28899663, 28901126, 28905457, 28905615, 28907196, 28912691
28915561, 28917080, 28918429, 28919145, 28922227, 28922532, 28922608
28925634, 28925880, 28927452, 28932914, 28933158, 28935293, 28936114
28937717, 28938422, 28938698, 28940179, 28940281, 28941901, 28942455
28945421, 28945994, 28946233, 28949888, 28950868, 28951533, 28952168
28954762, 28955606, 28955883, 28956908, 28957292, 28957723, 28958088
28959493, 28960863, 28962775, 28965084, 28965095, 28965231, 28965376
```

```
28966444, 28974083, 28977322, 28981871, 28983095, 28983486, 28985478
28986207, 28986231, 28986257, 28986326, 28986481, 28988482, 28989306
28993295, 28993353, 28994307, 28994542, 28996376, 29000000, 29001305
29001888, 29002488, 29002784, 29002927, 29003407, 29003738, 29006318
29006621, 29007321, 29007353, 29007775, 29008035, 29008669, 29009513
29010126, 29011936, 29012609, 29013475, 29013832, 29014076, 29015118
29017265, 29018655, 29019121, 29021063, 29021352, 29022986, 29024054
29024552, 29024732, 29026582, 29026606, 29027456, 29027694, 29027940
29031575, 29031600, 29032234, 29032276, 29032457, 29032607, 29033052
29033145, 29033200, 29033280, 29034587, 29037290, 29038528, 29038728
29039089, 29039510, 29040739, 29043554, 29043651, 29043725, 29044763
29044954, 29046482, 29047850, 29048178, 29048289, 29048498, 29048605
29050357, 29050560, 29050765, 29050886, 29051702, 29051953, 29052726
29053783, 29056024, 29056270, 29056560, 29056767, 29056894, 29059011
29060216, 29061016, 29061959, 29062692, 29062848, 29062860, 29062868
29110526, 29110783, 29110790, 29110797, 29110802, 29110805, 29111598
29113282, 29113305, 29115857, 29117526, 29117642, 29118543, 29119077
29120223, 29122224, 29122254, 29123297, 29123432, 29123482, 29124368
29125036, 29125374, 29125380, 29126345, 29127957, 29128693, 29128935
29129450, 29129497, 29129712, 29130219, 29131539, 29132869, 29132938
29133470, 29134447, 29135383, 29135649, 29136111, 29138641, 29139761
29139956, 29141316, 29141341, 29141685, 29142609, 29142667, 29143516
29144995, 29145214, 29145730, 29149829, 29150338, 29151520, 29152357
29154725, 29155099, 29157051, 29157389, 29158680, 29158899, 29159909
29159936, 29160174, 29161597, 29162095, 29163073, 29163156, 29163415
29163437, 29163524, 29163567, 29164376, 29167111, 29167342, 29167374
29167940, 29168137, 29168219, 29168433, 29169073, 29169215, 29170232
29171683, 29171942, 29172618, 29172826, 29173140, 29173373, 29173817
29174004, 29174753, 29176318, 29177466, 29177543, 29177886, 29178385
29179097, 29180313, 29180455, 29180559, 29180893, 29181153, 29181231
29181620, 29181743, 29181923, 29182019, 29182517, 29182901, 29183912
29184297, 29184666, 29185193, 29186456, 29189302, 29189307, 29189889
29190235, 29190474, 29190663, 29190740, 29191541, 29192419, 29192468
29192685, 29193207, 29194205, 29194367, 29194493, 29194827, 29194981
29195279, 29195337, 29195758, 29196725, 29198092, 29198913, 29199635
29199733, 29200316, 29200700, 29201494, 29201539, 29201787, 29202104
29202461, 29202850, 29203122, 29203166, 29203227, 29203425, 29203443
29203604, 29205281, 29205323, 29205419, 29205463, 29205767, 29205918
29206109, 29206605, 29207073, 29208260, 29208732, 29211457, 29211724
29212012, 29212433, 29212611, 29213320, 29213351, 29213613, 29213775
29213850, 29213879, 29214561, 29214960, 29216312, 29216723, 29216746
29216984, 29217294, 29217472, 29217828, 29217848, 29218570, 29219205
29219273, 29220079, 29221248, 29221891, 29221942, 29222031, 29222784
29223833, 29223859, 29223967, 29224065, 29224605, 29225076, 29225168
29225758, 29227602, 29228869, 29229164, 29229754, 29229844, 29229955
29230252, 29230565, 29231133, 29232117, 29232154, 29232449, 29233415
29233810, 29233953, 29234123, 29236573, 29237538, 29237575, 29237744
29240307, 29240759, 29241345, 29241651, 29242017, 29242884, 29243958
29245137, 29245160, 29246163, 29247415, 29247712, 29247906, 29248495
29248552, 29248835, 29248858, 29249289, 29249412, 29249991, 29250059
29250317, 29251259, 29253184, 29253871, 29254031, 29254930, 29255178
29255273, 29255431, 29255435, 29255973, 29256426, 29259119, 29259320
29260452, 29260956, 29261547, 29261548, 29261906, 29262512, 29262887
29265448, 29266248, 29266899, 29267292, 29268412, 29269171, 29269228
29269825, 29270585, 29273539, 29273570, 29273735, 29273812, 29273847
29274428, 29274564, 29274627, 29275461, 29276272, 29277317, 29278218
29278684, 29279658, 29279751, 29279854, 29281527, 29281691, 29281796
29282233, 29282898, 29285197, 29285503, 29285788, 29285956, 29286037
29286229, 29287130, 29287705, 29292837, 29293072, 29293574, 29297863
29297915, 29298220, 29299049, 29299082, 29299844, 29301463, 29301566
29302963, 29303918, 29304781, 29306226, 29306713, 29307638, 29311528
29311588, 29312310, 29312672, 29312734, 29312753, 29312889, 29313347
29313417, 29313525, 29314539, 29314636, 29317756, 29318410, 29319441
29321489, 29323946, 29324568, 29324735, 29325087, 29325105, 29325257
29325765, 29325993, 29327044, 29327892, 29329042, 29329087, 29329807
29330361, 29331066, 29331209, 29331380, 29331493, 29332292, 29332395
```

```
29332763, 29332771, 29333500, 29336843, 29337310, 29337742, 29338315
29338348, 29338453, 29338780, 29338913, 29339101, 29339155, 29341209
29343086, 29343156, 29343861, 29345937, 29346057, 29346211, 29346943
29347620, 29348176, 29350052, 29350762, 29351044, 29351386, 29351662
29351716, 29351735, 29351749, 29351771, 29352298, 29352724, 29352867
29352947, 29353271, 29353432, 29353821, 29353960, 29355654, 29356547
29356704, 29356711, 29356752, 29356782, 29358509, 29358828, 29360252
29360285, 29360672, 29360911, 29360950, 29361319, 29361472, 29361801
29363151, 29364171, 29364177, 29366940, 29367019, 29367561, 29368253
29368310, 29372541, 29373418, 29373588, 29374179, 29375355, 29375941
29375984, 29376346, 29377804, 29377986, 29378029, 29378287, 29378834
29378913, 29379750, 29379978, 29382641, 29382784, 29382815, 29383695
29384781, 29384854, 29384864, 29385339, 29385429, 29385652, 29386502
29386635, 29386660, 29387073, 29387274, 29387310, 29388020, 29388072
29388094, 29388524, 29388830, 29389889, 29390011, 29390435, 29390785
29391030, 29391237, 29391438, 29391849, 29391925, 29392966, 29393291
29394014, 29394140, 29394749, 29395657, 29397954, 29397996, 29398488
29398863, 29399046, 29399100, 29399121, 29399336, 29399938, 29402131
29404483, 29405012, 29405462, 29405651, 29405996, 29407488, 29407804
29408853, 29409149, 29409455, 29410311, 29410834, 29411037, 29411469
29412066, 29412269, 29413382, 29413517, 29413544, 29413634, 29416688
29416700, 29417084, 29417173, 29417719, 29417884, 29418165, 29420834
29421059, 29423003, 29423016, 29423156, 29423826, 29424999, 29426241
29426320, 29429017, 29429087, 29429264, 29429466, 29429566, 29430524
29430866, 29431192, 29431485, 29432176, 29434301, 29435474, 29435652
29436454, 29436514, 29436522, 29436727, 29437594, 29437712, 29438150
29438277, 29438736, 29439522, 29441196, 29443187, 29443250, 29444072
29444282, 29444602, 29446669, 29448498, 29449477, 29449845, 29449852
29450162, 29450193, 29450421, 29450812, 29450936, 29451386, 29452251
29452576, 29452936, 29452953, 29454978, 29455424, 29456538, 29456714
29457312, 29457370, 29457502, 29457807, 29457978, 29460252, 29461420
29461791, 29462594, 29462767, 29462957, 29463047, 29463528, 29463798
29464616, 29464779, 29465177, 29466674, 29467622, 29469565, 29470291
29471832, 29471860, 29472618, 29473708, 29476473, 29481584, 29483452
29483532, 29483626, 29483672, 29483685, 29483712, 29483723, 29483771
29485099, 29486181, 29486848, 29487189, 29488894, 29489436, 29489546
29490256, 29492127, 29492939, 29493122, 29494245, 29495057, 29495684
29497311, 29497588, 29497696, 29498198, 29500257, 29500826, 29500963
29502561, 29503543, 29503631, 29503827, 29504492, 29504682, 29505668
29507270, 29507616, 29508681, 29509777, 29510278, 29511611, 29511980
29512890, 29514479, 29515134, 29515240, 29515476, 29515766, 29515834
29516300, 29516727, 29516766, 29517168, 29517883, 29519131, 29521187
29521688, 29521748, 29521862, 29522358, 29522561, 29522662, 29523055
29523216, 29523511, 29524599, 29524985, 29525467, 29525886, 29526966
29527595, 29527610, 29528368, 29529147, 29530440, 29530515, 29530812
29530909, 29531654, 29531836, 29532532, 29536342, 29536445, 29538631
29541742, 29541769, 29542084, 29542449, 29542580, 29542643, 29543034
29543956, 29546817, 29547010, 29547867, 29548427, 29548592, 29548687
29548722, 29549040, 29549071, 29549104, 29549730, 29552773, 29553141
29554092, 29557144, 29557261, 29557336, 29557556, 29558238, 29558452
29558975, 29559187, 29559446, 29559908, 29559981, 29564592, 29564593
29565611, 29580394, 29580983, 29581771, 29584261, 29584693, 29586143
29587765, 29589544, 29591343, 29592215, 29597536, 29597754, 29598039
29598046, 29598233, 29599008, 29599300, 29601461, 29602831, 29603460
29603884, 29604002, 29604257, 29607136, 29607797, 29608000, 29610506
29611020, 29611991, 29615824, 29616244, 29616414, 29618074, 29618190
29620042, 29622936, 29625065, 29625804, 29625876, 29626154, 29626732
29628200, 29629430, 29629650, 29629681, 29629745, 29631749, 29632095
29632265, 29632611, 29633697, 29633753, 29633936, 29634643, 29635427
29635717, 29635990, 29637362, 29637526, 29638285, 29641736, 29643721
29644464, 29645349, 29647176, 29648928, 29651183, 29651520, 29653132
29653246, 29655668, 29656400, 29656819, 29656843, 29657399, 29657422
29657744, 29657960, 29661028, 29661065, 29661722, 29663191, 29663368
29663494, 29663601, 29664087, 29664161, 29665940, 29667527, 29667994
29668005, 29669413, 29670782, 29671363, 29672507, 29675446, 29676089
29677051, 29677173, 29677733, 29677927, 29679856, 29681987, 29683039
```

```
29683211, 29684518, 29685137, 29685276, 29687214, 29687220, 29687459
29687718, 29687763, 29689145, 29689255, 29692694, 29694869, 29695425
29695841, 29696310, 29700125, 29700460, 29700770, 29703932, 29707099
29707493, 29707896, 29708915, 29710188, 29710858, 29713810, 29715220
29716194, 29716227, 29716491, 29716871, 29717659, 29719146, 29720133
29721418, 29721576, 29724658, 29725476, 29725781, 29726695, 29738400
29739576, 29741976, 29742223, 29744225, 29746962, 29747493, 29747648
29747653, 29748285, 29748336, 29748513, 29749471, 29750673, 29751094
29753244, 29754196, 29754951, 29755821, 29756274, 29756444, 29757099
29757264, 29757651, 29758203, 29758217, 29758661, 29761678, 29761837
29761911, 29763158, 29765035, 29765393, 29766207, 29766503, 29766679
29768899, 29770750, 29771032, 29771242, 29773197, 29773842, 29775393
29779196, 29780140, 29782211, 29782823, 29782866, 29784106, 29785239
29787292, 29787766, 29791152, 29791880, 29792213, 29793318, 29794174
29794462, 29795712, 29795957, 29796378, 29797726, 29802695, 29804875
29805772, 29807964, 29809792, 29809837, 29812489, 29813503, 29813650
29813671, 29815713, 29817278, 29817784, 29821582, 29825525, 29827647
29827852, 29831196, 29834506, 29836096, 29838485, 29838773, 29839715
29840619, 29841267, 29841687, 29843277, 29843692, 29843831, 29844226
29845530, 29846126, 29846645, 29846688, 29848084, 29848849, 29849100
29850930, 29851733, 29853485, 29856859, 29858121, 29858376, 29859068
29860994, 29861075, 29864203, 29864261, 29865188, 29865590, 29865658
29869086, 29869404, 29869887, 29870065, 29871098, 29872401, 29872937
29872983, 29873665, 29875459, 29875565, 29876358, 29876989, 29877608
29878076, 29881050, 29881478, 29881643, 29881839, 29882427, 29882729
29884958, 29885890, 29887111, 29888621, 29889184, 29890740, 29891075
29891853, 29891916, 29892604, 29893132, 29896510, 29897418, 29897863
29900203, 29900824, 29902299, 29902327, 29902330, 29902659, 29903190
29903299, 29903454, 29904002, 29906678, 29907942, 29908389, 29908777
29909658, 29910402, 29912286, 29913966, 29914449, 29914544, 29915217
29915848, 29916975, 29919789, 29920025, 29920376, 29920804, 29921318
29923452, 29926466, 29927756, 29928210, 29928427, 29928564, 29932202
29932430, 29932780, 29934052, 29937565, 29938225, 29939400, 29939795
29940373, 29942096, 29942554, 29943670, 29944035, 29944660, 29944963
29945645, 29946388, 29947145, 29950220, 29951620, 29956016, 29956222
29957412, 29957493, 29961353, 29961609, 29962160, 29962248, 29962834
29962927, 29962939, 29965052, 29965603, 29965888, 29966768, 29967223
29968085, 29969557, 29970298, 29971027, 29971481, 29971888, 29971951
29972176, 29973012, 29989783, 29989845, 29991257, 29993717, 29997326
29997553, 30000664, 30001331, 30003187, 30006159, 30006985, 30007450
30007797, 30008125, 30008198, 30008214, 30009710, 30012181, 30015070
30017836, 30018017, 30019864, 30024618, 30025814, 30026016, 30028599
30029519, 30029806, 30031027, 30032376, 30033547, 30034456, 30035598
30038392, 30039800, 30039959, 30040157, 30041501, 30042490, 30043398
30043610, 30043930, 30044507, 30046497, 30047531, 30047702, 30047765
30047931, 30049966, 30051176, 30051783, 30051804, 30052928, 30053036
30053501, 30053748, 30054980, 30056058, 30057718, 30057799, 30058149
30058453, 30059106, 30059109, 30062364, 30064268, 30066352, 30067565
30071446, 30072905, 30073314, 30073744, 30074296, 30074349, 30074469
30074472, 30075037, 30076058, 30076197, 30076253, 30078675, 30078934
30079949, 30080266, 30081546, 30081580, 30082145, 30083100, 30083216
30083488, 30083807, 30084971, 30085897, 30086596, 30086992, 30090568
30092859, 30095591, 30095952, 30097092, 30097115, 30098251, 30099302
30099420, 30099454, 30100354, 30101186, 30103551, 30103553, 30104378
30104555, 30106748, 30109365, 30110224, 30110370, 30110518, 30114477
30114489, 30114534, 30116085, 30116854, 30117335, 30117593, 30118261
30118279, 30120608, 30122583, 30127522, 30127904, 30128047, 30131286
30131645, 30135396, 30135731, 30135942, 30136346, 30139392, 30142907
30143470, 30143593, 30147473, 30147928, 30149035, 30149658, 30150606
30153885, 30154633, 30155814, 30155837, 30159329, 30159511, 30159536
30159752, 30159760, 30163243, 30164714, 30165493, 30165503, 30165897
30169254, 30170104, 30172925, 30173113, 30173556, 30174401, 30175291
30177597, 30178250, 30178839, 30178990, 30179644, 30180208, 30181756
30183920, 30184102, 30185852, 30186319, 30186476, 30186706, 30187866
30189516, 30190090, 30191274, 30193165, 30193505, 30194612, 30194710
30194972, 30195667, 30195668, 30195684, 30196195, 30196358, 30198861
```

```
30198905, 30200034, 30200237, 30200758, 30202349, 30202388, 30204542
30206493, 30206675, 30207473, 30208327, 30209736, 30210884, 30213031
30213540, 30215130, 30215302, 30215351, 30217206, 30217982, 30218044
30218317, 30221237, 30222512, 30223712, 30223847, 30224650, 30224868
30224950, 30225265, 30225718, 30225844, 30228567, 30229683, 30232638
30235919, 30235979, 30236554, 30238211, 30239480, 30240010, 30241567
30242120, 30242724, 30244340, 30246053, 30246179, 30247305, 30249432
30252005, 30252098, 30252156, 30252458, 30252977, 30253035, 30253090
30253608, 30253835, 30254525, 30254726, 30255143, 30255528, 30256542
30257412, 30264405, 30265523, 30265608, 30265703, 30266791, 30267155
30269428, 30269748, 30270647, 30270744, 30271114, 30272329, 30274090
30274188, 30274324, 30275578, 30276243, 30277120, 30277451, 30282501
30282591, 30283296, 30283577, 30283579, 30283581, 30283932, 30284219
30284369, 30285457, 30285843, 30288343, 30288491, 30289458, 30294267
30294671, 30295110, 30295549, 30299367, 30299817, 30299934, 30300030
30300538, 30305264, 30305395, 30305568, 30305880, 30307814, 30307883
30308368, 30308624, 30308772, 30309098, 30309798, 30312094, 30313848
30314079, 30314837, 30316667, 30317209, 30318638, 30318943, 30319080
30322980, 30323658, 30323849, 30324180, 30327149, 30328168, 30330123
30334484, 30334563, 30335127, 30335832, 30335987, 30336032, 30336742
30339103, 30341713, 30342371, 30342878, 30345201, 30352581, 30352623
30355490, 30357463, 30362003, 30362850, 30363716, 30364329, 30364613
30365745, 30367193, 30368048, 30368534, 30371909, 30374345, 30374570
30374739, 30375109, 30381525, 30383286, 30384121, 30384152, 30389229
30389414, 30389507, 30392011, 30394738, 30394974, 30398257, 30398422
30399906, 30402386, 30403763, 30403902, 30403989, 30404117, 30408515
30408808, 30409207, 30409339, 30409590, 30412188, 30412921, 30413137
30414714, 30416034, 30421476, 30422487, 30424347, 30430921, 30431274
30431504, 30431698, 30431703, 30431717, 30441687, 30441959, 30442749
30442884, 30447060, 30448917, 30449194, 30453442, 30454090, 30458568
30458593, 30460922, 30463938, 30464250, 30469777, 30474167, 30474774
30475115, 30477588, 30477767, 30479715, 30485255, 30490014, 30493518
30495133, 30495483, 30496957, 30497057, 30500344, 30501574, 30503943
30505497, 30506794, 30507032, 30509277, 30510347, 30510527, 30513285
30513848, 30516868, 30517214, 30522285, 30523750, 30534351, 30534549
30534827, 30537405, 30537533, 30540109, 30544247, 30545281, 30549637
30549789, 30549881, 30564139, 30573703, 30576393, 30577071, 30579051
30582500, 30592859, 30598682, 30598746, 30599405, 30600184, 30602230
30609799, 30612199, 30613937, 30613971, 30619787, 30623142, 30629799
30633259, 30635302, 30641755, 30654558, 30657875, 30661939, 30662651
30671813, 30676209, 30708735, 30720736, 30730026, 30732711, 30741263
30761878, 30776416, 30783551, 30785101, 30790441, 30803210, 30808869
30815852, 30825391, 30825419, 30881407, 30886188, 30890971, 30919691
30922996, 30993198, 31016413, 29997959, 29997937, 28852325, 28730253
29213893, 30528704, 29540327, 29254623, 29445548, 29774362, 30134746
30160625, 29942275, 30534662, 29512125, 30855101, 27222128, 27572040
27604329, 27760043, 27877830, 28302580, 28470673, 28621543, 28642469
28699321, 28710663, 28755846, 28772816, 28785321, 28800508, 28808652
28815557, 28847541, 28847572, 28870496, 28871040, 28874416, 28877252
28881191, 28881848, 28888083, 28911140, 28925250, 28925460, 28935956
28940472, 3, 28942694, 28951332, 28963036, 28968779, 28980448, 28995287
29003207, 29003617, 29016294, 29018680, 29024876, 29026154, 29027933
29047127, 29052850, 29058476, 29111631, 29112455, 29117337, 29123444
29125708, 29125786, 29129476, 29131772, 29132456, 29139727, 29146157
29147849, 29149170, 29152603, 29152752, 29154631, 29154636, 29154829
29159216, 29159661, 29160462, 29161923, 29169540, 29169739, 29170717
29173618, 29181568, 29182920, 29183298, 29186091, 29191827, 29201143
29201695, 29209545, 29210577, 29210610, 29210624, 29210683, 29213641
29219627, 29224294, 29225861, 29229839, 29235934, 29242906, 29243749
29244495, 29244766, 29244968, 29248723, 29249583, 29251564, 29255616
29260224, 29261695, 29271019, 29273360, 29282090, 29282666, 29285453
29285621, 29290235, 29292232, 29293806, 29294753, 29299830, 29307090
29307109, 29311336, 29329675, 29330791, 29339299, 29357821, 29360467
29360775, 29367971, 29368725, 29379299, 29379381, 29380527, 29381000
29382296, 29391301, 29393649, 29402110, 29411931, 29413360, 29457319
29465047
```

Version 19.0.0.0.ru-2020-01.rur-2020-01.r1

La version 19.0.0.0.ru-2020-01.rur-2020-01.r1 comprend ce qui suit :

- Correctif 30557433 : Mise à jour de version de base de données : 19.6.0.0.200114
- Correctif 30484981 : MISE À JOUR DE VERSION OJVM : 19.6.0.0.200114
- Correctif 29997937 : MISE À JOUR DSTv34 pour SGBDR (TZDATA2019B)
- Correctif 29997959 : MISE À JOUR DSTV34 pour OJVM (TZDATA2019B)
- PreUpgrade Jar : preupgrade_19_cbuild_5_lf.zip
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS
- Correctif 29213893 : DBMS_ÉCHEC DES STATS AVEC ERREUR ORA-01422 LORS DU REGROUPEMENT DES STATS POUR LA TABLE UTILIATEUR$
- Correctif 30528704 : 19C RMAN RÉCUPÉRATION DU JOURNAL REDO D'UTILISATION DE BASE DE DONNÉES AU LIEU D'ARCHIVELOG APRÈS APPLICATION DE LA MISE À JOUR DE BASE DE DONNÉES D'OCT

Mise à jour de version Oracle 19.6.0.0.200114, publiée en janvier 2020

Bogues corrigés :

```
30545281, 8476681, 14735102, 17428816, 19080742, 19697993, 20313356
21374587, 21965541, 23296836, 23606241, 24687075, 25756945, 25806201
25883179, 25986062, 25997810, 26476244, 26611353, 26739322, 26777814
26872233, 27036163, 27044169, 27101798, 27126938, 27195935, 27244999
27254335, 27359766, 27369515, 27406105, 27411022, 27423500, 27439716
27453490, 27458357, 27489107, 27666312, 27710072, 27729678, 27846298
27880025, 27934711, 27935464, 27941110, 27957203, 27967484, 28064977
28072567, 28109326, 28125947, 28129791, 28181021, 28189466, 28204262
28205555, 28209985, 28210681, 28271258, 28271693, 28279456, 28294563
28313275, 28319114, 28326928, 28350595, 28371123, 28373960, 28375383
28379065, 28381939, 28386259, 28390273, 28395302, 28397317, 28402823
28410431, 28431445, 28435333, 28454215, 28463226, 28475242, 28484299
28489419, 28492006, 28498976, 28502773, 28513333, 28521330, 28530171
28534475, 28538439, 28542455, 28546290, 28547068, 28547926, 28558645
28561704, 28567417, 28567819, 28569897, 28572407, 28572533, 28572544
28572667, 28572834, 28578945, 28587723, 28589509, 28593682, 28594086
28597221, 28601957, 28605066, 28606598, 28612239, 28620697, 28625862
28627033, 28636532, 28639299, 28643718, 28644549, 28645570, 28646200
28646939, 28649388, 28655209, 28663782, 28672457, 28673945, 28692103
28692275, 28694872, 28696373, 28705231, 28710385, 28710734, 28714461
28715727, 28718469, 28719348, 28720204, 28720418, 28721497, 28722229
28730079, 28734355, 28740708, 28742555, 28749853, 28752923, 28755011
28758722, 28760206, 28765983, 28767240, 28769456, 28772390, 28774416
28776811, 28777214, 28781754, 28785531, 28789531, 28791852, 28795551
28795734, 28802734, 28804517, 28810381, 28811560, 28815123, 28815355
28817449, 28819640, 28820669, 28821847, 28824482, 28827682, 28831971
28833912, 28835937, 28836716, 28844738, 28849776, 28854004, 28855520
28855922, 28857552, 28862532, 28863432, 28863487, 28867992, 28873575
28875089, 28876253, 28876639, 28878865, 28882784, 28884931, 28887305
28888327, 28889730, 28892794, 28897512, 28899663, 28901126, 28905457
28905615, 28907196, 28912691, 28915561, 28917080, 28918429, 28919145
28922227, 28922532, 28922608, 28925634, 28925880, 28927452, 28932914
28933158, 28935293, 28936114, 28937717, 28938698, 28940179, 28940281
28941901, 28942455, 28945421, 28945994, 28949888, 28950868, 28951533
28952168, 28954762, 28955606, 28955883, 28956908, 28957292, 28957723
```

```
28958088, 28959493, 28960863, 28962775, 28965084, 28965095, 28965231
28965376, 28966444, 28974083, 28977322, 28983095, 28983486, 28985478
28986207, 28986231, 28986257, 28986326, 28986481, 28988482, 28989306
28993295, 28993353, 28994307, 28996376, 29000000, 29001305, 29001888
29002488, 29002784, 29002927, 29003407, 29003738, 29006318, 29006621
29007321, 29007353, 29007775, 29008035, 29008669, 29009513, 29010126
29011936, 29012609, 29013475, 29013832, 29014076, 29015118, 29017265
29018655, 29019121, 29021063, 29021352, 29022986, 29024054, 29024552
29024732, 29026582, 29026606, 29027456, 29027694, 29027940, 29031575
29031600, 29032234, 29032276, 29032457, 29032607, 29033052, 29033145
29033200, 29033280, 29034587, 29037290, 29038528, 29038728, 29039089
29039510, 29040739, 29043554, 29043651, 29043725, 29044763, 29044954
29046482, 29047850, 29048178, 29048289, 29048498, 29048605, 29050357
29050560, 29050765, 29050886, 29051702, 29051953, 29052726, 29053783
29056024, 29056270, 29056560, 29056767, 29056894, 29059011, 29060216
29061016, 29061959, 29062692, 29062848, 29062860, 29062868, 29110526
29110783, 29110790, 29110797, 29110802, 29110805, 29111598, 29113282
29113305, 29115857, 29117526, 29117642, 29118543, 29119077, 29120223
29122224, 29122254, 29123297, 29123432, 29123482, 29124368, 29125036
29125374, 29125380, 29126345, 29127957, 29128693, 29128935, 29129450
29129497, 29129712, 29130219, 29131539, 29132869, 29132938, 29133470
29134447, 29135383, 29135649, 29136111, 29138641, 29139956, 29141316
29141341, 29141685, 29142609, 29142667, 29143516, 29144995, 29145214
29145730, 29149829, 29150338, 29151520, 29152357, 29155099, 29157051
29157389, 29158680, 29158899, 29159909, 29159936, 29160174, 29162095
29163156, 29163415, 29163437, 29163524, 29163567, 29167111, 29167342
29167374, 29167940, 29168137, 29168219, 29168433, 29169073, 29169215
29170232, 29171683, 29171942, 29172618, 29172826, 29173140, 29173373
29173817, 29174004, 29176318, 29177466, 29177543, 29177886, 29178385
29180313, 29180455, 29180559, 29180893, 29181153, 29181231, 29181620
29181743, 29181923, 29182019, 29182517, 29182901, 29183912, 29184297
29184666, 29185193, 29186456, 29189302, 29189307, 29189889, 29190235
29190474, 29190663, 29190740, 29191541, 29192419, 29192468, 29192685
29193207, 29194205, 29194367, 29194493, 29194827, 29194981, 29195279
29195337, 29195758, 29196725, 29198092, 29198913, 29199635, 29199733
29200316, 29200700, 29201494, 29201539, 29201787, 29202104, 29202461
29202850, 29203122, 29203166, 29203425, 29203443, 29203604, 29205281
29205323, 29205419, 29205463, 29205767, 29205918, 29206109, 29206605
29207073, 29208260, 29208732, 29211457, 29211724, 29212012, 29212433
29212611, 29213320, 29213351, 29213613, 29213775, 29213850, 29213879
29214561, 29214960, 29216312, 29216723, 29216746, 29216984, 29217294
29217472, 29217828, 29217848, 29218570, 29219205, 29219273, 29220079
29221248, 29221891, 29221942, 29222031, 29222784, 29223833, 29223859
29223967, 29224065, 29224605, 29225076, 29225168, 29225758, 29227602
29228869, 29229164, 29229754, 29229844, 29229955, 29230252, 29230565
29231133, 29232117, 29232154, 29232449, 29233415, 29233810, 29233953
29234123, 29236573, 29237538, 29237575, 29237744, 29240307, 29240759
29241345, 29241651, 29242017, 29242884, 29243958, 29245137, 29245160
29246163, 29247415, 29247712, 29247906, 29248495, 29248552, 29248835
29248858, 29249412, 29249991, 29250059, 29250317, 29251259, 29253184
29253871, 29254031, 29254930, 29255178, 29255273, 29255431, 29255435
29256426, 29259119, 29259320, 29260452, 29260956, 29261547, 29261548
29261906, 29262512, 29262887, 29265448, 29266248, 29266899, 29267292
29268412, 29269171, 29269228, 29269825, 29270585, 29273539, 29273570
29273735, 29273812, 29273847, 29274428, 29274564, 29274627, 29275461
29276272, 29277317, 29278218, 29278684, 29279658, 29279751, 29279854
29281527, 29281691, 29281796, 29282233, 29282898, 29285197, 29285503
29285788, 29285956, 29286037, 29286229, 29287130, 29287705, 29292837
29293072, 29293574, 29297863, 29297915, 29298220, 29299049, 29299082
29299844, 29301463, 29301566, 29302963, 29303918, 29304781, 29306226
29306713, 29307638, 29311528, 29311588, 29312310, 29312672, 29312734
29312753, 29312889, 29313347, 29313417, 29313525, 29314539, 29314636
29317756, 29318410, 29319441, 29321489, 29323946, 29324568, 29324735
29325087, 29325105, 29325257, 29325765, 29325993, 29327044, 29329042
29329087, 29329807, 29330361, 29331066, 29331209, 29331380, 29331493
29332292, 29332395, 29332763, 29332771, 29333500, 29336843, 29337310
```

```
29337742, 29338315, 29338348, 29338453, 29338780, 29338913, 29339101
29339155, 29341209, 29343086, 29343861, 29345937, 29346057, 29346211
29346943, 29347620, 29348176, 29350052, 29350762, 29351386, 29351662
29351716, 29351735, 29351749, 29352298, 29352724, 29352867, 29352947
29353271, 29353432, 29353821, 29353960, 29355654, 29356547, 29356704
29356711, 29356752, 29358509, 29358828, 29360252, 29360285, 29360672
29360911, 29360950, 29361319, 29361472, 29361801, 29363151, 29364171
29364177, 29366940, 29367019, 29367561, 29368253, 29368310, 29372541
29373418, 29373588, 29374179, 29375355, 29375941, 29375984, 29376346
29377804, 29377986, 29378029, 29378834, 29378913, 29379978, 29382641
29382784, 29382815, 29383695, 29384781, 29384854, 29384864, 29385429
29385652, 29386502, 29386635, 29386660, 29387073, 29387274, 29388020
29388072, 29388094, 29388524, 29388830, 29389889, 29390011, 29390435
29390785, 29391030, 29391237, 29391849, 29391925, 29392966, 29393291
29394014, 29394140, 29394749, 29395657, 29397954, 29397996, 29398488
29398863, 29399046, 29399100, 29399121, 29399336, 29399938, 29402131
29404483, 29405012, 29405462, 29405651, 29405996, 29407804, 29408853
29409149, 29409455, 29410311, 29410834, 29411037, 29411469, 29412066
29412269, 29416688, 29417173, 29417719, 29417884, 29418165, 29420834
29421059, 29423003, 29423016, 29423156, 29423826, 29424999, 29426241
29429017, 29429264, 29429466, 29429566, 29430524, 29430866, 29431192
29431485, 29432176, 29434301, 29435474, 29435652, 29436454, 29436514
29436727, 29437594, 29437712, 29438277, 29438736, 29439522, 29441196
29443187, 29443250, 29444072, 29444282, 29444602, 29446669, 29448498
29449477, 29449845, 29449852, 29450193, 29450421, 29450812, 29450936
29451386, 29452251, 29452576, 29452936, 29452953, 29454978, 29455424
29456714, 29457312, 29457370, 29457502, 29457807, 29457978, 29460252
29461420, 29461791, 29462594, 29462767, 29462957, 29463047, 29463528
29464616, 29464779, 29465177, 29467622, 29469565, 29470291, 29471860
29472618, 29476473, 29481584, 29483452, 29483532, 29483626, 29483672
29483685, 29483712, 29483723, 29483771, 29485099, 29486181, 29488894
29489436, 29489546, 29490256, 29492127, 29492939, 29493122, 29494245
29495057, 29495684, 29497311, 29497588, 29497696, 29498198, 29500257
29500826, 29502561, 29503543, 29503631, 29503827, 29504492, 29504682
29505668, 29507270, 29507616, 29508681, 29509777, 29510278, 29511611
29514479, 29515134, 29515240, 29515476, 29515766, 29515834, 29516300
29516727, 29516766, 29517168, 29517883, 29521187, 29521688, 29521748
29521862, 29522358, 29522561, 29522662, 29523055, 29523511, 29524599
29525467, 29525886, 29526966, 29527595, 29527610, 29528368, 29529147
29530440, 29530515, 29530812, 29530909, 29531654, 29531836, 29532532
29536342, 29536445, 29538631, 29541742, 29541769, 29542084, 29542449
29542643, 29543034, 29543956, 29546817, 29547010, 29547867, 29548427
29548687, 29548722, 29549071, 29549104, 29549154, 29549730, 29552773
29553141, 29557144, 29557261, 29557336, 29557556, 29558238, 29558975
29559187, 29559446, 29559908, 29559981, 29564592, 29564593, 29565611
29580394, 29580983, 29581771, 29584261, 29584693, 29586143, 29587765
29597536, 29597754, 29598039, 29598046, 29598233, 29599008, 29599300
29601461, 29602831, 29603460, 29603884, 29604002, 29604257, 29607136
29607797, 29608000, 29610506, 29611020, 29611991, 29615824, 29616244
29616414, 29618074, 29618190, 29620042, 29622936, 29625065, 29625804
29625876, 29626154, 29626732, 29628200, 29629430, 29629650, 29629681
29629745, 29631749, 29632095, 29632265, 29632611, 29633697, 29633753
29633936, 29634643, 29635427, 29635717, 29635990, 29637362, 29637526
29638285, 29641736, 29643721, 29645349, 29648928, 29651183, 29651520
29653132, 29653246, 29655668, 29656819, 29657422, 29657960, 29661028
29661065, 29661722, 29663368, 29664087, 29664161, 29665940, 29667994
29668005, 29669413, 29670782, 29671363, 29672507, 29676089, 29677051
29677173, 29677733, 29677927, 29679856, 29681987, 29683039, 29687214
29687459, 29687718, 29687763, 29689145, 29689255, 29692694, 29694869
29695425, 29695841, 29696310, 29700125, 29700460, 29700770, 29703932
29707099, 29707896, 29708915, 29710188, 29710858, 29713810, 29715220
29716194, 29716491, 29717659, 29719146, 29720133, 29721418, 29725476
29725781, 29726695, 29739576, 29741976, 29742223, 29746962, 29747493
29747648, 29747653, 29748285, 29748336, 29748513, 29749471, 29750673
29751094, 29753244, 29754951, 29755821, 29756274, 29756444, 29757099
29757264, 29757651, 29758217, 29758661, 29761678, 29761837, 29761911
```

```
29765393, 29766207, 29766503, 29766679, 29768899, 29770750, 29771032
29771242, 29773197, 29773842, 29775393, 29779196, 29782211, 29782823
29782866, 29784106, 29785239, 29787292, 29787766, 29791152, 29791880
29793318, 29794462, 29795712, 29795957, 29796378, 29797726, 29802695
29804875, 29805772, 29809837, 29812489, 29813503, 29815713, 29817278
29821582, 29825525, 29827852, 29831196, 29834506, 29836096, 29838485
29838773, 29839715, 29840619, 29841267, 29841687, 29843277, 29843692
29844226, 29845530, 29846126, 29846645, 29848084, 29848849, 29849100
29850930, 29851733, 29853485, 29858121, 29858376, 29865188, 29865658
29869086, 29869404, 29869887, 29870065, 29871098, 29873665, 29875459
29875565, 29877608, 29878076, 29881478, 29881839, 29882729, 29884958
29887111, 29888621, 29890740, 29891916, 29893132, 29897418, 29897863
29900203, 29902327, 29902330, 29903299, 29903454, 29906678, 29907942
29909658, 29912286, 29914449, 29915217, 29915848, 29916975, 29920025
29921318, 29926466, 29927756, 29928210, 29937565, 29938225, 29940373
29942096, 29942554, 29943670, 29944035, 29944660, 29945645, 29946388
29951620, 29956016, 29957493, 29961609, 29962248, 29962927, 29962939
29966768, 29967223, 29968085, 29970298, 29971027, 29971888, 29989783
29989845, 29991257, 29997326, 30003187, 30006159, 30006985, 30007797
30008125, 30008214, 30009710, 30015070, 30019864, 30024618, 30029806
30032376, 30033547, 30034456, 30035598, 30038392, 30040157, 30042490
30043610, 30044507, 30047702, 30047765, 30051176, 30051783, 30053036
30058149, 30058453, 30059106, 30059109, 30066352, 30074349, 30074472
30075037, 30076197, 30078675, 30079949, 30080266, 30081580, 30083488
30084971, 30085897, 30086992, 30090568, 30092859, 30095591, 30095952
30097092, 30098251, 30099454, 30101186, 30104555, 30106748, 30110224
30110370, 30110518, 30114489, 30114534, 30127522, 30127904, 30131645
30135396, 30142907, 30149658, 30150606, 30154633, 30155837, 30159329
30164714, 30165493, 30165503, 30170104, 30174401, 30175291, 30177597
30178250, 30187866, 30189516, 30191274, 30193165, 30206493, 30218044
30223712, 30223847, 30224950, 30235919, 30246179, 30247305, 30252098
30252156, 30253608, 30255143, 30264405, 30266791, 30269428, 30274188
30282591, 30299817, 30312094, 30318638, 30324180, 30342878, 30365745
30389229, 30402386, 30408515, 30412188, 30453442, 30458593, 30474167
30474774, 30485255, 30534827, 30641755
```

Version 19.0.0.0.ru-2019-10.rur-2019-10.r1

La version 19.0.0.0.ru-2019-10.rur-2019-10.r1 comprend ce qui suit :

- Correctif 30125133 : MISE À JOUR DE VERSION DE BASE DE DONNÉES 19.5.0.0.0
- Correctif 30128191 : MISE À JOUR VERSION OJVM 19.5.0.0.0
- Correctif 29997937 : MISE À JOUR DSTv34 pour SGBDR (TZDATA2019B)
- Correctif 29997959 : MISE À JOUR DSTV34 pour OJVM (TZDATA2019B)
- PreUpgrade Jar : preupgrade_19_cbuild_4_lf.zip
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS
- Correctif 29213893 : DBMS_ÉCHEC DES STATS AVEC ERREUR ORA-01422 LORS DU REGROUPEMENT DES STATS POUR LA TABLE UTILIATEUR$
- Correctif 30528704 : 19C RMAN RÉCUPÉRATION DU JOURNAL REDO D'UTILISATION DE BASE DE DONNÉES AU LIEU D'ARCHIVELOG APRÈS APPLICATION DE LA MISE À JOUR DE BASE DE DONNÉES D'OCT
- Prise en charge de Redimensionnement de l'espace de table temporaire dans un réplica en lecture (p. 1128)

Mise à jour de version Oracle 19.5.0.0.0, publiée en octobre 2019

Bogues corrigés :

```
                    14735102, 17428816, 19080742, 19697993, 20313356, 21374587, 21965541
23296836, 23606241, 24687075, 25756945,
                    25806201, 25883179, 25986062 25997810, 26476244, 26611353, 26739322,
26872233, 27126938, 27244999 27359766,
                    27369515, 27406105, 27411022, 27423500, 27453490, 27458357 27489107,
27666312, 27710072, 27846298, 27880025,
                    27934711, 27935464 27941110, 27957203, 27967484, 28064977, 28072567,
28125947, 28129791 28181021, 28210681,
                    28271693, 28279456, 28294563, 28313275, 28319114 28326928, 28350595,
28371123, 28379065, 28381939, 28386259,
                    28390273 28395302, 28410431, 28431445, 28435333, 28463226, 28475242,
28484299 28489419, 28498976, 28502773,
                    28513333, 28521330, 28534475, 28542455 28547068, 28558645, 28561704,
28567417, 28567819, 28569897, 28572533,
                    28572544, 28572667, 28572834, 28587723, 28593682, 28594086, 28597221
28601957, 28605066, 28606598, 28612239,
                    28625862, 28627033, 28636532 28643718, 28644549, 28645570, 28646200,
28646939, 28649388, 28655209 28663782,
                    28672457, 28673945, 28692103, 28692275, 28694872, 28696373 28705231,
28710385, 28710734, 28714461, 28715727,
                    28718469, 28719348 28720418, 28721497, 28722229, 28730079, 28740708,
28742555, 28749853 28752923, 28755011,
                    28758722, 28760206, 28765983, 28767240, 28769456 28772390, 28774416,
28776811, 28777214, 28781754, 28785531,
                    28789531 28791852, 28795551, 28802734, 28804517, 28810381, 28811560,
28815123 28815355, 28817449, 28819640,
                    28820669, 28824482, 28827682, 28831971 28833912, 28835937, 28836716,
28849776, 28854004, 28855922, 28862532
                    28863432, 28863487, 28867992, 28873575, 28875089, 28876253, 28876639
28878865, 28884931, 28888327, 28889730,
                    28892794, 28897512, 28899663 28901126, 28905457, 28907196, 28912691,
28915561, 28917080, 28918429 28919145,
                    28922227, 28922532, 28922608, 28925634, 28925880, 28933158 28936114,
28937717, 28938698, 28940179, 28940281,
                    28941901, 28942455 28945421, 28945994, 28950868, 28951533, 28952168,
28954762, 28955606 28956908, 28957292,
                    28957723, 28958088, 28960863, 28962775, 28965084 28965231, 28966444,
28974083, 28977322, 28983095, 28983486,
                    28985478 28986207, 28986231, 28986326, 28986481, 28988482, 28989306,
28993295 28993353, 28994307, 28996376,
                    29000000, 29001305, 29001888, 29002488 29002784, 29002927, 29003738,
29006318, 29006621, 29007321, 29007353,
                    29007775, 29008035, 29008669, 29009513, 29010126, 29011936, 29012609
29013475, 29014076, 29015118, 29017265,
                    29018655, 29019121, 29021063 29021352, 29024054, 29024552, 29024732,
29026582, 29026606, 29027456 29027694,
                    29027940, 29031575, 29031600, 29032234, 29032276, 29032457 29032607,
29033052, 29033145, 29033200, 29033280,
                    29034587, 29037290 29038528, 29039089, 29039510, 29040739, 29043554,
29043651, 29043725 29044763, 29044954,
                    29047850, 29048178, 29048289, 29048498, 29048605 29050357, 29050560,
29050765, 29050886, 29051702, 29051953,
                    29052726 29053783, 29056024, 29056270, 29056560, 29056767, 29059011,
29060216 29061959, 29062692, 29062848,
                    29062860, 29062868, 29110526, 29110783 29110790, 29110797, 29110802,
29110805, 29111598, 29113282, 29113305
                    29117526, 29117642, 29119077, 29120223, 29122224, 29122254, 29123297
29123432, 29123482, 29124368, 29125036,
                    29125374, 29125380, 29126345 29127957, 29128693, 29128935, 29129450,
29129497, 29129712, 29130219 29131539,
                    29132869, 29132938, 29134447, 29135383, 29135649, 29136111 29138641,
29139956, 29141316, 29141341, 29141685,
                    29142609, 29142667 29143516, 29144995, 29145214, 29145730, 29149829,
29150338, 29151520 29152357, 29155099,
```

```
                    29157051, 29157389, 29158680, 29158899, 29159909 29159936, 29160174,
29162095, 29163156, 29163415, 29163437,
                    29163524 29163567, 29167111, 29167342, 29167374, 29167940, 29168137,
29168219 29168433, 29169073, 29169215,
                    29170232, 29171683, 29171942, 29172618 29172826, 29173140, 29173373,
29173817, 29174004, 29176318, 29177466,
                    29177543, 29177886, 29178385, 29180313, 29180455, 29180559, 29180893
29181153, 29181231, 29181620, 29181743,
                    29181923, 29182019, 29183912 29184297, 29184666, 29185193, 29186456,
29189302, 29189307, 29189889 29190235,
                    29190474, 29190740, 29191541, 29192419, 29192468, 29192685 29193207,
29194205, 29194367, 29194493, 29194827,
                    29194981, 29195279 29195337, 29195758, 29196725, 29198092, 29199635,
29199733, 29200316 29200700, 29201494,
                    29201539, 29202104, 29202850, 29203122, 29203166 29203425, 29203443,
29203604, 29205281, 29205323, 29205419,
                    29205463 29205767, 29205918, 29206109, 29206605, 29207073, 29208260,
29208732 29211457, 29211724, 29212012,
                    29212433, 29212611, 29213320, 29213351 29213613, 29213775, 29213850,
29213879, 29214561, 29214960, 29216746,
                    29216984, 29217294, 29217472, 29217828, 29217848, 29218570, 29219205
29219273, 29220079, 29221248, 29221891,
                    29222031, 29222784, 29223833 29223859, 29223967, 29224065, 29224605,
29225076, 29225168, 29225758 29227602,
                    29228869, 29229164, 29229754, 29229844, 29229955, 29230252 29230565,
29231133, 29232117, 29232154, 29232449,
                    29233415, 29234123 29236573, 29237538, 29237744, 29240307, 29241345,
29241651, 29242017 29242884, 29243958,
                    29245137, 29245160, 29246163, 29247415, 29247712 29247906, 29248495,
29248552, 29248835, 29248858, 29249991,
                    29250059 29250317, 29251259, 29253184, 29253871, 29254031, 29254930,
29255178 29255273, 29255431, 29255435,
                    29256426, 29259119, 29259320, 29260452 29261547, 29261906, 29262512,
29262887, 29265448, 29266248, 29266899,
                    29267292, 29268412, 29269171, 29269228, 29269825, 29270585, 29273539
29273570, 29273735, 29273812, 29273847,
                    29274428, 29274564, 29274627 29275461, 29276272, 29277317, 29278218,
29279658, 29279751, 29279854 29281527,
                    29281691, 29281796, 29282233, 29282898, 29285503, 29285788 29285956,
29286037, 29287130, 29287705, 29292837,
                    29293072, 29293574 29297863, 29297915, 29298220, 29299049, 29299082,
29299844, 29301463 29301566, 29302963,
                    29303918, 29304781, 29306226, 29306713, 29311528 29311588, 29312310,
29312672, 29312734, 29312753, 29313347,
                    29313417 29313525, 29314539, 29317756, 29318410, 29319441, 29321489,
29323946 29324568, 29324735, 29325087,
                    29325105, 29325257, 29325765, 29325993 29327044, 29329042, 29329087,
29329807, 29330361, 29331066, 29331209
                    29331380, 29331493, 29332292, 29332395, 29332771, 29333500, 29336843
29337310, 29337742, 29338315, 29338453,
                    29338780, 29338913, 29339101 29339155, 29341209, 29343086, 29345937,
29346057, 29346211, 29346943 29347620,
                    29348176, 29350052, 29350762, 29351386, 29351662, 29351716 29351735,
29351749, 29352298, 29352724, 29352867,
                    29352947, 29353271 29353432, 29353821, 29353960, 29355654, 29356547,
29356704, 29356711 29356752, 29358509,
                    29358828, 29360252, 29360285, 29360672, 29360911 29360950, 29361319,
29361472, 29361801, 29363151, 29364171,
                    29364177 29366940, 29367019, 29367561, 29368253, 29368310, 29372541,
29373418 29373588, 29374179, 29375941,
                    29376346, 29377986, 29378029, 29378834 29378913, 29379978, 29382784,
29382815, 29384781, 29384854, 29384864,
                    29385429, 29385652, 29386502, 29386635, 29386660, 29387073, 29387274
29388020, 29388072, 29388094, 29388524,
                    29388830, 29389889, 29390011 29390435, 29390785, 29391030, 29391237,
29391849, 29393291, 29394014 29394140,
```

```
                    29394749, 29395657, 29397954, 29397996, 29398488, 29398863 29399100,
29399121, 29399336, 29399938, 29402131,
                    29404483, 29405012 29405462, 29405651, 29405996, 29407804, 29408853,
29409149, 29409455 29410311, 29410834,
                    29411037, 29411469, 29412066, 29412269, 29417173 29417719, 29417884,
29420834, 29421059, 29423016, 29423156,
                    29423826 29424999, 29426241, 29429017, 29429264, 29429466, 29429566,
29430524 29430866, 29431192, 29431485,
                    29434301, 29435474, 29435652, 29436454 29436514, 29436727, 29437594,
29437712, 29438277, 29438736, 29439522,
                    29441196, 29443187, 29443250, 29444072, 29444282, 29444602, 29446669
29449477, 29449845, 29450193, 29450421,
                    29450812, 29450936, 29451386 29452576, 29452936, 29452953, 29454978,
29455424, 29457312, 29457370 29457807,
                    29460252, 29461420, 29461791, 29462594, 29462767, 29462957 29463047,
29463528, 29464616, 29464779, 29465177,
                    29467622, 29469565 29470291, 29471860, 29476473, 29481584, 29483532,
29483672, 29483685 29483712, 29483723,
                    29485099, 29486181, 29488894, 29489546, 29490256 29492127, 29492939,
29493122, 29494245, 29495057, 29495684,
                    29497311 29497696, 29498198, 29500257, 29500826, 29502561, 29503543,
29503631 29503827, 29504492, 29504682,
                    29505668, 29507270, 29507616, 29510278 29511611, 29514479, 29515134,
29515240, 29515476, 29515766, 29515834,
                    29516300, 29516766, 29517168, 29517883, 29521187, 29521748, 29521862
29522358, 29522561, 29522662, 29523511,
                    29524599, 29525467, 29525886 29527595, 29527610, 29529147, 29530440,
29530515, 29530812, 29531654 29532532,
                    29541742, 29541769, 29542449, 29542643, 29543034, 29543956 29546817,
29547867, 29548427, 29548687, 29548722,
                    29549071, 29549104 29549154, 29549730, 29552773, 29553141, 29557144,
29557261, 29557336 29558238, 29558975,
                    29559187, 29559446, 29559908, 29559981, 29565611 29580394, 29580983,
29581771, 29584261, 29584693, 29586143,
                    29587765 29597536, 29597754, 29598039, 29598046, 29598233, 29599008,
29599300 29601461, 29603460, 29604002,
                    29604257, 29607136, 29608000, 29611020 29611991, 29616244, 29616414,
29618074, 29618190, 29620042, 29622936,
                    29625065, 29625804, 29625876, 29626154, 29626732, 29628200, 29629430
29629650, 29629681, 29631749, 29632095,
                    29632265, 29633697, 29633753 29633936, 29634643, 29635427, 29635717,
29635990, 29637362, 29637526 29638285,
                    29641736, 29645349, 29651183, 29651520, 29653132, 29653246 29655668,
29656819, 29657422, 29657960, 29661028,
                    29661065, 29661722 29663368, 29664087, 29664161, 29667994, 29668005,
29669413, 29670782 29671363, 29672507,
                    29676089, 29677051, 29677733, 29677927, 29679856 29683039, 29687214,
29687459, 29687718, 29687763, 29689145,
                    29692694 29695425, 29695841, 29696310, 29700125, 29700460, 29703932,
29707099 29707896, 29708915, 29715220,
                    29720133, 29721418, 29725781, 29741976 29742223, 29747493, 29747648,
29749471, 29750673, 29751094, 29753244,
                    29754951, 29755821, 29756274, 29756444, 29757264, 29757651, 29758661
29761911, 29766207, 29766503, 29766679,
                    29771032, 29773842, 29775393 29779196, 29782211, 29782823, 29782866,
29785239, 29787766, 29791880 29795712,
                    29795957, 29802695, 29809837, 29815713, 29836096, 29838773 29845530,
29848849, 29850930, 29851733, 29858376,
                    29869086, 29869404 29869887, 29875459, 29875565, 29881478, 29881839,
29887111, 29888621 29893132, 29900203,
                    29902327, 29903299, 29903454, 29921318, 29926466 29943670, 29997326,
30006159, 30015070, 30019864, 30024618,
                    30033547 30034456, 30053036, 30075037, 30076197, 30092859, 30095591,
30114534 30142907, 30155837, 30174401
```

Version 19.0.0.0.ru-2019-07.rur-2019-07.r1

La version 19.0.0.0.ru-2019-07.rur-2019-07.r1 comprend ce qui suit :

- Correctif 29834717 : Mise à jour de version de base de données : 19.4.0.0.190716
- Correctif 29774421 : MISE À JOUR VERSION OJVM : 19.4.0.0.190716
- Correctif 28852325 : RDBMS - MISE À JOUR DSTV33 - TZDATA2018G
- Correctif 28852334 : MISE À JOUR DSTV33 - TZDATA2018G - CORRECTIF OJVM REQUIS
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS
- Correctif 29213893 : DBMS_ÉCHEC DES STATS AVEC ERREUR ORA-01422 LORS DU REGROUPEMENT DES STATS POUR LA TABLE UTILIATEUR$
- PreUpgrade Jar : preupgrade_19_cbuild_4_lf.zip

Mise à jour de version Oracle 19.4.0.0.190716, publiée en juillet 2019

Bogues corrigés :

```
29850930, 29225758, 29276272, 14735102, 17428816, 19080742, 19697993
20313356, 21374587, 21965541, 23296836, 23606241, 25756945, 25806201
25883179, 25986062, 25997810, 26476244, 26611353, 26739322, 26872233
27126938, 27244999, 27359766, 27369515, 27423500, 27453490, 27666312
27710072, 27846298, 27957203, 28064977, 28072567, 28125947, 28129791
28181021, 28210681, 28271693, 28279456, 28313275, 28326928, 28350595
28371123, 28379065, 28381939, 28390273, 28431445, 28463226, 28475242
28489419, 28502773, 28513333, 28534475, 28547068, 28561704, 28569897
28572533, 28572544, 28572667, 28572834, 28587723, 28593682, 28594086
28597221, 28601957, 28605066, 28606598, 28612239, 28625862, 28627033
28636532, 28643718, 28644549, 28645570, 28646200, 28646939, 28649388
28655209, 28663782, 28673945, 28692275, 28694872, 28696373, 28705231
28710385, 28710734, 28714461, 28715727, 28718469, 28719348, 28720418
28722229, 28730079, 28740708, 28742555, 28749853, 28755011, 28758722
28760206, 28767240, 28772390, 28774416, 28777214, 28781754, 28785531
28789531, 28791852, 28795551, 28802734, 28804517, 28810381, 28811560
28815123, 28815355, 28819640, 28824482, 28827682, 28833912, 28835937
28849776, 28854004, 28862532, 28863432, 28867992, 28873575, 28876253
28876639, 28884931, 28888327, 28889730, 28892794, 28897512, 28899663
28901126, 28905457, 28907196, 28912691, 28915561, 28917080, 28918429
28919145, 28922227, 28922532, 28922608, 28925634, 28925880, 28933158
28936114, 28937717, 28938698, 28940179, 28940281, 28941901, 28942455
28945421, 28945994, 28950868, 28951533, 28952168, 28954762, 28955606
28956908, 28957292, 28957723, 28962775, 28965231, 28966444, 28974083
28977322, 28983095, 28983486, 28986207, 28986231, 28986326, 28986481
28988482, 28989306, 28993295, 28993353, 28994307, 28996376, 29000000
29001305, 29001888, 29002784, 29002927, 29003738, 29006318, 29006621
29007321, 29007775, 29008035, 29008669, 29009513, 29011936, 29012609
29013475, 29014076, 29015118, 29017265, 29018655, 29019121, 29021063
29021352, 29024054, 29024552, 29024732, 29026582, 29026606, 29027456
29027694, 29027940, 29031575, 29031600, 29032234, 29032276, 29032457
29032607, 29033052, 29033145, 29033200, 29033280, 29034587, 29037290
29038528, 29039089, 29039510, 29040739, 29043554, 29043651, 29043725
29044763, 29044954, 29047850, 29048178, 29048289, 29048498, 29048605
29050357, 29050560, 29050765, 29051702, 29051953, 29052726, 29053783
29056024, 29056270, 29056560, 29056767, 29059011, 29061959, 29062692
29062848, 29062860, 29062868, 29110526, 29110783, 29110790, 29110797
29110802, 29110805, 29111598, 29113282, 29113305, 29117526, 29117642
29119077, 29120223, 29122224, 29122254, 29123297, 29123432, 29123482
29124368, 29125036, 29125374, 29125380, 29126345, 29127957, 29128693
```

```
29128935, 29129450, 29129497, 29129712, 29130219, 29131539, 29132938
29134447, 29135383, 29135649, 29136111, 29138641, 29141316, 29141341
29141685, 29142609, 29142667, 29144995, 29145214, 29145730, 29149829
29150338, 29151520, 29152357, 29155099, 29157389, 29158680, 29158899
29159909, 29159936, 29160174, 29162095, 29163156, 29163415, 29163437
29163524, 29163567, 29167111, 29167342, 29167374, 29167940, 29168219
29168433, 29169073, 29169215, 29171683, 29171942, 29172618, 29172826
29173140, 29173373, 29173817, 29174004, 29176318, 29177466, 29177543
29177886, 29178385, 29180313, 29180455, 29180559, 29180893, 29181153
29181231, 29181620, 29181743, 29181923, 29182019, 29183912, 29184297
29184666, 29185193, 29186456, 29189302, 29189307, 29189889, 29190235
29190474, 29190740, 29191541, 29192419, 29192468, 29192685, 29193207
29194205, 29194367, 29194493, 29194827, 29194981, 29195279, 29195337
29195758, 29196725, 29199635, 29199733, 29200316, 29200700, 29201494
29201539, 29202104, 29202850, 29203122, 29203166, 29203425, 29203443
29203604, 29205281, 29205323, 29205419, 29205463, 29205767, 29205918
29206109, 29206605, 29207073, 29208260, 29208732, 29211457, 29211724
29212012, 29212433, 29212611, 29213351, 29213775, 29213850, 29213879
29214561, 29214960, 29216746, 29216984, 29217294, 29217472, 29217828
29217848, 29218570, 29219205, 29219273, 29220079, 29221248, 29221891
29222031, 29222784, 29223833, 29223859, 29223967, 29224065, 29224605
29225076, 29225168, 29227602, 29228869, 29229164, 29229754, 29229844
29229955, 29230252, 29230565, 29231133, 29232117, 29232154, 29233415
29234123, 29237538, 29240307, 29241345, 29241651, 29242017, 29242884
29243958, 29245137, 29245160, 29246163, 29247415, 29247712, 29247906
29248495, 29248552, 29248835, 29248858, 29249991, 29250059, 29250317
29251259, 29253184, 29253871, 29254031, 29254930, 29255178, 29255273
29255431, 29255435, 29256426, 29259119, 29259320, 29260452, 29261547
29261906, 29262512, 29262887, 29265448, 29266248, 29266899, 29267292
29268412, 29269171, 29269228, 29270585, 29273539, 29273570, 29273735
29273812, 29273847, 29274428, 29274564, 29274627, 29275461, 29277317
29278218, 29279658, 29279751, 29279854, 29281527, 29281691, 29281796
29282233, 29282898, 29285503, 29285788, 29285956, 29286037, 29287130
29287705, 29292837, 29293072, 29293574, 29297863, 29297915, 29298220
29299049, 29299082, 29299844, 29301463, 29301566, 29302963, 29303918
29304781, 29306226, 29306713, 29311588, 29312310, 29312672, 29312734
29312753, 29313347, 29313417, 29313525, 29314539, 29317756, 29318410
29319441, 29321489, 29323946, 29324568, 29324735, 29325087, 29325105
29325257, 29325765, 29325993, 29327044, 29329042, 29329087, 29329807
29330361, 29331066, 29331209, 29331380, 29331493, 29332292, 29332395
29332771, 29333500, 29336843, 29337310, 29338315, 29338453, 29338780
29338913, 29339101, 29339155, 29341209, 29343086, 29345937, 29346057
29346211, 29346943, 29347620, 29348176, 29350052, 29351386, 29351716
29351735, 29351749, 29352298, 29352724, 29352867, 29352947, 29353271
29353432, 29353960, 29355654, 29356547, 29356704, 29356711, 29356752
29358509, 29358828, 29360285, 29360672, 29360911, 29360950, 29361472
29361801, 29363151, 29364171, 29364177, 29366940, 29367019, 29367561
29368253, 29372541, 29373418, 29373588, 29374179, 29375941, 29376346
29377986, 29378029, 29378834, 29378913, 29379978, 29382784, 29382815
29384781, 29384854, 29384864, 29385429, 29385652, 29386502, 29386635
29386660, 29387073, 29387274, 29388020, 29388072, 29388094, 29388524
29388830, 29389889, 29390011, 29390435, 29390785, 29391030, 29394014
29394140, 29394749, 29395657, 29397954, 29397996, 29398488, 29398863
29399100, 29399121, 29399938, 29402131, 29404483, 29405012, 29405462
29405651, 29405996, 29407804, 29409149, 29410311, 29410834, 29411037
29412066, 29412269, 29417719, 29417884, 29420834, 29421059, 29423826
29424999, 29426241, 29429017, 29429264, 29429566, 29430524, 29431192
29431485, 29434301, 29435474, 29435652, 29436454, 29436514, 29437594
29437712, 29438277, 29438736, 29439522, 29441196, 29443187, 29443250
29444072, 29444282, 29444602, 29446669, 29449477, 29450421, 29451386
29452576, 29452936, 29452953, 29455424, 29457312, 29457370, 29457807
29460252, 29461791, 29462594, 29462767, 29462957, 29464779, 29465177
29467622, 29476473, 29483532, 29483672, 29483685, 29483712, 29486181
29488894, 29489546, 29490256, 29492127, 29492939, 29494245, 29495057
29495684, 29497311, 29500826, 29502561, 29503543, 29503631, 29503827
29504492, 29504682, 29505668, 29507616, 29510278, 29511611, 29514479
```

```
29515134, 29515240, 29515766, 29515834, 29516300, 29517168, 29521187
29521748, 29522358, 29522561, 29522662, 29523511, 29525467, 29525886
29527595, 29529147, 29530440, 29530515, 29530812, 29531654, 29541769
29542449, 29543034, 29546817, 29547867, 29548687, 29548722, 29549154
29549730, 29557336, 29558975, 29559187, 29559446, 29559908, 29559981
29565611, 29580983, 29581771, 29584261, 29586143, 29597536, 29597754
29598039, 29598233, 29599300, 29601461, 29604002, 29608000, 29611020
29611991, 29616244, 29616414, 29618074, 29618190, 29622936, 29626732
29628200, 29629650, 29629681, 29631749, 29632095, 29633697, 29635427
29635717, 29637362, 29638285, 29641736, 29653246, 29656819, 29657422
29664087, 29664161, 29670782, 29676089, 29677051, 29677733, 29679856
29687459, 29687763, 29692694, 29695841, 29703932, 29707099, 29742223
29747648, 29751094, 29753244, 29754951, 29756274, 29757651, 29766207
29766503, 29766679, 29775393, 29779196, 29795957, 29838773
```

Moteur de base de données : 18.0.0.0

Les versions suivantes sont disponibles pour le moteur de base de données Oracle 18.0.0.0 :

- Version 18.0.0.0.ru-2020-07.rur-2020-07.r1 (p. 1231)
- Version 18.0.0.0.ru-2020-04.rur-2020-04.r1 (p. 1235)
- Version 18.0.0.0.ru-2020-01.rur-2020-01.r1 (p. 1239)
- Version 18.0.0.0.ru-2019-10.rur-2019-10.r1 (p. 1243)
- Version 18.0.0.0.ru-2019-07.rur-2019-07.r1 (p. 1246)

Version 18.0.0.0.ru-2020-07.rur-2020-07.r1

La version 18.0.0.0.ru-2020-07.rur-2020-07.r1 comprend ce qui suit :

- Correctif 31308624 : mise à jour 18.11.0.0.200714 de la version de base de données
- Correctif 31219909 : MISE À JOUR VERSION OJVM 18.11.0.0.200714
- Correctif 31335037 : DSTV35 pour RDBMS (TZDATA2020A)
- Correctif 31335142 : DSTV35 pour OJVM (TZDATA2020A)
- Correctif 29213893 : DBMS_ÉCHEC DES STATS AVEC ERREUR ORA-01422 LORS DU REGROUPEMENT DES STATS POUR LA TABLE UTILIATEUR$
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS
- Correctif 29374604 : IE ne démarre pas sur Oracle RDBMS Standard Edition 18c
- PreUpgrade Jar : preupgrade_181_cbuild_10_lf.zip

Correctifs combinés pour la version 18.0.0.0.ru-2020-07.rur-2020-07.r1, publiés en juillet 2020

Bogues corrigés :

```
7391838, 8932139, 9062315, 12816839, 13554903, 14221306, 18701017
18986501, 20436508, 20549013, 20917487, 21095391, 21223848, 21374587
21547051, 21744603, 21766220, 21806121, 21935698, 22174392, 22282748
22363790, 22645496, 22729345, 22734786, 23003564, 23061453, 23109325
23310101, 23698980, 23761724, 23840305, 24489904, 24596874, 24669730
```

```
24687075, 24689376, 24737581, 24798481, 24841671, 24844841, 24903291
24925863, 24971597, 25031502, 25035594, 25035599, 25060506, 25092651
25210690, 25287072, 25293659, 25303284, 25309116, 25348956, 25405687
25416731, 25487146, 25560538, 25573623, 25576115, 25591292, 25607397
25634405, 25644811, 25663488, 25686739, 25696520, 25709124, 25724089
25726981, 25736428, 25740844, 25743479, 25756945, 25809524, 25824236
25882883, 25890002, 25908728, 25911069, 25929650, 25943740, 25958554
25986062, 25997810, 26083489, 26115103, 26164661, 26226953, 26237338
26281476, 26284722, 26297826, 26299684, 26313403, 26336101, 26362155
26375330, 26399691, 26405036, 26410240, 26422277, 26423085, 26427905
26433972, 26440142, 26440169, 26441345, 26450454, 26476244, 26521043
26527054, 26536320, 26586174, 26587652, 26595088, 26598422, 26615291
26617804, 26646549, 26647619, 26654411, 26694735, 26724511, 26731697
26745002, 26785169, 26790514, 26790923, 26792891, 26798411, 26818960
26822620, 26827699, 26843558, 26843664, 26846077, 26860285, 26871815
26882126, 26882316, 26883456, 26894737, 26895149, 26898279, 26910716
26914402, 26927998, 26928317, 26933599, 26943004, 26943660, 26956033
26960097, 26961415, 26966120, 26966916, 26970175, 26976568, 26985002
26986173, 26992964, 26996813, 27000158, 27005278, 27006120, 27006664
27012915, 27013566, 27016033, 27018734, 27026401, 27028251, 27030974
27032726, 27033520, 27034318, 27034688, 27035653, 27036163, 27036408
27037839, 27038986, 27040560, 27041253, 27044169, 27044575, 27047831
27053044, 27054231, 27058530, 27060167, 27060859, 27061736, 27066451
27066519, 27072923, 27073066, 27075854, 27080748, 27080874, 27086406
27086821, 27090765, 27092991, 27093423, 27098733, 27100800, 27101105
27101527, 27101652, 27105900, 27106301, 27106915, 27110878, 27111780
27112686, 27114112, 27115422, 27119621, 27119861, 27121566, 27122162
27125872, 27126666, 27128580, 27133637, 27135647, 27142120, 27142529
27143756, 27143882, 27144533, 27144928, 27147979, 27150500, 27151826
27152892, 27153641, 27153755, 27155549, 27156355, 27160360, 27160922
27163928, 27164352, 27165231, 27166354, 27166715, 27169796, 27169888
27170305, 27174938, 27174948, 27177551, 27177852, 27179264, 27181521
27181537, 27181897, 27182006, 27182064, 27184253, 27185188, 27187440
27189611, 27190851, 27193810, 27195935, 27197334, 27199245, 27200959
27202015, 27203055, 27204476, 27207634, 27208795, 27208953, 27210038
27210263, 27210872, 27212837, 27213140, 27214085, 27214204, 27215007
27216046, 27216224, 27217412, 27220610, 27220937, 27221900, 27222121
27222423, 27222626, 27222938, 27223075, 27224987, 27226913, 27228786
27229389, 27231051, 27232983, 27233563, 27234962, 27236052, 27236110
27236722, 27238077, 27238258, 27240246, 27240570, 27241221, 27241247
27242226, 27242616, 27244337, 27244785, 27244999, 27249215, 27249531
27249544, 27250547, 27251690, 27252023, 27254335, 27254851, 27255377
27256000, 27256488, 27256534, 27256584, 27257509, 27258578, 27259307
27259386, 27259983, 27262601, 27262650, 27262798, 27262945, 27262991
27263276, 27263677, 27263996, 27264464, 27265816, 27266245, 27267992
27270197, 27271876, 27274143, 27274456, 27274536, 27275136, 27275533
27275776, 27276231, 27282707, 27283029, 27283960, 27284375, 27284499
27285244, 27285557, 27288230, 27288638, 27288894, 27292213, 27293599
27294480, 27299455, 27300007, 27301308, 27301568, 27302415, 27302594
27302632, 27302681, 27302695, 27302711, 27302714, 27302730, 27302777
27302800, 27302960, 27303287, 27303785, 27303938, 27304131, 27304410
27304906, 27304936, 27305318, 27307868, 27308088, 27309182, 27310092
27313687, 27314206, 27314390, 27314512, 27314697, 27315159, 27318117
27318869, 27320576, 27320985, 27321179, 27321834, 27326204, 27329812
27330158, 27330161, 27333658, 27333664, 27333693, 27333731, 27334316
27334353, 27334648, 27335682, 27338838, 27338912, 27338946, 27339115
27339396, 27339483, 27339495, 27341036, 27343844, 27345190, 27345231
27345450, 27345498, 27346329, 27346644, 27346709, 27346949, 27346984
27347126, 27348081, 27348707, 27349393, 27350267, 27351628, 27352600
27354783, 27356373, 27357773, 27358232, 27358241, 27359178, 27359368
27360126, 27362190, 27364854, 27364891, 27364916, 27364947, 27365014
27365139, 27365702, 27365993, 27367194, 27368850, 27369515, 27370933
27372756, 27375260, 27375542, 27376871, 27377219, 27378103, 27378959
27379233, 27379846, 27379956, 27381383, 27381417, 27381498, 27381656
27383281, 27384222, 27386467, 27389352, 27392187, 27392968, 27393421
27393570, 27394086, 27395404, 27395416, 27395794, 27396357, 27396365
```

```
27396377, 27396624, 27396666, 27396672, 27396720, 27396794, 27396813
27397048, 27398080, 27398223, 27398660, 27399499, 27399762, 27399985
27400416, 27400598, 27401618, 27401637, 27403244, 27404573, 27404599
27404668, 27405242, 27405645, 27405696, 27406105, 27410279, 27410300
27410595, 27412805, 27416327, 27416997, 27417186, 27420715, 27421101
27421733, 27422874, 27423251, 27424405, 27425507, 27425622, 27426277
27426363, 27427805, 27428790, 27430219, 27430254, 27430802, 27432062
27432338, 27432355, 27432826, 27433163, 27433385, 27433870, 27434050
27434193, 27434486, 27434974, 27435537, 27439835, 27441326, 27441980
27442041, 27444727, 27445330, 27445462, 27445727, 27447452, 27447687
27448162, 27449814, 27450355, 27450400, 27450783, 27451049, 27451182
27451187, 27451531, 27452046, 27452760, 27452897, 27453225, 27454722
27457666, 27457891, 27458164, 27458829, 27459593, 27459909, 27459948
27460675, 27461740, 27462994, 27465480, 27466597, 27467543, 27468303
27469245, 27469329, 27471876, 27472969, 27473800, 27475272, 27479358
27480784, 27481406, 27481765, 27483974, 27484556, 27486253, 27486805
27487309, 27487795, 27487919, 27489107, 27489719, 27492916, 27493674
27494663, 27496224, 27496308, 27496424, 27496806, 27497950, 27498477
27501327, 27501413, 27501465, 27502420, 27503318, 27503413, 27504190
27504770, 27505229, 27505603, 27506774, 27507968, 27508936, 27508984
27508985, 27510959, 27511196, 27512439, 27513114, 27517818, 27518227
27518310, 27519708, 27520070, 27520900, 27522245, 27523368, 27523800
27525909, 27526362, 27526744, 27528204, 27529661, 27532009, 27532375
27533780, 27533819, 27534289, 27534509, 27537472, 27539757, 27539876
27540613, 27541286, 27541468, 27542824, 27544030, 27544973, 27545630
27547732, 27550341, 27551855, 27554074, 27555481, 27558557, 27558559
27558861, 27560562, 27560602, 27560702, 27560735, 27562488, 27563629
27563767, 27565906, 27567477, 27570318, 27573154, 27573408, 27574335
27576342, 27576354, 27577122, 27577758, 27578007, 27579353, 27579969
27580996, 27581484, 27585755, 27585800, 27586810, 27586895, 27587672
27587905, 27588271, 27589260, 27591842, 27592466, 27593389, 27593501
27593585, 27593587, 27595096, 27595801, 27595973, 27599689, 27599927
27600706, 27601118, 27601441, 27602091, 27602488, 27603841, 27604293
27605482, 27607563, 27607805, 27608669, 27609819, 27610269, 27613080
27613247, 27613530, 27613554, 27615608, 27615649, 27616657, 27617522
27617978, 27620808, 27623159, 27623844, 27625010, 27625050, 27625274
27625620, 27627992, 27629756, 27629928, 27631506, 27632114, 27634676
27634991, 27635508, 27636900, 27642235, 27644757, 27645231, 27645940
27649707, 27652302, 27654039, 27654521, 27655217, 27657467, 27657712
27657920, 27658186, 27658205, 27662528, 27663370, 27664702, 27666312
27668379, 27671633, 27679488, 27679664, 27679793, 27679806, 27679961
27680162, 27680509, 27680669, 27682151, 27682288, 27686599, 27688036
27688099, 27688692, 27690513, 27690578, 27691717, 27691809, 27691920
27691939, 27692215, 27693416, 27693713, 27694261, 27695063, 27697092
27698953, 27700466, 27701795, 27702244, 27703242, 27704237, 27705761
27707544, 27708711, 27709046, 27710072, 27714373, 27718914, 27719187
27723002, 27723151, 27725967, 27726269, 27726780, 27729678, 27731346
27732323, 27733415, 27734470, 27735534, 27739006, 27739957, 27740424
27740844, 27740854, 27744211, 27745220, 27747407, 27747869, 27748321
27748954, 27751006, 27751755, 27753336, 27756900, 27757567, 27757794
27757888, 27757979, 27758544, 27758653, 27758972, 27759077, 27759457
27761402, 27766324, 27766679, 27767081, 27768034, 27769361, 27772093
27772815, 27773602, 27774320, 27774539, 27778433, 27779886, 27780562
27780683, 27782339, 27782464, 27783059, 27783289, 27786669, 27786699
27786772, 27791223, 27793533, 27797290, 27801337, 27801774, 27803665
27807441, 27810967, 27811439, 27812560, 27812593, 27813267, 27815347
27818389, 27818871, 27819881, 27824540, 27824543, 27825241, 27828794
27828892, 27829295, 27832643, 27833369, 27833672, 27834551, 27834569
27834984, 27835925, 27839353, 27839616, 27839732, 27840386, 27843646
27846298, 27846499, 27847259, 27849825, 27850112, 27850736, 27851757
27856471, 27861226, 27861452, 27861909, 27862636, 27864737, 27865439
27869075, 27869339, 27873412, 27873643, 27876671, 27882176, 27886087
27889841, 27892488, 27896388, 27896443, 27896458, 27897639, 27897759
27898015, 27900663, 27902561, 27906509, 27908396, 27908644, 27909478
27912301, 27917669, 27918832, 27920184, 27924147, 27926113, 27927431
27929287, 27929509, 27930478, 27931299, 27931506, 27934468, 27935348
```

```
27935464, 27935493, 27935826, 27936676, 27938736, 27940876, 27941110
27941514, 27941896, 27945870, 27948050, 27948153, 27950708, 27952586
27952762, 27957892, 27959594, 27960021, 27961746, 27964051, 27964513
27965400, 27965830, 27966472, 27967484, 27970265, 27971503, 27971575
27972265, 27975778, 27977039, 27978668, 27983174, 27984028, 27984314
27986817, 27989556, 27989849, 27991970, 27993289, 27993298, 27994325
27994333, 27995215, 27995248, 27997875, 27998003, 27999073, 27999597
27999638, 28000269, 28004853, 28006704, 28018962, 28019283, 28019592
28021205, 28022101, 28022847, 28023081, 28023399, 28023410, 28023482
28024347, 28024793, 28025398, 28025414, 28026866, 28032758, 28033429
28036487, 28039471, 28039953, 28043157, 28045209, 28045903, 28057267
28058612, 28059199, 28067846, 28071549, 28072130, 28072383, 28072464
28072567, 28073470, 28074713, 28079127, 28085865, 28088762, 28089440
28090453, 28091981, 28092783, 28098040, 28098160, 28098865, 28099592
28103600, 28103869, 28104176, 28104361, 28104409, 28106402, 28108003
28108898, 28109326, 28109698, 28111583, 28120036, 28120951, 28124631
28125601, 28125947, 28129791, 28131767, 28132287, 28135648, 28157786
28164480, 28165439, 28165545, 28169711, 28174827, 28174926, 28174951
28175445, 28180464, 28181021, 28182503, 28184554, 28184800, 28187706
28188330, 28189466, 28194173, 28199085, 28201419, 28204262, 28204423
28204443, 28209341, 28209985, 28210192, 28211734, 28214943, 28215510
28218832, 28220398, 28223871, 28226179, 28227512, 28229360, 28236305
28238264, 28240153, 28242712, 28250929, 28256164, 28258608, 28264172
28271107, 28271119, 28271693, 28276054, 28278547, 28278640, 28279837
28281094, 28282606, 28285766, 28290434, 28294563, 28302049, 28304709
28305001, 28305362, 28305607, 28309182, 28309406, 28312508, 28315031
28315995, 28319114, 28319623, 28320117, 28320399, 28321446, 28323201
28328895, 28329450, 28330714, 28330971, 28333072, 28338399, 28338999
28344964, 28350595, 28354603, 28357401, 28361083, 28361221, 28361787
28365111, 28369092, 28371123, 28373960, 28375383, 28378446, 28379065
28384353, 28385102, 28386259, 28388910, 28390273, 28391210, 28391582
28392168, 28392251, 28393678, 28396445, 28397317, 28401116, 28402823
28403295, 28413955, 28420042, 28420457, 28423598, 28432129, 28434028
28435825, 28437849, 28439086, 28445741, 28448314, 28454215, 28455212
28468312, 28468493, 28475164, 28478676, 28481149, 28481679, 28483184
28489150, 28492362, 28493478, 28498976, 28501075, 28502098, 28502403
28502773, 28503038, 28503484, 28504545, 28507324, 28508053, 28508296
28508557, 28512336, 28512761, 28513333, 28514693, 28521330, 28527416
28528349, 28530171, 28535127, 28535272, 28538439, 28542455, 28544633
28545134, 28545687, 28546290, 28547068, 28547478, 28553468, 28558645
28564479, 28565296, 28571483, 28572407, 28572834, 28578164, 28578945
28580528, 28584193, 28584217, 28584444, 28585411, 28587723, 28589509
28600233, 28601874, 28606598, 28608211, 28611037, 28612674, 28614072
28617631, 28617959, 28621470, 28622202, 28627255, 28627686, 28632559
28636676, 28639299, 28642273, 28642899, 28644549, 28646200, 28670445
28673203, 28678804, 28679454, 28680029, 28685371, 28689483, 28692103
28692275, 28695694, 28697806, 28702188, 28703812, 28708023, 28709063
28710469, 28710827, 28713840, 28714058, 28714988, 28715655, 28728040
28728272, 28730076, 28730253, 28734355, 28740708, 28742555, 28745367
28747182, 28749289, 28752599, 28755011, 28757758, 28758090, 28758722
28761812, 28767240, 28770146, 28774416, 28776431, 28776811, 28777174
28777214, 28777332, 28781754, 28785022, 28785531, 28791725, 28793062
28797711, 28803345, 28805612, 28805695, 28808314, 28809909, 28817449
28819640, 28820669, 28821847, 28827682, 28830691, 28831971, 28835937
28836716, 28838066, 28844866, 28847136, 28849751, 28852325, 28852691
28855922, 28856060, 28856172, 28863263, 28863487, 28865569, 28867992
28876639, 28878525, 28881723, 28887305, 28887509, 28889730, 28891984
28900506, 28905390, 28905457, 28910498, 28915870, 28919145, 28925880
28927452, 28938924, 28940179, 28949888, 28950868, 28951014, 28951382
28956908, 28959493, 28960211, 28965084, 28965095, 28986231, 28986257
28987454, 28993295, 28993353, 28993590, 28994890, 29000190, 29002488
29006527, 29007321, 29007353, 29009513, 29013832, 29015118, 29015706
29024054, 29026582, 29027694, 29027940, 29032276, 29033896, 29036278
29037290, 29039510, 29040739, 29044954, 29048498, 29048728, 29050886
29051702, 29055644, 29056270, 29056767, 29060216, 29061016, 29115857
29123482, 29125374, 29136111, 29139070, 29139591, 29158680, 29163567
```

```
29165682, 29170232, 29171683, 29173817, 29177886, 29179097, 29182517
29182901, 29189889, 29190663, 29198092, 29200700, 29202461, 29203604
29205918, 29212433, 29213320, 29213351, 29213893, 29224605, 29225076
29230252, 29230565, 29233415, 29237575, 29241345, 29242017, 29247712
29247906, 29249289, 29250317, 29254623, 29255273, 29260956, 29261548
29278684, 29285503, 29296257, 29301463, 29307638, 29311927, 29312672
29312889, 29314539, 29331209, 29331493, 29332763, 29339155, 29343086
29343156, 29343861, 29344541, 29346057, 29347981, 29350868, 29351662
29351771, 29353821, 29356752, 29361472, 29362596, 29364171, 29366406
29372069, 29372460, 29374604, 29375355, 29375984, 29376346, 29378913
29379978, 29382784, 29383695, 29386635, 29388020, 29388952, 29391849
29394749, 29395657, 29398488, 29399046, 29399336, 29404483, 29405462
29407804, 29408853, 29409149, 29409455, 29412269, 29417719, 29418165
29420254, 29426241, 29428230, 29429264, 29430524, 29434301, 29436454
29437712, 29439522, 29442936, 29445548, 29448498, 29450812, 29452251
29454978, 29457978, 29464779, 29465177, 29483626, 29483672, 29483723
29483771, 29489436, 29493122, 29500257, 29500963, 29501218, 29504682
29506942, 29511611, 29515766, 29521862, 29524599, 29524985, 29525886
29530515, 29531541, 29536342, 29538631, 29541742, 29542449, 29542580
29548413, 29548592, 29549071, 29557261, 29558238, 29559395, 29564592
29579919, 29580394, 29591343, 29604257, 29607136, 29608023, 29614098
29614987, 29616244, 29625065, 29626154, 29629430, 29629745, 29632265
29633753, 29637526, 29637560, 29643721, 29645167, 29645349, 29651520
29656843, 29667994, 29668005, 29676089, 29685137, 29687220, 29687459
29688867, 29703195, 29705793, 29707896, 29717901, 29719146, 29720133
29722167, 29724041, 29726695, 29739576, 29766435, 29773197, 29774362
29780140, 29782211, 29789911, 29791152, 29794462, 29807964, 29809792
29813494, 29815341, 29817278, 29822714, 29825525, 29827852, 29841687
29846645, 29853485, 29865188, 29869404, 29869906, 29875459, 29876358
29881050, 29881575, 29884958, 29891916, 29893132, 29896510, 29902299
29914449, 29922225, 29930457, 29944035, 29944660, 29951620, 29951759
29961353, 29962927, 29962939, 29965888, 29991257, 29997326, 29997937
30008125, 30018017, 30018903, 30031027, 30034456, 30039959, 30064268
30068871, 30073744, 30074349, 30076253, 30078934, 30085980, 30088912
30092280, 30098251, 30099302, 30114477, 30116203, 30120608, 30125944
30128047, 30131286, 30139392, 30147928, 30149035, 30160625, 30163243
30164714, 30173113, 30177597, 30179644, 30186706, 30189023, 30193165
30193736, 30194710, 30196358, 30200680, 30200758, 30215130, 30218044
30218317, 30223712, 30225443, 30232638, 30239480, 30240547, 30241567
30246179, 30247305, 30252098, 30252156, 30253255, 30259008, 30265523
30272329, 30282501, 30283932, 30293345, 30305880, 30312094, 30312559
30316897, 30325407, 30342878, 30352623, 30355490, 30357897, 30364613
30365745, 30368482, 30368668, 30372081, 30374739, 30376986, 30381207
30384121, 30384152, 30391272, 30397100, 30402386, 30403763, 30408515
30409339, 30412188, 30413137, 30416034, 30431274, 30441687, 30443393
30450787, 30453442, 30458593, 30460922, 30464655, 30474774, 30475115
30476768, 30485255, 30496957, 30497057, 30501574, 30503943, 30509277
30510527, 30522998, 30528547, 30528704, 30533172, 30534662, 30544595
30581448, 30582500, 30599407, 30602230, 30613937, 30623138, 30624864
30635302, 30652853, 30654454, 30668407, 30671813, 30681462, 30691604
30698289, 30741263, 30758943, 30773164, 30783551, 30803210, 30814285
30815852, 30816938, 30829779, 30855101, 30881588, 30887501, 30904672
30922819, 30957739, 30964194, 30968737, 30987088, 30998759, 31001455
31004719, 31013127, 31019767, 31022858, 31029936, 31100172, 31106577
31156383, 31172207, 31182793, 31200845, 31306261, 31335037, 31335142
31393600
```

Version 18.0.0.0.ru-2020-04.rur-2020-04.r1

La version 18.0.0.0.ru-2020-04.rur-2020-04.r1 comprend ce qui suit :

- Correctif 30872794 : Mise à jour 18.10.0.0.200414 de la version de base de données
- Correctif 30805598 : Mise à jour 18.10.0.0.200414 de la version d’Oracle JVM

- Correctif 29997937 : DSTv34 pour RDBMS (TZDATA2019B)
- Correctif 29997959 : DSTv34 pour OJVM (TZDATA2019G)
- PreUpgrade Jar : preupgrade_181_cbuild_9_lf.zip
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS incluse dans CORRECTIF BASE DE DONNÉES 30138470
- Correctif 29213893 : DBMS_ÉCHEC DES STATS AVEC ERREUR ORA-01422 LORS DU REGROUPEMENT DES STATS POUR LA TABLE UTILIATEUR$
- Prise en charge de Purge de la corbeille (p. 1129)
- Prise en charge de Génération de rapports de performance avec AWR (Automatic Workload Repository) (p. 1119) utilisant le package `rdsadmin.rdsadmin_diagnostic_util`.

Correctifs combinés pour la version 18.0.0.0.ru-2020-04.rur-2020-04.r1, publiés en avril 2020

Bogues corrigés :

```
8932139, 9062315, 13554903, 14221306, 20436508, 20549013, 21095391
21223848, 21374587, 21547051, 21744603, 21766220, 21806121, 21935698
22174392, 22282748, 22363790, 22645496, 23003564, 23061453, 23109325
23310101, 23761724, 24489904, 24687075, 24689376, 24737581, 24841671
24844841, 24903291, 24925863, 24971597, 25031502, 25035594, 25035599
25060506, 25210690, 25287072, 25293659, 25303284, 25309116, 25348956
25405687, 25416731, 25487146, 25573623, 25591292, 25607397, 25634405
25644811, 25663488, 25686739, 25696520, 25726981, 25736428, 25740844
25743479, 25756945, 25809524, 25824236, 25882883, 25890002, 25908728
25911069, 25929650, 25943740, 25958554, 25986062, 25997810, 26083489
26115103, 26164661, 26226953, 26237338, 26281476, 26284722, 26297826
26336101, 26362155, 26399691, 26405036, 26410240, 26422277, 26423085
26427905, 26440169, 26450454, 26476244, 26521043, 26536320, 26595088
26598422, 26615291, 26617804, 26646549, 26654411, 26694735, 26724511
26731697, 26745002, 26785169, 26790514, 26790923, 26792891, 26798411
26818960, 26822620, 26843558, 26843664, 26846077, 26871815, 26883456
26894737, 26895149, 26898279, 26910716, 26927998, 26928317, 26933599
26943004, 26956033, 26960097, 26961415, 26966120, 26966916, 26970175
26976568, 26985002, 26986173, 26992964, 27000158, 27005278, 27006120
27006664, 27013566, 27016033, 27026401, 27028251, 27030974, 27033520
27034688, 27035653, 27036163, 27036408, 27037839, 27038986, 27041253
27044169, 27044575, 27047831, 27053044, 27054231, 27058530, 27060167
27060859, 27061736, 27066451, 27066519, 27072923, 27073066, 27075854
27080874, 27086821, 27090765, 27093423, 27100800, 27101105, 27101527
27101652, 27105900, 27106301, 27110878, 27111780, 27112686, 27115422
27119621, 27119861, 27122162, 27125872, 27126666, 27128580, 27135647
27142120, 27142529, 27143756, 27143882, 27144928, 27147979, 27150500
27151826, 27152892, 27153641, 27155549, 27156355, 27160360, 27160922
27163928, 27164352, 27165231, 27166354, 27169796, 27169888, 27170305
27179264, 27181521, 27181537, 27181897, 27185188, 27187440, 27189611
27190851, 27193810, 27195935, 27197334, 27199245, 27200959, 27202015
27203055, 27208795, 27208953, 27210038, 27210263, 27210872, 27214085
27214204, 27215007, 27216046, 27216224, 27217412, 27220937, 27221900
27222121, 27222626, 27223075, 27224987, 27226913, 27228786, 27229389
27231051, 27232983, 27233563, 27234962, 27236052, 27236110, 27236722
27240246, 27240570, 27241221, 27241247, 27242226, 27242616, 27244337
27244785, 27244999, 27249215, 27249531, 27250547, 27251690, 27254851
27255377, 27256000, 27256488, 27256534, 27256584, 27258578, 27259307
27259386, 27259983, 27262601, 27262650, 27262798, 27262945, 27262991
27263276, 27263996, 27264464, 27266245, 27270197, 27274456, 27274536
27275136, 27275533, 27275776, 27276231, 27282707, 27283029, 27283960
27284375, 27284499, 27285244, 27288230, 27288638, 27288894, 27292213
27293599, 27294480, 27301308, 27301568, 27302594, 27302632, 27302681
```

```
27302695, 27302711, 27302714, 27302730, 27302777, 27302800, 27302960
27303287, 27303785, 27303938, 27304410, 27304906, 27304936, 27305318
27307868, 27308088, 27310092, 27313687, 27314206, 27314390, 27314697
27318117, 27318869, 27320576, 27321179, 27321834, 27326204, 27329812
27330158, 27330161, 27333658, 27333664, 27333693, 27333731, 27334316
27334648, 27335682, 27338912, 27338946, 27339115, 27339396, 27339483
27339495, 27341036, 27343844, 27345190, 27345231, 27345450, 27345498
27346329, 27346644, 27346709, 27346949, 27347126, 27348081, 27348707
27349393, 27350267, 27351628, 27352600, 27354783, 27356373, 27357773
27358241, 27359178, 27359368, 27360126, 27364854, 27364891, 27364916
27364947, 27365139, 27365702, 27365993, 27367194, 27368850, 27369515
27372756, 27375260, 27375542, 27376871, 27378103, 27379233, 27381383
27381417, 27381498, 27381656, 27383281, 27384222, 27386467, 27389352
27392187, 27393570, 27394086, 27395404, 27395416, 27395794, 27396357
27396365, 27396377, 27396624, 27396666, 27396672, 27396720, 27396794
27396813, 27397048, 27398080, 27398660, 27400416, 27400598, 27401637
27404573, 27404668, 27405242, 27405645, 27405696, 27406105, 27410279
27410300, 27410595, 27412805, 27416327, 27416997, 27417186, 27420715
27421101, 27421733, 27422874, 27423251, 27424405, 27425507, 27425622
27426363, 27427805, 27430802, 27432062, 27432338, 27432355, 27432826
27433385, 27433870, 27434050, 27434193, 27434486, 27434974, 27435537
27439835, 27441326, 27441980, 27442041, 27444727, 27445330, 27445462
27445727, 27447452, 27447687, 27448162, 27449814, 27450355, 27450400
27450783, 27451049, 27451182, 27451187, 27451531, 27452046, 27452760
27453225, 27454722, 27457666, 27457891, 27458164, 27459593, 27459909
27459948, 27460675, 27462994, 27466597, 27467543, 27468303, 27469245
27469329, 27471876, 27472969, 27473800, 27479358, 27480784, 27483974
27484556, 27486253, 27486805, 27487309, 27487795, 27487919, 27489107
27489719, 27493674, 27494663, 27496224, 27496308, 27496424, 27497950
27498477, 27501327, 27501413, 27501465, 27502420, 27504190, 27504770
27505229, 27505603, 27506774, 27507968, 27508985, 27510959, 27511196
27512439, 27517818, 27518227, 27518310, 27520070, 27520900, 27522245
27523368, 27523800, 27525909, 27526744, 27529661, 27532375, 27533780
27533819, 27534509, 27537472, 27539757, 27540613, 27541286, 27541468
27542824, 27544030, 27544973, 27545630, 27547732, 27550341, 27551855
27554074, 27555481, 27558557, 27558559, 27558861, 27560602, 27560702
27562488, 27563629, 27563767, 27565906, 27567477, 27570318, 27576342
27576354, 27577758, 27578007, 27579353, 27580996, 27585755, 27585800
27586810, 27586895, 27587672, 27587905, 27588271, 27591842, 27592466
27593389, 27593501, 27593585, 27595096, 27595973, 27599689, 27599927
27601118, 27601441, 27602091, 27602488, 27603841, 27604293, 27607563
27607805, 27608669, 27610269, 27613080, 27613247, 27613530, 27615608
27616657, 27617522, 27617978, 27620808, 27623159, 27623844, 27625274
27625620, 27629756, 27631506, 27632114, 27634676, 27634991, 27635508
27644757, 27645231, 27645940, 27649707, 27652302, 27654521, 27655217
27657712, 27658186, 27658205, 27662528, 27663370, 27664702, 27666312
27671633, 27679488, 27679664, 27679793, 27679806, 27679961, 27680162
27680509, 27680669, 27682151, 27686599, 27688036, 27688099, 27688692
27690513, 27690578, 27691809, 27691920, 27691939, 27692215, 27693416
27693713, 27694261, 27695063, 27697092, 27698953, 27700466, 27701795
27704237, 27705761, 27707544, 27709046, 27710072, 27718914, 27719187
27723002, 27723151, 27726269, 27726780, 27729678, 27732323, 27733415
27739006, 27740424, 27740844, 27744211, 27745220, 27747869, 27748954
27751006, 27751755, 27753336, 27756900, 27757567, 27757794, 27757888
27758544, 27758653, 27758972, 27759077, 27759457, 27761402, 27766324
27767081, 27769361, 27772093, 27772815, 27773602, 27774320, 27774539
27779886, 27780562, 27780683, 27782339, 27783289, 27786772, 27791223
27793533, 27797290, 27801337, 27803665, 27807441, 27810967, 27812560
27812593, 27813267, 27815347, 27818389, 27818871, 27819881, 27824540
27824543, 27825241, 27828794, 27829295, 27832643, 27833369, 27833672
27834551, 27834569, 27834984, 27835925, 27839353, 27840386, 27843646
27846298, 27846499, 27847259, 27849825, 27850112, 27851757, 27856471
27861226, 27861452, 27861909, 27869075, 27869339, 27873412, 27873643
27876671, 27882176, 27886087, 27892488, 27896443, 27896458, 27897759
27898015, 27900663, 27902561, 27908644, 27909478, 27912301, 27917669
27918832, 27920184, 27924147, 27926113, 27927431, 27929287, 27930478
```

```
27931299, 27934468, 27935348, 27935464, 27935493, 27938736, 27940876
27941110, 27941896, 27945870, 27948050, 27948153, 27950708, 27952762
27959594, 27960021, 27961746, 27964051, 27965400, 27965830, 27966472
27967484, 27970265, 27971503, 27971575, 27972265, 27975778, 27977039
27983174, 27984028, 27986817, 27989556, 27989849, 27991970, 27993289
27994325, 27994333, 27995215, 27995248, 27997875, 27998003, 27999073
27999597, 27999638, 28000269, 28004853, 28006704, 28018962, 28019283
28021205, 28022101, 28022847, 28023081, 28023399, 28023482, 28024347
28024793, 28025414, 28026866, 28033429, 28036487, 28043157, 28045903
28057267, 28058612, 28059199, 28067846, 28071549, 28072130, 28072383
28072464, 28072567, 28074713, 28079127, 28085865, 28088762, 28089440
28090453, 28091981, 28098160, 28098865, 28103600, 28103869, 28104361
28104409, 28106402, 28108003, 28108898, 28109326, 28111583, 28120036
28120951, 28124631, 28125947, 28129791, 28132287, 28135648, 28157786
28164480, 28165439, 28165545, 28169711, 28174827, 28174951, 28175445
28180464, 28181021, 28184554, 28184800, 28187706, 28188330, 28189466
28194173, 28199085, 28201419, 28204262, 28204443, 28209341, 28209985
28210192, 28211734, 28214943, 28215510, 28218832, 28220398, 28223871
28226179, 28227512, 28229360, 28236305, 28238264, 28242712, 28250929
28256164, 28258608, 28264172, 28271107, 28271119, 28271693, 28276054
28279837, 28281094, 28282606, 28285766, 28290434, 28294563, 28302049
28304709, 28305001, 28305362, 28309182, 28309406, 28312508, 28315031
28315995, 28319114, 28319623, 28320117, 28320399, 28321446, 28323201
28328895, 28329450, 28330714, 28330971, 28333072, 28338399, 28338999
28344964, 28350595, 28354603, 28357401, 28361083, 28361221, 28361787
28365111, 28369092, 28371123, 28373960, 28375383, 28378446, 28379065
28384353, 28385102, 28386259, 28388910, 28390273, 28391210, 28391582
28392168, 28392251, 28393678, 28396445, 28397317, 28401116, 28402823
28403295, 28413955, 28420042, 28420457, 28423598, 28432129, 28434028
28435825, 28437849, 28439086, 28445741, 28448314, 28454215, 28455212
28468312, 28468493, 28475164, 28478676, 28481149, 28481679, 28483184
28489150, 28492362, 28493478, 28498976, 28501075, 28502403, 28502773
28503038, 28503484, 28504545, 28507324, 28508053, 28508296, 28508557
28512336, 28512761, 28513333, 28514693, 28521330, 28527416, 28528349
28530171, 28535127, 28535272, 28538439, 28542455, 28544633, 28545134
28545687, 28546290, 28547068, 28553468, 28558645, 28564479, 28571483
28572407, 28572834, 28578164, 28578945, 28580528, 28584193, 28584217
28584444, 28585411, 28587723, 28589509, 28600233, 28608211, 28611037
28612674, 28614072, 28617631, 28617959, 28621470, 28622202, 28627255
28627686, 28632559, 28636676, 28639299, 28644549, 28646200, 28670445
28673203, 28678804, 28679454, 28680029, 28685371, 28692103, 28692275
28695694, 28697806, 28702188, 28708023, 28709063, 28710469, 28710827
28713840, 28714058, 28714988, 28728040, 28728272, 28730076, 28734355
28740708, 28742555, 28747182, 28749289, 28752599, 28755011, 28758090
28758722, 28761812, 28767240, 28770146, 28774416, 28776811, 28777174
28777214, 28777332, 28781754, 28785022, 28785531, 28791725, 28797711
28803345, 28805612, 28805695, 28809909, 28817449, 28819640, 28820669
28821847, 28830691, 28831971, 28835937, 28836716, 28838066, 28844866
28849751, 28852691, 28855922, 28856060, 28856172, 28863263, 28863487
28865569, 28867992, 28876639, 28878525, 28881723, 28887305, 28887509
28889730, 28891984, 28905457, 28919145, 28925880, 28927452, 28938924
28940179, 28949888, 28950868, 28951014, 28951382, 28956908, 28959493
28960211, 28965084, 28965095, 28986231, 28986257, 28987454, 28993295
28993353, 28993590, 29000190, 29002488, 29006527, 29007321, 29007353
29009513, 29013832, 29015118, 29015706, 29024054, 29026582, 29027694
29027940, 29032276, 29033896, 29037290, 29040739, 29048498, 29050886
29051702, 29056270, 29056767, 29060216, 29061016, 29115857, 29123482
29125374, 29136111, 29139591, 29158680, 29163567, 29170232, 29171683
29173817, 29177886, 29179097, 29182517, 29182901, 29189889, 29190663
29198092, 29200700, 29202461, 29203604, 29205918, 29212433, 29213320
29213351, 29224605, 29225076, 29230252, 29230565, 29233415, 29237575
29241345, 29242017, 29247712, 29247906, 29249289, 29250317, 29255273
29260956, 29261548, 29278684, 29285503, 29301463, 29312672, 29314539
29331209, 29331493, 29332763, 29339155, 29343086, 29343861, 29347981
29351662, 29351771, 29353821, 29356752, 29361472, 29364171, 29372460
29375355, 29375984, 29376346, 29378913, 29379978, 29382784, 29383695
```

```
29386635, 29388020, 29388952, 29391849, 29394749, 29395657, 29398488
29399046, 29399336, 29404483, 29405462, 29407804, 29408853, 29409149
29409455, 29412269, 29417719, 29426241, 29429264, 29430524, 29434301
29436454, 29437712, 29439522, 29448498, 29450812, 29452251, 29454978
29457978, 29464779, 29465177, 29483626, 29483672, 29483723, 29483771
29489436, 29493122, 29500257, 29500963, 29504682, 29511611, 29515766
29521862, 29524599, 29524985, 29525886, 29530515, 29531541, 29536342
29538631, 29541742, 29542449, 29542580, 29548413, 29548592, 29549071
29557261, 29558238, 29580394, 29591343, 29604257, 29607136, 29614098
29616244, 29625065, 29626154, 29629430, 29629745, 29632265, 29633753
29637526, 29643721, 29645349, 29651520, 29656843, 29667994, 29668005
29676089, 29685137, 29687220, 29687459, 29703195, 29707896, 29719146
29720133, 29724041, 29726695, 29739576, 29773197, 29780140, 29782211
29791152, 29794462, 29807964, 29813494, 29817278, 29825525, 29827852
29841687, 29846645, 29853485, 29865188, 29869404, 29875459, 29876358
29881050, 29884958, 29891916, 29893132, 29896510, 29902299, 29914449
29944035, 29944660, 29951620, 29961353, 29962927, 29962939, 29991257
29997326, 30018017, 30031027, 30034456, 30064268, 30073744, 30074349
30076253, 30078934, 30088912, 30098251, 30099302, 30114477, 30120608
30125944, 30128047, 30131286, 30147928, 30149035, 30163243, 30164714
30173113, 30177597, 30179644, 30189023, 30193165, 30194710, 30196358
30200758, 30215130, 30218044, 30218317, 30223712, 30232638, 30239480
30241567, 30246179, 30247305, 30252098, 30252156, 30253255, 30259008
30265523, 30272329, 30282501, 30283932, 30305880, 30312094, 30342878
30352623, 30355490, 30364613, 30365745, 30374739, 30384152, 30402386
30403763, 30408515, 30409339, 30412188, 30413137, 30416034, 30431274
30441687, 30453442, 30458593, 30460922, 30475115, 30485255, 30496957
30497057, 30501574, 30503943, 30509277, 30510527, 30582500, 30613937
30635302, 30654454, 30671813, 30741263, 30783551, 30803210, 30815852
30881588, 30533172, 30312559, 30085980, 29997959, 29997937, 28852325
28125601, 29213893, 28730253, 27304131, 27539876, 27952586, 27642235
27636900, 27461740, 28278547, 28278640, 27936676, 28502098, 28915870
28601874, 29445548, 29254623, 29774362, 30160625, 30534662, 26914402
30855101, 12816839, 18701017, 22734786, 23698980, 23840305, 25709124
25724089, 26299684, 26313403, 26433972, 26527054, 26586174, 26587652
26647619, 26827699, 26860285, 26882126, 26882316, 26943660, 26996813
27012915, 27018734, 27032726, 27034318, 27040560, 27080748, 27086406
27092991, 27098733, 27106915, 27114112, 27121566, 27133637, 27144533
27153755, 27166715, 27174938, 27174948, 27177551, 27177852, 27182006
27182064, 27184253, 27204476, 27212837, 27213140, 27220610, 27222423
27222938, 27238077, 27238258, 27249544, 27252023, 27257509, 27263677
27265816, 27267992, 27271876, 27274143, 27285557, 27299455, 27300007
27302415, 27309182, 27314512, 27315159, 27320985, 27334353, 27338838
27346984, 27358232, 27362190, 27370933, 27377219, 27378959, 27379846
27379956, 27393421, 27398223, 27399499, 27399762, 27399985, 27401618
27403244, 27404599, 27426277, 27428790, 27430219, 27430254, 27433163
27452897, 27458829, 27465480, 27475272, 27481406, 27481765, 27492916
27496806, 27503318, 27503413, 27508936, 27508984, 27513114, 27519708
27526362, 27528204, 27532009, 27534289, 27560562, 27560735, 27573154
27573408, 27574335, 27577122, 27579969, 27581484, 27593587, 27595801
27600706, 27609819, 27625010, 27625050, 27627992, 27654039, 27657467
27657920, 27668379, 27682288, 27691717, 27702244, 27703242, 27708711
27714373, 27725967, 27731346, 27734470, 27735534, 27739957, 27740854
27747407, 27748321, 27757979, 27766679, 27768034, 27778433, 27782464
27783059, 27786669, 27786699, 27801774, 27811439, 27839732, 27850736
27862636, 27864737, 27865439, 27889841, 27896388, 27897639, 27906509
27931506, 27935826, 27941514, 27957892, 27978668, 27984314, 27993298
28023410, 28025398, 28032758, 28039471, 28039953, 28045209, 28099592
28109698, 28174926, 28182503, 28204423, 28240153
```

Version 18.0.0.0.ru-2020-01.rur-2020-01.r1

La version 18.0.0.0.ru-2020-01.rur-2020-01.r1 comprend ce qui suit :

- Correctif 30480385 : Mise à jour de version de base de données : 18.9.0.0.200114
- Correctif 30501926 : MISE À JOUR VERSION OJVM : 18.9.0.0.200114
- Correctif 29997937 : DSTv34 pour RDBMS (TZDATA2019B)
- Correctif 29997959 : DSTv34 pour OJVM (TZDATA2019G)
- PreUpgrade Jar : preupgrade_181_cbuild_9_lf.zip
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS incluse dans CORRECTIF BASE DE DONNÉES 30138470
- Correctif 29213893 : DBMS_ÉCHEC DES STATS AVEC ERREUR ORA-01422 LORS DU REGROUPEMENT DES STATS POUR LA TABLE UTILIATEUR$

Mise à jour de version Oracle 18.9.0.0.200114, publiée en janvier 2020

Bogues corrigés :

```
8932139, 9062315, 13554903, 14221306, 20436508, 20549013, 21095391
21223848, 21374587, 21547051, 21744603, 21766220, 21806121, 21935698
22174392, 22282748, 22363790, 22645496, 23003564, 23061453, 23109325
23310101, 23761724, 24489904, 24687075, 24689376, 24737581, 24841671
24844841, 24903291, 24925863, 24971597, 25035594, 25035599, 25060506
25210690, 25287072, 25293659, 25303284, 25309116, 25348956, 25405687
25487146, 25573623, 25591292, 25607397, 25634405, 25644811, 25663488
25686739, 25696520, 25726981, 25736428, 25743479, 25756945, 25824236
25882883, 25890002, 25908728, 25911069, 25929650, 25943740, 25958554
25986062, 25997810, 26083489, 26115103, 26164661, 26226953, 26237338
26281476, 26284722, 26297826, 26336101, 26362155, 26399691, 26405036
26410240, 26422277, 26423085, 26427905, 26440169, 26450454, 26476244
26521043, 26536320, 26595088, 26598422, 26615291, 26617804, 26646549
26654411, 26694735, 26724511, 26731697, 26745002, 26785169, 26790514
26792891, 26798411, 26818960, 26822620, 26843558, 26843664, 26846077
26871815, 26883456, 26894737, 26895149, 26898279, 26910716, 26927998
26928317, 26933599, 26943004, 26956033, 26960097, 26961415, 26966120
26966916, 26970175, 26976568, 26985002, 26986173, 26992964, 27000158
27005278, 27006120, 27006664, 27016033, 27026401, 27028251, 27030974
27033520, 27034688, 27035653, 27036163, 27036408, 27037839, 27038986
27041253, 27044169, 27044575, 27047831, 27053044, 27054231, 27058530
27060167, 27060859, 27061736, 27066451, 27066519, 27072923, 27073066
27075854, 27080874, 27086821, 27090765, 27093423, 27101105, 27101527
27101652, 27105900, 27106301, 27110878, 27111780, 27112686, 27115422
27119621, 27119861, 27122162, 27125872, 27126666, 27128580, 27135647
27142529, 27143756, 27143882, 27144928, 27147979, 27150500, 27151826
27152892, 27153641, 27155549, 27156355, 27160360, 27160922, 27163928
27164352, 27165231, 27166354, 27169796, 27169888, 27170305, 27179264
27181521, 27181537, 27181897, 27185188, 27187440, 27189611, 27190851
27193810, 27195935, 27197334, 27199245, 27200959, 27202015, 27203055
27208795, 27208953, 27210038, 27210263, 27210872, 27214085, 27214204
27215007, 27216046, 27216224, 27220937, 27221900, 27222121, 27222626
27223075, 27224987, 27226913, 27228786, 27229389, 27231051, 27232983
27233563, 27234962, 27236052, 27236110, 27236722, 27240246, 27240570
27241221, 27241247, 27242226, 27242616, 27244337, 27244785, 27244999
27249215, 27249531, 27250547, 27251690, 27254851, 27255377, 27256000
27256488, 27256534, 27256584, 27258578, 27259307, 27259386, 27259983
27262601, 27262650, 27262798, 27262945, 27262991, 27263276, 27263996
27264464, 27266245, 27270197, 27274456, 27274536, 27275136, 27275533
27275776, 27276231, 27282707, 27283029, 27283960, 27284375, 27284499
27285244, 27288230, 27288638, 27288894, 27292213, 27293599, 27294480
27301308, 27301568, 27302594, 27302632, 27302681, 27302695, 27302711
27302714, 27302730, 27302777, 27302800, 27302960, 27303287, 27303785
27303938, 27304410, 27304906, 27304936, 27305318, 27307868, 27308088
27310092, 27313687, 27314206, 27314390, 27318117, 27318869, 27320576
```

```
27321179, 27321834, 27326204, 27329812, 27330158, 27330161, 27333658
27333664, 27333693, 27333731, 27334316, 27334648, 27335682, 27338912
27338946, 27339115, 27339396, 27339483, 27339495, 27341036, 27345190
27345231, 27345450, 27345498, 27346329, 27346644, 27346709, 27346949
27347126, 27348081, 27348707, 27349393, 27350267, 27351628, 27352600
27354783, 27356373, 27357773, 27358241, 27359178, 27359368, 27360126
27364854, 27364891, 27364916, 27364947, 27365139, 27365702, 27365993
27367194, 27368850, 27369515, 27372756, 27375260, 27375542, 27376871
27378103, 27379233, 27381383, 27381417, 27381498, 27381656, 27383281
27384222, 27386467, 27389352, 27392187, 27393570, 27394086, 27395404
27395416, 27395794, 27396357, 27396365, 27396377, 27396624, 27396666
27396672, 27396720, 27396813, 27397048, 27398080, 27398660, 27400416
27400598, 27401637, 27404573, 27404668, 27405242, 27405645, 27405696
27406105, 27410279, 27410300, 27410595, 27412805, 27416327, 27416997
27417186, 27420715, 27421101, 27421733, 27422874, 27423251, 27424405
27425507, 27425622, 27426363, 27427805, 27430802, 27432062, 27432338
27432355, 27432826, 27433385, 27433870, 27434050, 27434193, 27434486
27434974, 27435537, 27439835, 27441326, 27441980, 27442041, 27444727
27445330, 27445462, 27445727, 27447452, 27447687, 27448162, 27449814
27450355, 27450400, 27450783, 27451049, 27451182, 27451187, 27451531
27452046, 27452760, 27453225, 27454722, 27457666, 27457891, 27458164
27459909, 27459948, 27460675, 27462994, 27466597, 27467543, 27468303
27469245, 27469329, 27471876, 27472969, 27473800, 27479358, 27480784
27483974, 27484556, 27486253, 27486805, 27487309, 27487795, 27487919
27489107, 27489719, 27493674, 27496224, 27496308, 27496424, 27497950
27498477, 27501327, 27501413, 27501465, 27502420, 27504190, 27504770
27505229, 27505603, 27506774, 27507968, 27508985, 27510959, 27511196
27512439, 27517818, 27518227, 27518310, 27520070, 27520900, 27522245
27523368, 27523800, 27525909, 27526744, 27529661, 27532375, 27533780
27533819, 27534509, 27537472, 27539757, 27540613, 27541286, 27541468
27542824, 27544030, 27544973, 27545630, 27547732, 27550341, 27551855
27554074, 27555481, 27558557, 27558559, 27558861, 27560602, 27560702
27562488, 27563629, 27563767, 27565906, 27567477, 27570318, 27576342
27576354, 27577758, 27578007, 27579353, 27580996, 27585755, 27585800
27586810, 27586895, 27587672, 27587905, 27588271, 27591842, 27592466
27593389, 27593501, 27593585, 27595096, 27595973, 27599689, 27599927
27601118, 27601441, 27602091, 27602488, 27603841, 27604293, 27607563
27607805, 27608669, 27610269, 27613080, 27613247, 27613530, 27615608
27616657, 27617522, 27617978, 27620808, 27623159, 27623844, 27625274
27625620, 27629756, 27631506, 27632114, 27634676, 27634991, 27635508
27644757, 27645940, 27649707, 27652302, 27654521, 27655217, 27657712
27658186, 27658205, 27662528, 27663370, 27664702, 27666312, 27671633
27679488, 27679664, 27679793, 27679806, 27679961, 27680162, 27680509
27680669, 27682151, 27686599, 27688036, 27688099, 27688692, 27690513
27690578, 27691809, 27691920, 27691939, 27692215, 27693416, 27693713
27694261, 27695063, 27697092, 27698953, 27700466, 27701795, 27704237
27705761, 27707544, 27709046, 27710072, 27718914, 27719187, 27723002
27723151, 27726269, 27726780, 27729678, 27732323, 27733415, 27739006
27740424, 27740844, 27744211, 27745220, 27747869, 27748954, 27751006
27751755, 27753336, 27756900, 27757567, 27757794, 27757888, 27758544
27758653, 27758972, 27759077, 27759457, 27761402, 27766324, 27767081
27769361, 27772093, 27772815, 27773602, 27774320, 27774539, 27779886
27780562, 27780683, 27782339, 27783289, 27786772, 27791223, 27793533
27797290, 27801337, 27803665, 27807441, 27810967, 27812560, 27812593
27813267, 27815347, 27818389, 27818871, 27819881, 27824540, 27824543
27825241, 27828794, 27829295, 27832643, 27833369, 27833672, 27834551
27834569, 27834984, 27835925, 27839353, 27840386, 27843646, 27846298
27846499, 27847259, 27849825, 27850112, 27851757, 27856471, 27861226
27861452, 27861909, 27869075, 27869339, 27873412, 27873643, 27876671
27882176, 27886087, 27892488, 27896443, 27896458, 27897759, 27898015
27900663, 27902561, 27908644, 27909478, 27912301, 27917669, 27918832
27920184, 27924147, 27926113, 27927431, 27929287, 27930478, 27931299
27934468, 27935348, 27935493, 27938736, 27940876, 27941110, 27941896
27945870, 27948050, 27948153, 27950708, 27952762, 27959594, 27960021
27961746, 27964051, 27965400, 27965830, 27966472, 27967484, 27970265
27971503, 27971575, 27972265, 27975778, 27977039, 27983174, 27984028
```

```
27986817, 27989556, 27989849, 27991970, 27993289, 27994325, 27994333
27995215, 27995248, 27997875, 27998003, 27999073, 27999597, 27999638
28000269, 28004853, 28006704, 28018962, 28019283, 28021205, 28022101
28022847, 28023081, 28023399, 28023482, 28024347, 28026866, 28033429
28036487, 28043157, 28045903, 28057267, 28058612, 28059199, 28067846
28071549, 28072130, 28072464, 28072567, 28074713, 28079127, 28085865
28088762, 28089440, 28090453, 28091981, 28098160, 28098865, 28103600
28103869, 28104361, 28104409, 28106402, 28108003, 28108898, 28109326
28111583, 28120036, 28120951, 28124631, 28125947, 28129791, 28132287
28135648, 28164480, 28165439, 28165545, 28169711, 28174827, 28174951
28175445, 28180464, 28181021, 28184554, 28184800, 28187706, 28188330
28189466, 28194173, 28199085, 28201419, 28204262, 28204443, 28209341
28209985, 28210192, 28211734, 28214943, 28215510, 28218832, 28220398
28223871, 28226179, 28227512, 28229360, 28236305, 28238264, 28242712
28256164, 28258608, 28264172, 28271119, 28271693, 28279837, 28281094
28282606, 28285766, 28290434, 28294563, 28302049, 28304709, 28305001
28305362, 28309182, 28309406, 28312508, 28315031, 28315995, 28319114
28319623, 28320117, 28320399, 28321446, 28323201, 28328895, 28329450
28330714, 28330971, 28333072, 28338399, 28338999, 28344964, 28350595
28354603, 28357401, 28361083, 28361221, 28361787, 28365111, 28369092
28371123, 28373960, 28375383, 28378446, 28379065, 28384353, 28385102
28386259, 28388910, 28390273, 28391210, 28391582, 28392168, 28392251
28393678, 28396445, 28397317, 28401116, 28402823, 28403295, 28413955
28420042, 28420457, 28423598, 28432129, 28434028, 28435825, 28437849
28445741, 28448314, 28454215, 28455212, 28468312, 28468493, 28475164
28478676, 28481149, 28481679, 28483184, 28489150, 28492362, 28493478
28498976, 28501075, 28502403, 28502773, 28503484, 28504545, 28507324
28508053, 28508296, 28508557, 28512336, 28512761, 28513333, 28514693
28521330, 28527416, 28528349, 28530171, 28535272, 28538439, 28542455
28544633, 28545134, 28545687, 28546290, 28547068, 28553468, 28558645
28571483, 28572407, 28572834, 28578164, 28578945, 28580528, 28584193
28584217, 28584444, 28585411, 28587723, 28589509, 28600233, 28612674
28614072, 28617631, 28617959, 28621470, 28627255, 28627686, 28632559
28636676, 28639299, 28644549, 28646200, 28670445, 28673203, 28678804
28679454, 28680029, 28685371, 28692103, 28692275, 28695694, 28697806
28702188, 28708023, 28710827, 28713840, 28714058, 28714988, 28728040
28728272, 28730076, 28734355, 28742555, 28747182, 28749289, 28752599
28755011, 28758090, 28758722, 28761812, 28767240, 28770146, 28774416
28776811, 28777174, 28777214, 28777332, 28781754, 28785022, 28785531
28791725, 28797711, 28803345, 28805612, 28805695, 28809909, 28817449
28819640, 28820669, 28821847, 28830691, 28831971, 28836716, 28838066
28844866, 28849751, 28852691, 28855922, 28856060, 28856172, 28863487
28867992, 28876639, 28878525, 28881723, 28887305, 28887509, 28889730
28891984, 28905457, 28919145, 28925880, 28927452, 28938924, 28940179
28949888, 28951014, 28951382, 28956908, 28959493, 28960211, 28965084
28965095, 28986231, 28986257, 28987454, 28993353, 28993590, 29000190
29002488, 29006527, 29007321, 29007353, 29009513, 29013832, 29015118
29015706, 29024054, 29027694, 29027940, 29032276, 29033896, 29037290
29040739, 29050886, 29051702, 29056270, 29056767, 29060216, 29061016
29115857, 29123482, 29125374, 29136111, 29139591, 29158680, 29163567
29170232, 29171683, 29173817, 29177886, 29182901, 29189889, 29190663
29198092, 29200700, 29202461, 29203604, 29205918, 29212433, 29213320
29213351, 29224605, 29225076, 29230252, 29230565, 29233415, 29237575
29241345, 29242017, 29247906, 29250317, 29255273, 29260956, 29261548
29278684, 29285503, 29301463, 29312672, 29314539, 29331209, 29331493
29339155, 29347981, 29351662, 29353821, 29356752, 29364171, 29375355
29375984, 29376346, 29378913, 29379978, 29382784, 29383695, 29386635
29388020, 29388952, 29391849, 29394749, 29395657, 29398488, 29399336
29404483, 29405462, 29407804, 29408853, 29409149, 29412269, 29417719
29429264, 29430524, 29434301, 29436454, 29437712, 29439522, 29448498
29450812, 29452251, 29454978, 29457978, 29464779, 29465177, 29483626
29483672, 29483723, 29483771, 29489436, 29493122, 29500257, 29504682
29511611, 29515766, 29524599, 29525886, 29530515, 29531541, 29536342
29538631, 29541742, 29542449, 29548413, 29549071, 29557261, 29558238
29604257, 29607136, 29614098, 29616244, 29626154, 29629430, 29629745
29632265, 29633753, 29637526, 29643721, 29645349, 29651520, 29667994
```

```
29668005, 29676089, 29687459, 29703195, 29707896, 29719146, 29720133
29724041, 29726695, 29739576, 29773197, 29782211, 29791152, 29794462
29813494, 29817278, 29825525, 29841687, 29846645, 29853485, 29865188
29869404, 29875459, 29884958, 29893132, 29914449, 29944035, 29944660
29951620, 29962927, 29962939, 29991257, 29997326, 30034456, 30074349
30088912, 30098251, 30125944, 30164714, 30189023, 30193165, 30218044
30223712, 30252098, 30252156, 30253255, 30259008, 30342878, 30365745
30402386, 30408515, 30458593, 30485255
```

Version 18.0.0.0.ru-2019-10.rur-2019-10.r1

La version 18.0.0.0.ru-2019-10.rur-2019-10.r1 comprend ce qui suit :

- Correctif 30112122 : MISE À JOUR VERSION OCT 2019 BASE DE DONNÉES 18.0.0.0.191015
- Correctif 30133625 : MISE À JOUR VERSION OJVM 12.2.0.1.191015
- Correctif 29997937 : DSTv34 pour RDBMS (TZDATA2019G)
- Correctif 29997959 : DSTv34 pour OJVM (TZDATA2019G)
- PreUpgrade Jar : preupgrade_181_cbuild_8_lf.zip
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS incluse dans CORRECTIF BASE DE DONNÉES 30138470
- Correctif 29213893 : DBMS_ÉCHEC DES STATS AVEC ERREUR ORA-01422 LORS DU REGROUPEMENT DES STATS POUR LA TABLE UTILIATEUR$
- Prise en charge de Redimensionnement de l'espace de table temporaire dans un réplica en lecture (p. 1128)

Mise à jour de version Oracle 18.8.0.0.0, publiée en octobre 2019

Bogues corrigés :

```
30259008, 30253255, 8932139, 9062315, 13554903, 14221306, 20436508
21095391, 21223848, 21374587, 21547051, 21744603, 21766220, 21806121
21935698, 23003564, 23061453, 23310101, 23761724, 24489904, 24687075
24689376, 24737581, 24841671, 24844841, 24903291, 24925863, 24971597
25035594, 25035599, 25060506, 25287072, 25293659, 25303284, 25309116
25348956, 25405687, 25487146, 25591292, 25607397, 25634405, 25644811
25663488, 25686739, 25696520, 25726981, 25736428, 25743479, 25756945
25824236, 25882883, 25890002, 25908728, 25911069, 25929650, 25943740
25958554, 25986062, 25997810, 26083489, 26115103, 26164661, 26226953
26237338, 26281476, 26284722, 26297826, 26336101, 26362155, 26399691
26422277, 26423085, 26427905, 26440169, 26450454, 26476244, 26521043
26536320, 26595088, 26598422, 26615291, 26617804, 26646549, 26654411
26694735, 26724511, 26731697, 26745002, 26785169, 26790514, 26792891
26798411, 26818960, 26822620, 26843558, 26843664, 26846077, 26871815
26883456, 26894737, 26895149, 26898279, 26910716, 26927998, 26928317
26933599, 26943004, 26956033, 26960097, 26961415, 26966120, 26966916
26970175, 26976568, 26985002, 26986173, 26992964, 27000158, 27005278
27006120, 27006664, 27016033, 27026401, 27028251, 27030974, 27033520
27034688, 27035653, 27036408, 27037839, 27038986, 27041253, 27044575
27047831, 27053044, 27054231, 27058530, 27060167, 27060859, 27061736
27066451, 27066519, 27072923, 27073066, 27075854, 27080874, 27086821
27090765, 27093423, 27101105, 27101527, 27101652, 27105900, 27106301
27110878, 27111780, 27112686, 27115422, 27119621, 27122162, 27125872
27126666, 27128580, 27135647, 27142529, 27143756, 27143882, 27144928
27147979, 27150500, 27151826, 27152892, 27153641, 27155549, 27156355
27160360, 27160922, 27163928, 27164352, 27165231, 27166354, 27169796
27169888, 27170305, 27179264, 27181521, 27181537, 27181897, 27185188
```

```
27187440, 27189611, 27190851, 27193810, 27197334, 27199245, 27200959
27202015, 27208795, 27208953, 27210038, 27210263, 27210872, 27214085
27214204, 27215007, 27216046, 27216224, 27220937, 27221900, 27222121
27222626, 27223075, 27224987, 27226913, 27228786, 27229389, 27231051
27232983, 27233563, 27236052, 27236110, 27236722, 27240246, 27240570
27241221, 27241247, 27242226, 27242616, 27244337, 27244785, 27249215
27249531, 27250547, 27251690, 27254851, 27255377, 27256000, 27256488
27256534, 27256584, 27258578, 27259307, 27259386, 27259983, 27262601
27262650, 27262798, 27262945, 27262991, 27263276, 27263996, 27264464
27266245, 27270197, 27274456, 27274536, 27275136, 27275533, 27275776
27276231, 27282707, 27283029, 27283960, 27284375, 27284499, 27285244
27288230, 27288638, 27288894, 27292213, 27293599, 27294480, 27301308
27301568, 27302594, 27302632, 27302681, 27302695, 27302711, 27302714
27302730, 27302777, 27302800, 27302960, 27303287, 27303785, 27303938
27304410, 27304906, 27304936, 27305318, 27307868, 27308088, 27310092
27313687, 27314206, 27314390, 27318117, 27318869, 27320576, 27321179
27321834, 27326204, 27329812, 27330158, 27330161, 27333658, 27333664
27333693, 27333731, 27334316, 27334648, 27335682, 27338912, 27338946
27339115, 27339396, 27339483, 27339495, 27341036, 27345190, 27345231
27345450, 27345498, 27346329, 27346644, 27346709, 27346949, 27347126
27348081, 27348707, 27349393, 27350267, 27351628, 27352600, 27354783
27356373, 27357773, 27358241, 27359178, 27359368, 27360126, 27364854
27364891, 27364916, 27364947, 27365139, 27365702, 27365993, 27367194
27368850, 27369515, 27372756, 27375260, 27375542, 27376871, 27378103
27379233, 27381383, 27381417, 27381498, 27381656, 27383281, 27384222
27386467, 27389352, 27392187, 27393570, 27394086, 27395404, 27395416
27395794, 27396357, 27396365, 27396377, 27396624, 27396666, 27396672
27396813, 27397048, 27398080, 27398660, 27400416, 27400598, 27401637
27404573, 27404668, 27405242, 27405645, 27405696, 27406105, 27410279
27410300, 27410595, 27412805, 27416327, 27416997, 27417186, 27420715
27421101, 27421733, 27422874, 27423251, 27424405, 27425507, 27425622
27426363, 27427805, 27430802, 27432062, 27432338, 27432355, 27432826
27433385, 27433870, 27434050, 27434193, 27434486, 27434974, 27435537
27439835, 27441326, 27441980, 27442041, 27444727, 27445330, 27445462
27445727, 27447452, 27447687, 27448162, 27449814, 27450355, 27450400
27450783, 27451049, 27451182, 27451187, 27451531, 27452046, 27452760
27453225, 27454722, 27457666, 27457891, 27458164, 27459909, 27459948
27460675, 27462994, 27466597, 27467543, 27468303, 27469245, 27469329
27471876, 27472969, 27473800, 27479358, 27480784, 27483974, 27484556
27486253, 27487309, 27487795, 27487919, 27489719, 27493674, 27496224
27496308, 27496424, 27497950, 27498477, 27501327, 27501413, 27501465
27502420, 27504190, 27504770, 27505229, 27505603, 27506774, 27507968
27508985, 27510959, 27511196, 27512439, 27517818, 27518227, 27518310
27520070, 27520900, 27522245, 27523368, 27523800, 27525909, 27526744
27532375, 27533780, 27533819, 27534509, 27537472, 27539757, 27540613
27541286, 27541468, 27542824, 27544030, 27544973, 27545630, 27547732
27550341, 27551855, 27554074, 27555481, 27558557, 27558559, 27558861
27560602, 27560702, 27562488, 27563629, 27563767, 27565906, 27567477
27570318, 27576342, 27576354, 27577758, 27578007, 27579353, 27580996
27585755, 27585800, 27586810, 27586895, 27587672, 27588271, 27591842
27592466, 27593389, 27593501, 27593585, 27595973, 27599689, 27599927
27601118, 27601441, 27602091, 27602488, 27603841, 27604293, 27607563
27607805, 27608669, 27610269, 27613080, 27613247, 27613530, 27615608
27616657, 27617522, 27617978, 27620808, 27623159, 27623844, 27625274
27625620, 27629756, 27631506, 27632114, 27634676, 27634991, 27635508
27644757, 27645940, 27649707, 27652302, 27654521, 27655217, 27658186
27658205, 27662528, 27663370, 27664702, 27666312, 27671633, 27679488
27679664, 27679793, 27679806, 27679961, 27680162, 27680509, 27680669
27682151, 27686599, 27688036, 27688099, 27688692, 27690513, 27690578
27691809, 27691920, 27691939, 27692215, 27693416, 27693713, 27694261
27695063, 27697092, 27698953, 27700466, 27701795, 27704237, 27705761
27707544, 27709046, 27710072, 27718914, 27719187, 27723002, 27723151
27726269, 27726780, 27729678, 27732323, 27733415, 27739006, 27740424
27740844, 27744211, 27745220, 27747869, 27748954, 27751006, 27751755
27753336, 27756900, 27757567, 27757794, 27757888, 27758544, 27758653
27758972, 27759077, 27759457, 27761402, 27766324, 27767081, 27772093
```

```
27772815, 27773602, 27774320, 27774539, 27779886, 27780562, 27782339
27783289, 27786772, 27791223, 27793533, 27797290, 27801337, 27803665
27807441, 27810967, 27812560, 27812593, 27813267, 27815347, 27818871
27824540, 27824543, 27825241, 27829295, 27832643, 27833369, 27833672
27834551, 27834569, 27834984, 27835925, 27839353, 27840386, 27843646
27846298, 27846499, 27847259, 27849825, 27850112, 27851757, 27856471
27861226, 27861452, 27861909, 27869075, 27869339, 27873412, 27873643
27876671, 27882176, 27886087, 27892488, 27896443, 27896458, 27898015
27900663, 27902561, 27908644, 27912301, 27918832, 27920184, 27924147
27926113, 27930478, 27931299, 27934468, 27935348, 27935493, 27938736
27940876, 27941110, 27941896, 27945870, 27948050, 27948153, 27950708
27952762, 27959594, 27960021, 27961746, 27964051, 27965400, 27965830
27966472, 27967484, 27970265, 27971503, 27971575, 27972265, 27975778
27977039, 27983174, 27984028, 27986817, 27989556, 27989849, 27991970
27993289, 27994325, 27994333, 27995215, 27995248, 27997875, 27998003
27999073, 27999597, 27999638, 28000269, 28004853, 28006704, 28018962
28019283, 28021205, 28022101, 28022847, 28023081, 28023399, 28023482
28024347, 28026866, 28033429, 28036487, 28043157, 28045903, 28057267
28058612, 28059199, 28067846, 28072130, 28072464, 28072567, 28074713
28085865, 28088762, 28090453, 28091981, 28098865, 28103600, 28103869
28104361, 28104409, 28106402, 28108003, 28108898, 28111583, 28120036
28120951, 28124631, 28125947, 28129791, 28132287, 28135648, 28165439
28165545, 28169711, 28174827, 28174951, 28175445, 28180464, 28181021
28184554, 28184800, 28187706, 28188330, 28189466, 28194173, 28199085
28201419, 28204443, 28209341, 28210192, 28211734, 28214943, 28215510
28218832, 28220398, 28223871, 28226179, 28227512, 28229360, 28236305
28238264, 28242712, 28256164, 28258608, 28264172, 28271119, 28271693
28279837, 28281094, 28282606, 28285766, 28290434, 28294563, 28302049
28304709, 28305001, 28305362, 28309182, 28312508, 28315031, 28315995
28319114, 28319623, 28320117, 28320399, 28321446, 28323201, 28328895
28329450, 28330714, 28333072, 28338399, 28338999, 28344964, 28350595
28354603, 28357401, 28361083, 28361221, 28361787, 28365111, 28369092
28371123, 28378446, 28379065, 28384353, 28385102, 28390273, 28391210
28391582, 28392168, 28392251, 28393678, 28396445, 28401116, 28403295
28413955, 28420042, 28420457, 28423598, 28432129, 28434028, 28435825
28445741, 28448314, 28455212, 28468312, 28475164, 28478676, 28481149
28481679, 28483184, 28489150, 28492362, 28493478, 28498976, 28501075
28502403, 28502773, 28503484, 28504545, 28507324, 28508053, 28508296
28508557, 28512761, 28513333, 28514693, 28521330, 28527416, 28528349
28535272, 28542455, 28544633, 28545134, 28545687, 28547068, 28553468
28571483, 28572834, 28578164, 28580528, 28584193, 28584217, 28584444
28585411, 28587723, 28600233, 28612674, 28614072, 28617631, 28617959
28621470, 28627255, 28627686, 28632559, 28636676, 28644549, 28646200
28670445, 28673203, 28678804, 28679454, 28680029, 28685371, 28692103
28692275, 28695694, 28697806, 28702188, 28708023, 28710827, 28713840
28714058, 28714988, 28728040, 28728272, 28730076, 28742555, 28747182
28749289, 28752599, 28755011, 28758090, 28758722, 28761812, 28767240
28770146, 28774416, 28776811, 28777214, 28781754, 28785022, 28785531
28791725, 28797711, 28803345, 28805612, 28805695, 28809909, 28817449
28819640, 28820669, 28831971, 28849751, 28852691, 28855922, 28856060
28856172, 28867992, 28876639, 28878525, 28881723, 28887509, 28889730
28891984, 28905457, 28919145, 28925880, 28938924, 28940179, 28951014
28951382, 28956908, 28960211, 28965084, 28986231, 28987454, 28993353
28993590, 29000190, 29002488, 29006527, 29009513, 29015118, 29015706
29024054, 29027694, 29027940, 29032276, 29033896, 29037290, 29051702
29056270, 29056767, 29123482, 29125374, 29136111, 29139591, 29158680
29163567, 29171683, 29177886, 29189889, 29198092, 29200700, 29203604
29205918, 29212433, 29213320, 29213351, 29224605, 29225076, 29230252
29230565, 29233415, 29241345, 29242017, 29247906, 29250317, 29255273
29285503, 29301463, 29312672, 29314539, 29331209, 29331493, 29339155
29347981, 29351662, 29353821, 29356752, 29364171, 29376346, 29378913
29379978, 29382784, 29386635, 29388020, 29388952, 29391849, 29394749
29395657, 29398488, 29404483, 29405462, 29407804, 29409149, 29412269
29417719, 29429264, 29430524, 29436454, 29437712, 29439522, 29464779
29465177, 29483672, 29483723, 29493122, 29500257, 29504682, 29511611
29515766, 29524599, 29525886, 29530515, 29531541, 29541742, 29542449
```

```
29548413, 29557261, 29607136, 29614098, 29616244, 29632265, 29633753
29637526, 29645349, 29668005, 29676089, 29687459, 29707896, 29724041
29782211, 29813494, 29893132, 30034456, 30088912, 30189023
```

Version 18.0.0.0.ru-2019-07.rur-2019-07.r1

La version 18.0.0.0.ru-2019-07.rur-2019-07.r1 comprend ce qui suit :

- Correctif 29757256 : Mise à jour de version de base de données : 18.7.0.0.190716
- Correctif 29774410 : MISE À JOUR DE VERSION OJVM : 18.7.0.0.190716
- Correctif 27539475 : « ORA-3816 – INFORMATION SUR LE MESSAGE MANQUANT POUR L'ERREUR 3816 ».
- Correctif 29213893 : « DBMS_ÉCHEC DES STATS AVEC ERREUR ORA-01422 LORS DU REGROUPEMENT DES STATS POUR LA TABLE USER$ »
- Correctif 28125601 : DSTv32 pour RDBMS (TZDATA2018E)
- Correctif 28852325 : DSTv33 pour RDBMS (TZDATA2018G)
- Correctif 28852334 : DSTv33 pour OJVM (TZDATA2018G)
- PreUpgrade Jar : preupgrade_181_cbuild_7_lf.zip
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS

Mise à jour de version Oracle 18.7.0.0.190716, publiée en juillet 2019

Bogues corrigés :

```
8932139, 9062315, 13554903, 14221306, 20436508, 21095391, 21223848
21547051, 21744603, 21766220, 21806121, 23003564, 23061453, 23310101
23761724, 24489904, 24689376, 24737581, 24841671, 24844841, 24903291
24925863, 24971597, 25035594, 25035599, 25287072, 25293659, 25303284
25309116, 25348956, 25405687, 25487146, 25591292, 25607397, 25634405
25644811, 25663488, 25686739, 25726981, 25736428, 25743479, 25756945
25824236, 25882883, 25890002, 25908728, 25911069, 25929650, 25943740
25958554, 25986062, 25997810, 26083489, 26115103, 26164661, 26226953
26237338, 26281476, 26284722, 26297826, 26336101, 26362155, 26399691
26422277, 26423085, 26427905, 26440169, 26450454, 26476244, 26521043
26536320, 26595088, 26598422, 26615291, 26617804, 26646549, 26654411
26694735, 26731697, 26745002, 26785169, 26790514, 26792891, 26818960
26822620, 26843558, 26843664, 26846077, 26871815, 26883456, 26894737
26895149, 26898279, 26927998, 26928317, 26933599, 26943004, 26956033
26960097, 26961415, 26966120, 26966916, 26970175, 26985002, 26986173
26992964, 27000158, 27005278, 27006120, 27006664, 27016033, 27026401
27028251, 27030974, 27034688, 27035653, 27036408, 27037839, 27038986
27041253, 27044575, 27047831, 27053044, 27054231, 27058530, 27060167
27060859, 27061736, 27066451, 27066519, 27073066, 27075854, 27080874
27086821, 27090765, 27093423, 27101105, 27101527, 27101652, 27105900
27106301, 27110878, 27111780, 27112686, 27115422, 27119621, 27122162
27125872, 27126666, 27128580, 27135647, 27142529, 27143756, 27143882
27147979, 27150500, 27151826, 27152892, 27153641, 27155549, 27156355
27160360, 27160922, 27163928, 27164352, 27165231, 27166354, 27169796
27169888, 27170305, 27179264, 27181521, 27181537, 27181897, 27185188
27187440, 27189611, 27190851, 27193810, 27197334, 27199245, 27200959
27202015, 27208795, 27208953, 27210038, 27210263, 27210872, 27214085
27215007, 27216046, 27216224, 27220937, 27221900, 27222121, 27222626
27223075, 27224987, 27226913, 27228786, 27229389, 27231051, 27232983
```

```
27233563, 27236052, 27236110, 27236722, 27240246, 27240570, 27241221
27241247, 27242226, 27242616, 27244337, 27244785, 27249215, 27249531
27250547, 27251690, 27254851, 27255377, 27256000, 27256488, 27256534
27256584, 27258578, 27259307, 27259386, 27259983, 27262601, 27262650
27262798, 27262945, 27262991, 27263276, 27263996, 27266245, 27270197
27274456, 27274536, 27275136, 27275533, 27275776, 27276231, 27282707
27283029, 27283960, 27284375, 27284499, 27285244, 27288230, 27288638
27288894, 27292213, 27293599, 27294480, 27301308, 27301568, 27302594
27302632, 27302681, 27302695, 27302711, 27302714, 27302730, 27302777
27302800, 27302960, 27303287, 27303785, 27303938, 27304410, 27304936
27305318, 27307868, 27308088, 27310092, 27313687, 27314206, 27314390
27318117, 27318869, 27320576, 27321179, 27321834, 27326204, 27329812
27330158, 27330161, 27333658, 27333664, 27333693, 27333731, 27334316
27334648, 27335682, 27338912, 27338946, 27339115, 27339396, 27339483
27339495, 27341036, 27345190, 27345231, 27345450, 27345498, 27346329
27346644, 27346709, 27346949, 27347126, 27348081, 27348707, 27349393
27350267, 27351628, 27352600, 27354783, 27356373, 27357773, 27358241
27359178, 27359368, 27360126, 27364854, 27364891, 27364916, 27364947
27365139, 27365702, 27365993, 27367194, 27368850, 27372756, 27375260
27375542, 27376871, 27378103, 27379233, 27381383, 27381417, 27381498
27381656, 27384222, 27386467, 27389352, 27392187, 27394086, 27395404
27395416, 27395794, 27396357, 27396365, 27396377, 27396624, 27396666
27396672, 27396813, 27397048, 27398080, 27398660, 27400416, 27400598
27401637, 27404668, 27405242, 27405645, 27405696, 27410279, 27410300
27410595, 27412805, 27416327, 27416997, 27417186, 27420715, 27421101
27421733, 27422874, 27423251, 27424405, 27425507, 27425622, 27426363
27427805, 27430802, 27432062, 27432338, 27432355, 27432826, 27433870
27434050, 27434193, 27434486, 27434974, 27435537, 27439835, 27441326
27441980, 27442041, 27444727, 27445330, 27445462, 27445727, 27447452
27447687, 27448162, 27449814, 27450355, 27450400, 27450783, 27451049
27451182, 27451187, 27451531, 27452046, 27452760, 27453225, 27454722
27457666, 27457891, 27458164, 27459909, 27460675, 27462994, 27466597
27467543, 27468303, 27469245, 27469329, 27471876, 27472969, 27473800
27479358, 27480784, 27483974, 27484556, 27486253, 27487309, 27487795
27487919, 27489719, 27493674, 27496224, 27496308, 27496424, 27497950
27498477, 27501327, 27501413, 27501465, 27502420, 27504190, 27504770
27505229, 27505603, 27506774, 27507968, 27508985, 27510959, 27511196
27512439, 27517818, 27518227, 27518310, 27520070, 27520900, 27522245
27523368, 27523800, 27525909, 27526744, 27532375, 27533819, 27534509
27537472, 27539757, 27540613, 27541286, 27541468, 27542824, 27544030
27544973, 27545630, 27547732, 27550341, 27551855, 27554074, 27555481
27558557, 27558559, 27558861, 27560602, 27560702, 27562488, 27563629
27563767, 27565906, 27567477, 27570318, 27576342, 27577758, 27578007
27579353, 27580996, 27585755, 27585800, 27586810, 27586895, 27587672
27591842, 27592466, 27593389, 27593501, 27593585, 27595973, 27599689
27599927, 27601118, 27602091, 27602488, 27603841, 27604293, 27607563
27607805, 27608669, 27610269, 27613080, 27613247, 27613530, 27615608
27616657, 27617522, 27617978, 27620808, 27623844, 27625274, 27625620
27629756, 27631506, 27634676, 27634991, 27635508, 27644757, 27645940
27649707, 27652302, 27654521, 27655217, 27658186, 27658205, 27662528
27663370, 27664702, 27666312, 27671633, 27679488, 27679664, 27679793
27679806, 27679961, 27680162, 27680509, 27680669, 27682151, 27686599
27688036, 27688099, 27688692, 27690513, 27690578, 27691809, 27691920
27691939, 27692215, 27693416, 27693713, 27694261, 27695063, 27697092
27698953, 27700466, 27701795, 27704237, 27705761, 27707544, 27709046
27710072, 27718914, 27719187, 27723002, 27723151, 27726269, 27726780
27729678, 27732323, 27733415, 27739006, 27740424, 27740844, 27744211
27745220, 27747869, 27748954, 27751006, 27751755, 27753336, 27756900
27757567, 27757794, 27757888, 27758972, 27759077, 27759457, 27761402
27766324, 27767081, 27772093, 27772815, 27773602, 27774320, 27774539
27779886, 27780562, 27782339, 27783289, 27786772, 27791223, 27793533
27797290, 27801337, 27803665, 27807441, 27810967, 27812560, 27812593
27813267, 27815347, 27818871, 27824540, 27824543, 27825241, 27829295
27832643, 27833369, 27833672, 27834551, 27834984, 27835925, 27839353
27840386, 27843646, 27846298, 27846499, 27847259, 27849825, 27851757
27856471, 27861226, 27861452, 27861909, 27869075, 27869339, 27873643
```

```
27876671, 27882176, 27892488, 27896443, 27896458, 27898015, 27900663
27908644, 27912301, 27918832, 27920184, 27924147, 27926113, 27930478
27931299, 27934468, 27935348, 27938736, 27940876, 27941110, 27941896
27945870, 27948050, 27948153, 27950708, 27952762, 27959594, 27960021
27961746, 27964051, 27965830, 27966472, 27970265, 27971503, 27971575
27972265, 27975778, 27977039, 27983174, 27984028, 27986817, 27989556
27989849, 27991970, 27993289, 27994325, 27994333, 27995215, 27995248
27997875, 27998003, 27999073, 27999597, 27999638, 28000269, 28004853
28006704, 28018962, 28019283, 28021205, 28022101, 28022847, 28023081
28023399, 28023482, 28024347, 28026866, 28033429, 28036487, 28045903
28057267, 28058612, 28059199, 28067846, 28072130, 28072464, 28072567
28074713, 28085865, 28088762, 28090453, 28091981, 28098865, 28103600
28103869, 28104361, 28106402, 28108003, 28108898, 28111583, 28120036
28120951, 28124631, 28129791, 28132287, 28135648, 28165439, 28165545
28169711, 28174827, 28174951, 28175445, 28180464, 28181021, 28184554
28184800, 28187706, 28188330, 28189466, 28194173, 28199085, 28201419
28204443, 28209341, 28210192, 28211734, 28214943, 28215510, 28218832
28220398, 28223871, 28226179, 28227512, 28229360, 28236305, 28238264
28242712, 28258608, 28264172, 28271119, 28271693, 28279837, 28281094
28282606, 28285766, 28290434, 28302049, 28304709, 28305001, 28305362
28309182, 28312508, 28315031, 28315995, 28319623, 28320117, 28320399
28321446, 28323201, 28328895, 28329450, 28330714, 28333072, 28338399
28338999, 28344964, 28350595, 28354603, 28357401, 28361083, 28361221
28361787, 28365111, 28369092, 28371123, 28378446, 28379065, 28385102
28390273, 28391582, 28392168, 28392251, 28393678, 28396445, 28403295
28413955, 28420042, 28420457, 28423598, 28432129, 28434028, 28435825
28445741, 28448314, 28455212, 28468312, 28475164, 28478676, 28481149
28481679, 28483184, 28489150, 28492362, 28493478, 28501075, 28502403
28502773, 28503484, 28504545, 28507324, 28508053, 28508296, 28508557
28512761, 28513333, 28514693, 28521330, 28527416, 28528349, 28535272
28544633, 28545134, 28545687, 28547068, 28553468, 28571483, 28572834
28578164, 28580528, 28584193, 28584217, 28584444, 28587723, 28600233
28612674, 28614072, 28617631, 28617959, 28621470, 28627255, 28632559
28636676, 28644549, 28646200, 28670445, 28673203, 28679454, 28680029
28685371, 28692275, 28695694, 28702188, 28708023, 28710827, 28713840
28714058, 28728040, 28728272, 28730076, 28742555, 28747182, 28749289
28752599, 28755011, 28758090, 28758722, 28761812, 28767240, 28770146
28774416, 28777214, 28781754, 28785022, 28785531, 28803345, 28805612
28805695, 28809909, 28819640, 28849751, 28852691, 28856060, 28856172
28878525, 28881723, 28887509, 28891984, 28919145, 28925880, 28938924
28940179, 28951014, 28951382, 28956908, 28960211, 28986231, 28987454
28993353, 28993590, 29000190, 29006527, 29015118, 29015706, 29024054
29027694, 29032276, 29033896, 29037290, 29051702, 29056270, 29123482
29125374, 29136111, 29139591, 29158680, 29171683, 29177886, 29189889
29200700, 29203604, 29205918, 29224605, 29230565, 29242017, 29301463
29314539, 29331209, 29331493, 29339155, 29347981, 29356752, 29364171
29376346, 29378913, 29379978, 29382784, 29388020, 29388952, 29394749
29395657, 29405462, 29409149, 29412269, 29429264, 29430524, 29436454
29437712, 29439522, 29504682, 29511611, 29531541, 29542449, 29616244
29676089, 29813494
```

Moteur de base de données : 12.2.0.1

Pour Oracle 12c version 12.2.0.1, Oracle a modifié la façon dont il distribue les mises à jour Oracle Database. Au lieu des mises à jour d'ensemble de correctifs (PSU), Oracle fournit des mises à jour de version (RU) et des révisions des mises à jour de version (RUR). Les RU incluent des modifications de l'optimiseur, des ajouts de fonctionnalités et des correctifs de sécurité. Les RUR contiennent uniquement des correctifs de sécurité pour les deux cycles de correctifs trimestriels précédents. Avec ce nouveau système, vous avez plus de contrôle sur les fonctions que vous installez à chaque mise à jour.

Les conventions d'attribution de noms ont également changé pour Oracle 12c version 12.2.0.1 Dans les versions précédentes, Amazon RDS pour Oracle utilisait la convention d'attribution de noms *version-*

oracle.v*version-correctif* pour les PSU. La section *version-correctif* correspondait à une PSU Oracle. Par exemple, dans Oracle pour Amazon RDS version 12.1.0.2.v13, la section v13 du numéro de version correspond à une PSU Oracle.

Les conventions d'attribution de noms Oracle 12c version 12.2.0.1 représentent les mises à jour de type RU et RUR. Par exemple, la première version Amazon RDS pour Oracle disponible est 12.2.0.1.ru-2018-10.rur-2018-10.r1. Dans cet exemple, 12.2 correspond à la version majeure, et 0.1 à la version mineure. La version de la révision possède les sections suivantes :

- ru-2018-10 – RU d'octobre
- rur-2018-10 – RUR d'octobre pour la RU d'octobre
- r1 – Révision Amazon RDS interne, qui permet à Amazon RDS de distinguer les correctifs d'urgence des RU/RUR préexistants

Pour en savoir plus sur le nouveau système de gestion des versions d'Oracle Database, consultez les articles Differences between PSU / BP and RU / RUR du blog Upgrade your Database – NOW! et RU and RUR patches for Oracle 12.2 du blog Oracle–Help.

Les versions suivantes sont disponibles pour le moteur de base de données Oracle 12.2.0.2 :

- Version 12.2.0.1.ru-2020-07.rur-2020-07.r1 (p. 1249)
- Version 12.2.0.1.ru-2020-04.rur-2020-04.r1 (p. 1254)
- Version 12.2.0.1.ru-2020-01.rur-2020-01.r1 (p. 1258)
- Version 12.2.0.1.ru-2019-10.rur-2019-10.r1 (p. 1262)
- Version 12.2.0.1.ru-2019-07.rur-2019-07.r1 (p. 1266)
- Version 12.2.0.1.ru-2019-04.rur-2019-04.r1 (p. 1269)
- Version 12.2.0.1.ru-2019-01.rur-2019-01.r1 (p. 1272)
- Version 12.2.0.1.ru-2018-10.rur-2018-10.r1 (p. 1275)

Version 12.2.0.1.ru-2020-07.rur-2020-07.r1

La version 12.2.0.1.ru-2020-07.rur-2020-07.r1 comprend ce qui suit :

- Correctif 31312468 : mise à jour version base de données juillet 2020 : 12.2.0.1.200714
- Correctif 31219919 : MISE À JOUR VERSION OJVM 12.2.0.1.200714
- Correctif 31335037 : DSTV35 pour RDBMS (TZDATA2020A)
- Correctif 31335142 : DSTV35 pour OJVM (TZDATA2020A)
- Correctif 29213893 : DBMS_ÉCHEC DES STATS AVEC ERREUR ORA-01422 LORS DU REGROUPEMENT DES STATS POUR LA TABLE UTILIATEUR$
- PreUpgrade Jar : preupgrade_12201_cbuild_23_lf.zip

Correctifs combinés pour la version 12.2.0.1.ru-2020-07.rur-2020-07.r1, publiés en juillet 2020

Bogues corrigés :

```
7391838, 8480838, 8932139, 8975044, 12763598, 13554903, 14221306
14690846, 15931756, 16002385, 16438495, 16727454, 16942578, 17027695
17533661, 17947871, 18308268, 18521691, 18594510, 18774543, 18878420
18986501, 19072655, 19211433, 19285025, 19327292, 19526548, 19614243
```

```
19647894, 19649997, 19702201, 19721304, 20003668, 20087519, 20118035
20120236, 20324049, 20436508, 20532077, 20549013, 20588486, 20591151
20617383, 20620169, 20736227, 20756305, 20866970, 20976443, 21070321
21089435, 21095391, 21143725, 21147908, 21159907, 21178363, 21186167
21197098, 21216226, 21320338, 21433452, 21479706, 21517767, 21520266
21547051, 21638600, 21744603, 21788462, 21837606, 21882528, 21935698
21981529, 21985256, 22007324, 22070226, 22070473, 22070853, 22072543
22087683, 22104866, 22107360, 22174392, 22179537, 22282748, 22310426
22347493, 22363790, 22364044, 22367053, 22379010, 22446455, 22454940
22495673, 22503283, 22503297, 22504793, 22522515, 22530986, 22564336
22568728, 22581771, 22594071, 22599050, 22628825, 22645009, 22645496
22654475, 22700845, 22726044, 22729345, 22826067, 22843979, 22845846
22864303, 22898198, 22921674, 22939829, 22950945, 22970869, 22981722
23018676, 23019710, 23026585, 23035249, 23055900, 23056058, 23061453
23065002, 23066146, 23080557, 23104033, 23105538, 23109325, 23110523
23125560, 23126545, 23127945, 23143074, 23151677, 23168363, 23169712
23177923, 23179662, 23184263, 23197730, 23234232, 23237091, 23249829
23271203, 23278750, 23281269, 23300142, 23306590, 23308065, 23310101
23312077, 23328639, 23333567, 23336559, 23342170, 23481673, 23491861
23499004, 23499160, 23521523, 23527363, 23533647, 23548817, 23567857
23572982, 23581777, 23588722, 23599216, 23600861, 23602213, 23614158
23645516, 23665623, 23709062, 23715460, 23715518, 23730961, 23733981
23735292, 23738304, 23741944, 23743596, 23746128, 23749454, 23761724
24006569, 24010030, 24289874, 24289895, 24294174, 24303148, 24307571
24308349, 24326444, 24326846, 24328857, 24330708, 24332831, 24334708
24336249, 24337882, 24341675, 24343905, 24345420, 24346821, 24348685
24350620, 24352981, 24355111, 24357348, 24368004, 24371491, 24373528
24373756, 24374976, 24376875, 24376878, 24383086, 24385983, 24401351
24403922, 24409977, 24415926, 24416451, 24421668, 24423416, 24425056
24425998, 24435982, 24437162, 24440648, 24443539, 24457597, 24460392
24461826, 24467122, 24468470, 24470606, 24471079, 24471473, 24473736
24484749, 24485034, 24485161, 24485174, 24485619, 24486059, 24486237
24509056, 24516314, 24530364, 24534401, 24554533, 24555417, 24556862
24556967, 24560906, 24563422, 24570214, 24570598, 24573817, 24578718
24578797, 24588377, 24589081, 24589590, 24591506, 24593740, 24595699
24596874, 24600330, 24609592, 24609996, 24611527, 24616637, 24617969
24623975, 24624166, 24642495, 24654629, 24655717, 24664211, 24668398
24669189, 24669730, 24674197, 24674955, 24676172, 24677696, 24680959
24687075, 24689376, 24692973, 24693010, 24693290, 24697323, 24699619
24701840, 24710696, 24713381, 24714096, 24717183, 24717859, 24718260
24719799, 24735430, 24737064, 24737403, 24737581, 24737954, 24739791
24744383, 24744686, 24752618, 24757934, 24759556, 24760407, 24764085
24766309, 24784414, 24786669, 24791883, 24792678, 24793511, 24796092
24797119, 24798481, 24800423, 24801152, 24802934, 24808504, 24811725
24812047, 24818566, 24827228, 24827654, 24831514, 24835919, 24841671
24843188, 24844549, 24844841, 24845157, 24848746, 24848923, 24850622
24907917, 24908063, 24908321, 24911709, 24912588, 24920582, 24921478
24922704, 24923080, 24923215, 24923338, 24923790, 24924667, 24926999
24929210, 24938784, 24940060, 24942749, 24953434, 24957555, 24960044
24960809, 24965426, 24966594, 24966788, 24967993, 24968162, 24976007
24978100, 25022574, 25027852, 25028996, 25029022, 25029423, 25031502
25032818, 25034396, 25036006, 25036474, 25042823, 25044977, 25045228
25050160, 25051465, 25051628, 25054064, 25057811, 25058080, 25060506
25062592, 25063971, 25065563, 25072986, 25077278, 25078611, 25086233
25087436, 25091141, 25092777, 25093872, 25095982, 25098160, 25099339
25099497, 25099758, 25100063, 25100579, 25103996, 25107662, 25110233
25114561, 25120284, 25120668, 25120742, 25121089, 25123585, 25124363
25129925, 25130312, 25140197, 25145163, 25145215, 25150925, 25159176
25162645, 25164293, 25166187, 25171041, 25171084, 25173124, 25175723
25176408, 25178032, 25178101, 25178179, 25179774, 25182817, 25184453
25184555, 25186079, 25189723, 25191872, 25192044, 25192528, 25192729
25195901, 25199585, 25200101, 25201454, 25202355, 25203656, 25205954
25206864, 25207410, 25209912, 25210268, 25210499, 25210690, 25211628
25219450, 25223839, 25224242, 25225795, 25226665, 25227381, 25230870
25230945, 25237577, 25240188, 25240590, 25241448, 25241625, 25244807
25248384, 25250109, 25251648, 25257085, 25259611, 25262869, 25263960
```

```
25265499, 25269133, 25283790, 25287072, 25293659, 25296876, 25299227
25299807, 25300427, 25303284, 25303756, 25305405, 25307368, 25309116
25313154, 25313411, 25316758, 25317989, 25320555, 25323525, 25328093
25328518, 25329664, 25335249, 25335360, 25335790, 25337332, 25337640
25348956, 25353983, 25356118, 25357142, 25360661, 25362958, 25367588
25367721, 25382812, 25383204, 25384462, 25386748, 25388573, 25388896
25392535, 25393714, 25395696, 25397936, 25398306, 25404202, 25405100
25405687, 25405813, 25410017, 25410180, 25410802, 25410877, 25411036
25415713, 25416731, 25417050, 25417056, 25417958, 25425005, 25425451
25425760, 25427662, 25429959, 25430120, 25433696, 25435038, 25437699
25440818, 25442559, 25444961, 25445168, 25451531, 25452452, 25455795
25457409, 25459958, 25462714, 25463844, 25472112, 25472885, 25476125
25476149, 25477657, 25478885, 25479164, 25481087, 25482971, 25486384
25489342, 25489367, 25489607, 25492379, 25498930, 25498994, 25516250
25524955, 25528838, 25530080, 25530814, 25535668, 25536819, 25537470
25539063, 25540738, 25546580, 25546608, 25547901, 25551676, 25553616
25554787, 25555252, 25557886, 25558986, 25560487, 25560538, 25561296
25569149, 25570929, 25573623, 25575348, 25575369, 25575628, 25576115
25579458, 25579761, 25591394, 25594901, 25597525, 25598473, 25599425
25600342, 25600421, 25601999, 25602488, 25603923, 25606091, 25607726
25612095, 25614866, 25616268, 25616359, 25616417, 25616645, 25631933
25633101, 25634317, 25634348, 25635149, 25638456, 25639019, 25643818
25643889, 25643931, 25646373, 25647325, 25648731, 25653109, 25654459
25654936, 25655390, 25655966, 25659655, 25660847, 25661819, 25662088
25662101, 25662524, 25663488, 25667973, 25669791, 25670786, 25671354
25672640, 25674386, 25680221, 25685152, 25686739, 25687460, 25691904
25694206, 25695903, 25696520, 25699321, 25700654, 25709368, 25710420
25715167, 25717371, 25722055, 25722608, 25722720, 25723097, 25723158
25728085, 25729507, 25730014, 25734963, 25736747, 25739065, 25740844
25741955, 25743479, 25747569, 25749273, 25752755, 25754606, 25756945
25757697, 25757748, 25760195, 25762221, 25764020, 25766822, 25768681
25772669, 25774077, 25775213, 25775444, 25780343, 25783447, 25784002
25785331, 25785441, 25788879, 25789041, 25789277, 25789579, 25790353
25792911, 25795865, 25797092, 25797124, 25797305, 25800464, 25802510
25803364, 25803545, 25807997, 25809524, 25810263, 25810704, 25811105
25811650, 25812390, 25813931, 25818707, 25822410, 25823532, 25823754
25824372, 25825910, 25826740, 25830492, 25832935, 25834581, 25835365
25838361, 25838755, 25852885, 25856821, 25858672, 25861398, 25865785
25866948, 25870579, 25871177, 25871639, 25871753, 25872127, 25872389
25873336, 25874050, 25874678, 25881255, 25882264, 25883438, 25885148
25888073, 25888984, 25890002, 25890046, 25890056, 25890673, 25890782
25894239, 25895224, 25897615, 25898228, 25904273, 25904490, 25905130
25906117, 25906886, 25908728, 25911724, 25914276, 25919622, 25932524
25932728, 25933494, 25941836, 25942868, 25943271, 25945130, 25947799
25951571, 25953857, 25954022, 25954054, 25957038, 25963024, 25964954
25967544, 25967985, 25970731, 25971286, 25972417, 25973152, 25975723
25977302, 25980605, 25980770, 25981498, 25982666, 25986062, 25990907
25995938, 25997810, 26006257, 26007010, 26019148, 26023042, 26024732
26024784, 26025681, 26029075, 26029777, 26029780, 26032573, 26034119
26036748, 26037215, 26038086, 26039623, 26040483, 26045732, 26051656
26078437, 26078493, 26080410, 26083298, 26087754, 26088426, 26088836
26089669, 26090767, 26090893, 26091640, 26091786, 26095327, 26095405
26096382, 26108080, 26108337, 26110259, 26110632, 26111842, 26112621
26115103, 26121990, 26124078, 26130486, 26137367, 26137416, 26138085
26145560, 26149904, 26153372, 26153977, 26168933, 26169341, 26169345
26170659, 26170715, 26176002, 26187943, 26189861, 26198757, 26198926
26201113, 26203182, 26223039, 26237338, 26237431, 26237773, 26238195
26242031, 26242677, 26243698, 26244115, 26245237, 26248143, 26249718
26256131, 26257953, 26259265, 26261327, 26263328, 26263721, 26268756
26269790, 26271001, 26274660, 26275023, 26275415, 26277439, 26281476
26285062, 26285933, 26308650, 26309047, 26317991, 26318627, 26323308
26324206, 26324769, 26325856, 26327418, 26327624, 26327775, 26330994
26331743, 26333141, 26334602, 26336977, 26338953, 26351334, 26351996
26353617, 26354844, 26356098, 26358670, 26359091, 26362155, 26362821
26366517, 26367012, 26367460, 26371725, 26373967, 26374791, 26375052
26375250, 26375330, 26380097, 26385189, 26386858, 26388538, 26396790
```

```
26398675, 26399626, 26399691, 26405036, 26406387, 26407408, 26410240
26412540, 26418088, 26420561, 26421667, 26422277, 26423085, 26426526
26426967, 26430323, 26430737, 26434436, 26434999, 26435073, 26436168
26438612, 26439748, 26440142, 26440169, 26440749, 26441345, 26442308
26444601, 26444887, 26446098, 26452606, 26474662, 26474703, 26475419
26476090, 26476244, 26478970, 26479173, 26482376, 26486365, 26492866
26493289, 26498354, 26513067, 26513709, 26521043, 26522439, 26523432
26526726, 26526799, 26536320, 26537307, 26542135, 26542236, 26542835
26544823, 26545688, 26546070, 26546664, 26546754, 26548363, 26556014
26558437, 26569225, 26570134, 26575788, 26580633, 26582460, 26584641
26588069, 26597140, 26599395, 26608137, 26608238, 26609942, 26615291
26615690, 26617804, 26623652, 26626879, 26629381, 26633355, 26633558
26635897, 26637273, 26637824, 26639167, 26641610, 26641852, 26650226
26650540, 26654363, 26658759, 26659182, 26669550, 26680105, 26712331
26714486, 26714910, 26717528, 26724511, 26725687, 26727397, 26729494
26729611, 26740700, 26743240, 26744595, 26745002, 26751106, 26751171
26755171, 26758193, 26764561, 26765212, 26768025, 26775602, 26784509
26790923, 26794786, 26797591, 26798411, 26798514, 26798516, 26802503
26816582, 26820076, 26822314, 26822620, 26824833, 26828994, 26829845
26830694, 26832296, 26833932, 26837569, 26837702, 26840654, 26844406
26844870, 26849779, 26871815, 26875822, 26883456, 26895149, 26896659
26898563, 26907236, 26907327, 26908788, 26909100, 26909504, 26910716
26911000, 26923777, 26939314, 26943004, 26944190, 26947373, 26958896
26963310, 26966616, 26966916, 26967713, 26968670, 26969321, 26970175
26970717, 26981902, 26983259, 26985002, 26986173, 26992964, 26999139
27000158, 27000702, 27006120, 27006664, 27009164, 27013146, 27015449
27028251, 27032785, 27033520, 27033652, 27034890, 27036163, 27037839
27038986, 27039712, 27044169, 27044297, 27045634, 27052607, 27056711
27058530, 27060167, 27060859, 27061736, 27072923, 27073314, 27079140
27084613, 27087426, 27090765, 27092508, 27093423, 27097854, 27100800
27101105, 27105900, 27106179, 27110878, 27115422, 27117822, 27119621
27119861, 27122162, 27124624, 27125872, 27133662, 27134734, 27135647
27135993, 27138325, 27142120, 27142373, 27142529, 27144928, 27151826
27153641, 27160922, 27161071, 27162390, 27162405, 27163928, 27165231
27169796, 27170305, 27181537, 27181897, 27185188, 27195935, 27199245
27200959, 27202015, 27203055, 27207110, 27207634, 27208795, 27213224
27216046, 27217412, 27223075, 27229389, 27231051, 27234962, 27236722
27242226, 27244337, 27244999, 27248917, 27249531, 27250547, 27251690
27254335, 27255377, 27256000, 27258578, 27259307, 27262945, 27264464
27266245, 27274456, 27274536, 27275533, 27276231, 27283960, 27284499
27285244, 27288638, 27292213, 27293599, 27302711, 27302730, 27303287
27303938, 27304410, 27304906, 27305039, 27308088, 27314206, 27314390
27314697, 27320576, 27321179, 27329612, 27333106, 27334316, 27338912
27338946, 27339115, 27345231, 27346709, 27348081, 27349393, 27350267
27351628, 27359178, 27364854, 27365014, 27367194, 27369515, 27370965
27375542, 27381498, 27383281, 27386467, 27392968, 27393570, 27394703
27395416, 27396624, 27396672, 27396813, 27397048, 27400416, 27400598
27404573, 27404668, 27405645, 27416997, 27423251, 27424405, 27426363
27432062, 27432826, 27433385, 27433870, 27434193, 27439835, 27441326
27442041, 27445727, 27457891, 27459593, 27459948, 27461740, 27466597
27468303, 27486805, 27487919, 27489107, 27493674, 27494663, 27501373
27501413, 27502420, 27504770, 27505229, 27508985, 27510959, 27525909
27529661, 27533780, 27533819, 27534509, 27539876, 27540613, 27544973
27548131, 27554074, 27555481, 27558861, 27560602, 27562488, 27565906
27567477, 27576342, 27576354, 27587905, 27588271, 27589260, 27593501
27595973, 27601118, 27601441, 27607563, 27611612, 27613080, 27613530
27613554, 27615649, 27617978, 27620808, 27623159, 27629756, 27629928
27632114, 27634676, 27634991, 27642235, 27645231, 27657712, 27658186
27666312, 27671633, 27680669, 27686599, 27687880, 27688036, 27688099
27688692, 27691920, 27691939, 27693416, 27693713, 27695063, 27698953
27700466, 27704237, 27709046, 27710072, 27719000, 27726780, 27729678
27739006, 27740424, 27748954, 27751755, 27757567, 27757888, 27758544
27758653, 27758972, 27759077, 27769361, 27779886, 27793533, 27799032
27801337, 27818389, 27819881, 27824540, 27824543, 27825241, 27828794
27828892, 27829295, 27833672, 27834551, 27834569, 27835925, 27839353
27839616, 27846298, 27846499, 27847259, 27850112, 27855490, 27861226
```

```
27873412, 27882176, 27886087, 27897759, 27898015, 27902561, 27908396
27909478, 27927431, 27929287, 27929509, 27931299, 27935493, 27940876
27945870, 27951817, 27952586, 27959048, 27959594, 27964513, 27966472
27967484, 27983174, 27986817, 27994325, 27995215, 27995248, 27997875
27998003, 27999073, 27999638, 28000269, 28019592, 28022101, 28023081
28023399, 28023482, 28024793, 28025414, 28026866, 28033429, 28040776
28043157, 28045903, 28067846, 28071549, 28072383, 28072567, 28073470
28074713, 28079127, 28090453, 28092783, 28098040, 28098160, 28099662
28104176, 28108003, 28111583, 28120036, 28120951, 28124631, 28125601
28125947, 28129791, 28140658, 28157786, 28164480, 28165439, 28171079
28174827, 28180464, 28181021, 28184554, 28188330, 28190796, 28194173
28199085, 28201419, 28204262, 28209985, 28215510, 28218832, 28220398
28223871, 28226179, 28229360, 28236305, 28238264, 28242712, 28250929
28256164, 28271119, 28276054, 28279837, 28281094, 28282606, 28287484
28290434, 28294563, 28302049, 28305001, 28305362, 28305607, 28309406
28319114, 28320399, 28330714, 28330971, 28350595, 28354603, 28357401
28361221, 28365111, 28369092, 28371123, 28373960, 28375383, 28378446
28384353, 28386259, 28388910, 28390273, 28391210, 28396445, 28397317
28401116, 28402823, 28420042, 28420457, 28423598, 28432129, 28434028
28435902, 28437315, 28439086, 28454215, 28454242, 28468312, 28468493
28481149, 28483184, 28489150, 28501075, 28502098, 28502343, 28503038
28507324, 28508053, 28508557, 28512336, 28521330, 28522441, 28528349
28530171, 28535127, 28535272, 28537715, 28538439, 28542455, 28545134
28546290, 28547068, 28547478, 28564479, 28566241, 28571483, 28572407
28572834, 28578164, 28578945, 28585411, 28587723, 28589509, 28600233
28606598, 28608211, 28612674, 28614372, 28617631, 28617959, 28621470
28622202, 28627255, 28636676, 28639299, 28642899, 28678804, 28691965
28692103, 28692275, 28697806, 28703812, 28708023, 28709063, 28710469
28714988, 28715655, 28728272, 28734355, 28740708, 28742555, 28749289
28749724, 28758090, 28758722, 28774416, 28776431, 28777174, 28791725
28797711, 28803345, 28808314, 28817449, 28819640, 28820669, 28821847
28827682, 28830691, 28831971, 28835937, 28836716, 28838066, 28844866
28847136, 28849751, 28852325, 28852691, 28855922, 28856060, 28856172
28863263, 28863487, 28867992, 28887305, 28889730, 28891984, 28905390
28910498, 28915870, 28927452, 28949888, 28951026, 28951382, 28956908
28959493, 28960211, 28965095, 28965787, 28986231, 28986257, 28987439
28991884, 28993295, 28993590, 29002488, 29006527, 29007321, 29007353
29009513, 29013832, 29024054, 29026582, 29027694, 29032276, 29039510
29040739, 29044954, 29048498, 29048728, 29050886, 29060216, 29061016
29115857, 29125374, 29158680, 29163567, 29170232, 29173817, 29179097
29182517, 29182901, 29189889, 29198092, 29200700, 29203604, 29213320
29213893, 29224605, 29237575, 29247712, 29249289, 29250230, 29250317
29254623, 29260956, 29278684, 29296257, 29301463, 29307638, 29312889
29339155, 29343086, 29343156, 29343861, 29347943, 29353821, 29372069
29372460, 29375355, 29375984, 29376346, 29378913, 29379978, 29383695
29388020, 29398488, 29399336, 29405462, 29409149, 29409455, 29420254
29426241, 29434301, 29436454, 29437712, 29450812, 29452251, 29454978
29464779, 29483626, 29483672, 29483723, 29483771, 29500257, 29500963
29501218, 29504682, 29511611, 29524985, 29530515, 29536342, 29538631
29542449, 29542580, 29548592, 29549071, 29559395, 29564592, 29580394
29591343, 29608023, 29614575, 29614987, 29621961, 29625065, 29626154
29629430, 29633753, 29637526, 29637560, 29645349, 29651520, 29656843
29667994, 29676089, 29678163, 29685137, 29687220, 29688867, 29690625
29703195, 29705793, 29707896, 29717901, 29719146, 29724063, 29726695
29766435, 29767177, 29774362, 29782211, 29791152, 29794462, 29807964
29813494, 29815341, 29817278, 29822714, 29825525, 29836659, 29841687
29846645, 29853485, 29865188, 29869404, 29869906, 29875459, 29876358
29881050, 29881575, 29884958, 29893132, 29902299, 29902311, 29914449
29930457, 29944035, 29944660, 29951620, 29951759, 29961353, 29962927
29962939, 29965888, 29991257, 29997937, 30008125, 30018017, 30018903
30031027, 30039959, 30064268, 30068871, 30076253, 30078934, 30086166
30088912, 30092280, 30098251, 30099302, 30114477, 30116203, 30120608
30125995, 30131286, 30139392, 30147928, 30150731, 30160625, 30163243
30164714, 30173113, 30177597, 30179644, 30186706, 30189023, 30193736
30196358, 30200680, 30200758, 30215130, 30218044, 30218317, 30223712
30225443, 30239480, 30241567, 30244787, 30246179, 30247305, 30252098
```

```
30252156, 30253255, 30265523, 30272329, 30281591, 30282501, 30283932
30293345, 30305880, 30312094, 30312568, 30316897, 30325407, 30342878
30352623, 30355490, 30357897, 30364613, 30365745, 30368482, 30372081
30374739, 30381207, 30384121, 30384152, 30391272, 30397100, 30402386
30403763, 30408515, 30413137, 30416034, 30431274, 30441687, 30443393
30453442, 30458593, 30460922, 30464655, 30474774, 30475115, 30476768
30485255, 30496957, 30497057, 30501574, 30503943, 30509277, 30510527
30522998, 30528547, 30528704, 30533198, 30534662, 30581448, 30582500
30613937, 30623138, 30624864, 30635302, 30652853, 30654409, 30668407
30671813, 30681462, 30698289, 30741263, 30758943, 30803210, 30814285
30815852, 30816938, 30855101, 30887501, 30904672, 30922870, 30964194
30968208, 30980615, 30987088, 30998759, 31001455, 31004719, 31013127
31022858, 31100172, 31106577, 31156383, 31172207, 31182793, 31200845
31306261, 31335037, 31335142, 31341859, 31393600
```

Version 12.2.0.1.ru-2020-04.rur-2020-04.r1

La version 12.2.0.1.ru-2020-04.rur-2020-04.r1 comprend ce qui suit :

- Correctif 30886680 : Mise à jour 12.2.0.1.200414 de la version de base de données d'avril 2020
- Correctif 30805580 : Mise à jour 12.2.0.1.200414 de la version d'Oracle JVM
- Correctif 29997937 : DSTv34 pour RDBMS (TZDATA2019G)
- Correctif 29997959 : DSTv34 pour OJVM (TZDATA2019G)
- PreUpgrade Jar : preupgrade_12201_cbuild_23_lf.zip
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS incluse dans CORRECTIF BASE DE DONNÉES 30138470
- Prise en charge de Purge de la corbeille (p. 1129)
- Prise en charge de Génération de rapports de performance avec AWR (Automatic Workload Repository) (p. 1119) utilisant le package `rdsadmin.rdsadmin_diagnostic_util`.

Correctifs combinés pour la version 12.2.0.1.ru-2020-04.rur-2020-04.r1, publiés en avril 2020

Bogues corrigés :

```
30533198, 30312568, 30086166, 28951026, 28435902, 8480838, 8932139
12763598, 13554903, 14221306, 14690846, 15931756, 16002385, 16438495
16727454, 16942578, 17027695, 17533661, 17947871, 18308268, 18521691
18594510, 18774543, 18878420, 19072655, 19211433, 19285025, 19327292
19526548, 19614243, 19647894, 19649997, 19702201, 19721304, 20003668
20087519, 20118035, 20120236, 20324049, 20436508, 20532077, 20549013
20588486, 20591151, 20617383, 20620169, 20736227, 20756305, 20866970
20976443, 21089435, 21095391, 21143725, 21147908, 21159907, 21178363
21186167, 21197098, 21216226, 21320338, 21433452, 21479706, 21517767
21520266, 21547051, 21638600, 21744603, 21788462, 21837606, 21882528
21935698, 21981529, 21985256, 22007324, 22070473, 22070853, 22072543
22087683, 22104866, 22107360, 22174392, 22179537, 22282748, 22310426
22347493, 22363790, 22364044, 22367053, 22379010, 22446455, 22454940
22495673, 22503283, 22503297, 22504793, 22522515, 22530986, 22564336
22568728, 22581771, 22594071, 22599050, 22628825, 22645009, 22645496
22654475, 22700845, 22726044, 22729345, 22826067, 22843979, 22845846
22864303, 22898198, 22921674, 22939829, 22950945, 22970869, 22981722
23018676, 23019710, 23026585, 23035249, 23055900, 23061453, 23065002
23066146, 23080557, 23104033, 23105538, 23109325, 23110523, 23125560
23126545, 23127945, 23143074, 23151677, 23168363, 23169712, 23177923
23179662, 23184263, 23197730, 23234232, 23237091, 23249829, 23271203
```

```
23278750, 23300142, 23306590, 23308065, 23310101, 23312077, 23328639
23333567, 23336559, 23342170, 23481673, 23491861, 23499004, 23499160
23521523, 23527363, 23533647, 23548817, 23567857, 23572982, 23581777
23588722, 23599216, 23600861, 23602213, 23645516, 23665623, 23709062
23715460, 23715518, 23730961, 23733981, 23735292, 23738304, 23741944
23743596, 23746128, 23749454, 23761724, 24006569, 24010030, 24289874
24289895, 24294174, 24303148, 24307571, 24308349, 24326444, 24326846
24328857, 24330708, 24332831, 24334708, 24336249, 24337882, 24341675
24343905, 24345420, 24346821, 24348685, 24350620, 24352981, 24355111
24357348, 24368004, 24371491, 24373528, 24373756, 24374976, 24376875
24376878, 24383086, 24385983, 24401351, 24403922, 24409977, 24415926
24416451, 24421668, 24423416, 24425056, 24425998, 24435982, 24437162
24440648, 24443539, 24457597, 24460392, 24461826, 24467122, 24468470
24470606, 24471079, 24471473, 24473736, 24485034, 24485161, 24485174
24486059, 24486237, 24509056, 24516314, 24530364, 24534401, 24554533
24555417, 24556862, 24556967, 24560906, 24563422, 24570214, 24570598
24573817, 24578718, 24578797, 24588377, 24589081, 24589590, 24591506
24593740, 24595699, 24600330, 24609592, 24609996, 24611527, 24616637
24617969, 24623975, 24624166, 24642495, 24654629, 24655717, 24664211
24668398, 24669189, 24674197, 24674955, 24676172, 24677696, 24680959
24687075, 24689376, 24692973, 24693010, 24693290, 24697323, 24699619
24710696, 24713381, 24714096, 24717183, 24717859, 24718260, 24719799
24735430, 24737064, 24737403, 24737581, 24737954, 24739791, 24744383
24744686, 24752618, 24757934, 24759556, 24760407, 24764085, 24766309
24784414, 24786669, 24791883, 24792678, 24793511, 24796092, 24797119
24800423, 24801152, 24802934, 24808504, 24811725, 24812047, 24818566
24827228, 24827654, 24831514, 24835919, 24841671, 24843188, 24844549
24844841, 24845157, 24848746, 24848923, 24850622, 24907917, 24908321
24911709, 24912588, 24920582, 24921478, 24922704, 24923080, 24923215
24923338, 24923790, 24924667, 24926999, 24929210, 24938784, 24940060
24942749, 24953434, 24957555, 24960044, 24960809, 24965426, 24966594
24966788, 24967993, 24968162, 24976007, 24978100, 25022574, 25027852
25028996, 25029022, 25029423, 25031502, 25032818, 25034396, 25036006
25036474, 25042823, 25044977, 25045228, 25050160, 25051465, 25051628
25054064, 25057811, 25058080, 25060506, 25062592, 25063971, 25065563
25072986, 25077278, 25078611, 25086233, 25087436, 25092777, 25093872
25095982, 25098160, 25099339, 25099497, 25099758, 25100063, 25100579
25103996, 25107662, 25110233, 25114561, 25120284, 25120668, 25120742
25121089, 25123585, 25124363, 25129925, 25130312, 25140197, 25145163
25145215, 25150925, 25159176, 25162645, 25164293, 25166187, 25171041
25171084, 25175723, 25176408, 25178032, 25178101, 25178179, 25179774
25182817, 25184453, 25184555, 25186079, 25191872, 25192044, 25192528
25192729, 25195901, 25199585, 25201454, 25202355, 25203656, 25205954
25206864, 25207410, 25209912, 25210268, 25210499, 25210690, 25211628
25219450, 25223839, 25224242, 25225795, 25226665, 25227381, 25230870
25230945, 25237577, 25240188, 25240590, 25241448, 25241625, 25244807
25248384, 25250109, 25251648, 25257085, 25259611, 25262869, 25263960
25265499, 25269133, 25283790, 25287072, 25293659, 25296876, 25299227
25299807, 25300427, 25303284, 25303756, 25305405, 25307368, 25309116
25313154, 25313411, 25316758, 25317989, 25320555, 25323525, 25328093
25328518, 25329664, 25335249, 25335360, 25335790, 25337332, 25337640
25348956, 25353983, 25356118, 25357142, 25360661, 25362958, 25367588
25367721, 25382812, 25383204, 25384462, 25386748, 25388896, 25392535
25393714, 25395696, 25397936, 25398306, 25404202, 25405100, 25405687
25405813, 25410017, 25410180, 25410802, 25410877, 25411036, 25415713
25416731, 25417050, 25417056, 25417958, 25425005, 25425451, 25425760
25427662, 25429959, 25430120, 25433696, 25435038, 25437699, 25440818
25442559, 25444961, 25445168, 25451531, 25455795, 25457409, 25459958
25462714, 25463844, 25472112, 25472885, 25476125, 25476149, 25477657
25478885, 25479164, 25481087, 25482971, 25486384, 25489342, 25489367
25489607, 25492379, 25498930, 25498994, 25516250, 25524955, 25528838
25530080, 25530814, 25535668, 25536819, 25537470, 25539063, 25540738
25546580, 25546608, 25547901, 25551676, 25553616, 25554787, 25555252
25557886, 25558986, 25560487, 25561296, 25569149, 25570929, 25573623
25575348, 25575369, 25575628, 25579458, 25579761, 25591394, 25594901
25597525, 25598473, 25599425, 25600342, 25600421, 25601999, 25602488
```

```
25603923, 25606091, 25607726, 25612095, 25614866, 25616268, 25616359
25616417, 25616645, 25631933, 25633101, 25634317, 25634348, 25635149
25638456, 25639019, 25643818, 25643889, 25643931, 25646373, 25647325
25648731, 25653109, 25654459, 25654936, 25655390, 25655966, 25659655
25660847, 25661819, 25662088, 25662101, 25662524, 25663488, 25667973
25669791, 25670786, 25671354, 25672640, 25674386, 25680221, 25685152
25686739, 25687460, 25691904, 25694206, 25695903, 25696520, 25699321
25700654, 25709368, 25710420, 25715167, 25717371, 25722055, 25722608
25722720, 25723097, 25723158, 25728085, 25729507, 25730014, 25734963
25736747, 25739065, 25740844, 25741955, 25743479, 25747569, 25749273
25752755, 25754606, 25756945, 25757697, 25757748, 25760195, 25762221
25764020, 25766822, 25768681, 25772669, 25774077, 25775213, 25775444
25780343, 25783447, 25784002, 25785331, 25785441, 25788879, 25789041
25789277, 25789579, 25790353, 25792911, 25795865, 25797092, 25797124
25797305, 25800464, 25802510, 25803364, 25803545, 25807997, 25809524
25810263, 25810704, 25811650, 25812390, 25813931, 25818707, 25822410
25823532, 25823754, 25825910, 25826740, 25830492, 25832935, 25834581
25835365, 25838361, 25838755, 25852885, 25856821, 25858672, 25861398
25865785, 25870579, 25871177, 25871639, 25871753, 25872127, 25872389
25873336, 25874050, 25874678, 25882264, 25883438, 25885148, 25888073
25888984, 25890056, 25890673, 25890782, 25894239, 25895224, 25897615
25898228, 25904273, 25904490, 25905130, 25906117, 25906886, 25908728
25911724, 25914276, 25919622, 25932524, 25932728, 25933494, 25941836
25943271, 25945130, 25947799, 25951571, 25953857, 25954022, 25954054
25957038, 25963024, 25964954, 25967544, 25967985, 25970731, 25971286
25972417, 25973152, 25975723, 25977302, 25980605, 25980770, 25981498
25982666, 25986062, 25990907, 25995938, 25997810, 26006257, 26007010
26019148, 26024732, 26024784, 26025681, 26029075, 26029777, 26029780
26032573, 26034119, 26036748, 26037215, 26038086, 26039623, 26040483
26045732, 26051656, 26078437, 26078493, 26080410, 26083298, 26087754
26088426, 26088836, 26090767, 26090893, 26091640, 26091786, 26095327
26095405, 26096382, 26108080, 26108337, 26110259, 26110632, 26111842
26112621, 26115103, 26121990, 26124078, 26130486, 26137367, 26137416
26138085, 26145560, 26149904, 26153372, 26153977, 26168933, 26169341
26169345, 26170659, 26170715, 26176002, 26187943, 26189861, 26198757
26198926, 26201113, 26203182, 26223039, 26237338, 26237431, 26237773
26238195, 26242031, 26242677, 26243698, 26244115, 26245237, 26248143
26249718, 26256131, 26257953, 26259265, 26261327, 26263328, 26263721
26268756, 26269790, 26271001, 26274660, 26275023, 26275415, 26277439
26281476, 26285062, 26285933, 26308650, 26309047, 26317991, 26318627
26323308, 26324206, 26324769, 26325856, 26327418, 26327624, 26327775
26330994, 26331743, 26333141, 26336977, 26338953, 26351334, 26351996
26353617, 26358670, 26359091, 26362155, 26362821, 26366517, 26367012
26367460, 26371725, 26373967, 26374791, 26375052, 26375250, 26380097
26385189, 26388538, 26396790, 26398675, 26399626, 26399691, 26405036
26406387, 26407408, 26410240, 26412540, 26418088, 26420561, 26421667
26422277, 26423085, 26426526, 26426967, 26430323, 26430737, 26434436
26434999, 26435073, 26436168, 26438612, 26439748, 26440169, 26440749
26442308, 26444601, 26444887, 26446098, 26452606, 26474662, 26474703
26475419, 26476244, 26478970, 26479173, 26482376, 26486365, 26492866
26493289, 26498354, 26513067, 26513709, 26521043, 26522439, 26523432
26526726, 26526799, 26536320, 26537307, 26542135, 26542236, 26542835
26544823, 26545688, 26546070, 26546664, 26546754, 26548363, 26556014
26558437, 26569225, 26575788, 26580633, 26582460, 26584641, 26588069
26597140, 26599395, 26608137, 26608238, 26609942, 26615291, 26615690
26617804, 26623652, 26626879, 26629381, 26633355, 26633558, 26635897
26637273, 26637824, 26639167, 26641610, 26650226, 26650540, 26654363
26658759, 26659182, 26669550, 26680105, 26712331, 26714486, 26714910
26717528, 26724511, 26725687, 26727397, 26729494, 26729611, 26740700
26744595, 26745002, 26751106, 26751171, 26755171, 26758193, 26764561
26765212, 26768025, 26775602, 26784509, 26790923, 26794786, 26797591
26798411, 26798516, 26802503, 26816582, 26820076, 26822314, 26822620
26824833, 26828994, 26829845, 26833932, 26837569, 26837702, 26840654
26844406, 26844870, 26849779, 26871815, 26875822, 26883456, 26895149
26896659, 26898563, 26907236, 26907327, 26908788, 26909100, 26909504
26910716, 26911000, 26939314, 26943004, 26944190, 26958896, 26963310
```

```
26966616, 26966916, 26967713, 26968670, 26969321, 26970175, 26970717
26981902, 26983259, 26985002, 26986173, 26992964, 27000158, 27006120
27006664, 27009164, 27013146, 27028251, 27032785, 27033520, 27033652
27034890, 27036163, 27037839, 27038986, 27039712, 27044169, 27044297
27045634, 27052607, 27056711, 27058530, 27060167, 27060859, 27061736
27072923, 27073314, 27079140, 27084613, 27087426, 27090765, 27092508
27093423, 27097854, 27100800, 27101105, 27105900, 27106179, 27110878
27115422, 27117822, 27119621, 27119861, 27122162, 27124624, 27125872
27133662, 27134734, 27135647, 27135993, 27138325, 27142120, 27142373
27142529, 27144928, 27151826, 27153641, 27160922, 27161071, 27162390
27162405, 27163928, 27165231, 27169796, 27170305, 27181537, 27181897
27185188, 27195935, 27199245, 27200959, 27202015, 27203055, 27207110
27208795, 27213224, 27216046, 27217412, 27223075, 27229389, 27231051
27234962, 27236722, 27242226, 27244337, 27244999, 27248917, 27249531
27250547, 27251690, 27255377, 27256000, 27258578, 27259307, 27262945
27264464, 27266245, 27274456, 27274536, 27275533, 27276231, 27283960
27284499, 27285244, 27288638, 27292213, 27293599, 27302711, 27302730
27303287, 27303938, 27304410, 27304906, 27305039, 27308088, 27314206
27314390, 27314697, 27320576, 27321179, 27329612, 27333106, 27334316
27338912, 27338946, 27339115, 27345231, 27346709, 27348081, 27349393
27350267, 27351628, 27359178, 27364854, 27367194, 27369515, 27370965
27375542, 27381498, 27383281, 27386467, 27393570, 27394703, 27395416
27396624, 27396672, 27396813, 27397048, 27400416, 27400598, 27404573
27404668, 27405645, 27416997, 27423251, 27424405, 27426363, 27432062
27432826, 27433385, 27433870, 27434193, 27439835, 27441326, 27442041
27445727, 27457891, 27459593, 27459948, 27466597, 27468303, 27486805
27487919, 27489107, 27493674, 27494663, 27501373, 27501413, 27502420
27504770, 27505229, 27508985, 27510959, 27525909, 27529661, 27533780
27533819, 27534509, 27540613, 27544973, 27548131, 27554074, 27555481
27558861, 27560602, 27562488, 27565906, 27567477, 27576342, 27576354
27587905, 27588271, 27593501, 27595973, 27601118, 27601441, 27607563
27611612, 27613080, 27613530, 27617978, 27620808, 27623159, 27629756
27632114, 27634676, 27634991, 27645231, 27657712, 27658186, 27666312
27671633, 27680669, 27686599, 27687880, 27688036, 27688099, 27688692
27691920, 27691939, 27693416, 27693713, 27695063, 27698953, 27700466
27704237, 27709046, 27710072, 27719000, 27726780, 27729678, 27739006
27740424, 27748954, 27751755, 27757567, 27757888, 27758544, 27758653
27758972, 27759077, 27769361, 27793533, 27799032, 27801337, 27818389
27819881, 27824540, 27824543, 27825241, 27828794, 27829295, 27833672
27834551, 27834569, 27835925, 27839353, 27846298, 27846499, 27847259
27850112, 27855490, 27861226, 27873412, 27882176, 27886087, 27897759
27898015, 27902561, 27909478, 27927431, 27929287, 27931299, 27935493
27940876, 27945870, 27951817, 27959048, 27959594, 27966472, 27967484
27983174, 27986817, 27994325, 27995215, 27995248, 27997875, 27998003
27999073, 27999638, 28000269, 28022101, 28023081, 28023399, 28023482
28024793, 28025414, 28026866, 28033429, 28040776, 28043157, 28045903
28067846, 28071549, 28072383, 28072567, 28074713, 28079127, 28090453
28098160, 28099662, 28108003, 28111583, 28120036, 28120951, 28124631
28125947, 28129791, 28140658, 28157786, 28164480, 28165439, 28171079
28174827, 28180464, 28181021, 28184554, 28188330, 28190796, 28194173
28199085, 28201419, 28209985, 28215510, 28218832, 28220398, 28223871
28226179, 28229360, 28236305, 28238264, 28242712, 28250929, 28256164
28271119, 28276054, 28279837, 28281094, 28282606, 28290434, 28294563
28302049, 28305001, 28305362, 28309406, 28319114, 28320399, 28330714
28330971, 28354603, 28357401, 28361221, 28365111, 28369092, 28371123
28373960, 28375383, 28378446, 28384353, 28386259, 28388910, 28390273
28391210, 28396445, 28397317, 28401116, 28402823, 28420042, 28420457
28423598, 28432129, 28434028, 28437315, 28439086, 28454215, 28454242
28468312, 28468493, 28481149, 28483184, 28489150, 28501075, 28502343
28503038, 28507324, 28508053, 28508557, 28512336, 28521330, 28522441
28528349, 28530171, 28535127, 28535272, 28537715, 28538439, 28542455
28545134, 28546290, 28547068, 28564479, 28571483, 28572407, 28572834
28578164, 28578945, 28585411, 28587723, 28589509, 28600233, 28608211
28612674, 28617631, 28617959, 28621470, 28622202, 28627255, 28636676
28639299, 28642899, 28678804, 28691965, 28692103, 28692275, 28697806
28708023, 28709063, 28710469, 28714988, 28728272, 28734355, 28740708
```

```
28742555, 28749289, 28749724, 28758090, 28758722, 28774416, 28777174
28791725, 28797711, 28803345, 28817449, 28819640, 28820669, 28821847
28830691, 28831971, 28835937, 28836716, 28838066, 28844866, 28849751
28852691, 28855922, 28856060, 28856172, 28863263, 28863487, 28867992
28887305, 28889730, 28891984, 28927452, 28949888, 28951382, 28956908
28959493, 28960211, 28965095, 28965787, 28986231, 28986257, 28987439
28991884, 28993295, 28993590, 29002488, 29006527, 29007321, 29007353
29009513, 29013832, 29024054, 29026582, 29027694, 29032276, 29040739
29048498, 29050886, 29060216, 29061016, 29115857, 29125374, 29158680
29163567, 29170232, 29173817, 29179097, 29182517, 29182901, 29189889
29198092, 29200700, 29203604, 29213320, 29224605, 29237575, 29247712
29249289, 29250230, 29250317, 29260956, 29278684, 29301463, 29339155
29343086, 29343861, 29347943, 29353821, 29372069, 29372460, 29375355
29375984, 29376346, 29378913, 29379978, 29383695, 29388020, 29398488
29399336, 29405462, 29409149, 29409455, 29426241, 29434301, 29436454
29437712, 29450812, 29452251, 29454978, 29464779, 29483626, 29483672
29483723, 29483771, 29500257, 29500963, 29504682, 29511611, 29524985
29530515, 29536342, 29538631, 29542449, 29542580, 29548592, 29549071
29580394, 29614575, 29621961, 29625065, 29626154, 29629430, 29633753
29637526, 29645349, 29651520, 29656843, 29667994, 29676089, 29678163
29685137, 29687220, 29690625, 29703195, 29707896, 29719146, 29724063
29726695, 29767177, 29782211, 29791152, 29794462, 29807964, 29813494
29817278, 29825525, 29836659, 29841687, 29846645, 29853485, 29865188
29869404, 29875459, 29876358, 29881050, 29884958, 29893132, 29902311
29914449, 29944035, 29944660, 29951620, 29961353, 29962927, 29962939
29991257, 30018017, 30031027, 30064268, 30076253, 30078934, 30088912
30098251, 30099302, 30114477, 30120608, 30125995, 30131286, 30147928
30150731, 30163243, 30164714, 30173113, 30177597, 30179644, 30189023
30196358, 30200758, 30215130, 30218044, 30218317, 30223712, 30239480
30241567, 30244787, 30246179, 30247305, 30252098, 30252156, 30253255
30265523, 30272329, 30281591, 30282501, 30283932, 30305880, 30312094
30342878, 30364613, 30365745, 30374739, 30384152, 30402386, 30403763
30408515, 30413137, 30416034, 30431274, 30441687, 30453442, 30458593
30460922, 30475115, 30485255, 30496957, 30497057, 30501574, 30503943
30509277, 30510527, 30582500, 30613937, 30635302, 30654409, 30671813
30741263, 30803210, 30815852, 30968208, 29997959, 29997937, 28852325
28125601, 27015449, 25881255, 25173124, 24701840, 23614158, 29213893
25811105, 25890046, 26023042, 26570134, 27000702, 27461740, 27952586
27642235, 27539876, 28502098, 28915870, 29254623, 29774362, 30160625
30534662, 30855101
```

Version 12.2.0.1.ru-2020-01.rur-2020-01.r1

La version 12.2.0.1.ru-2020-01.rur-2020-01.r1 comprend ce qui suit :

- Correctif 30593149 : Mise à jour version base de données janvier 2020 : 12.2.0.1.200114
- Correctif 30502018 : MISE À JOUR VERSION OJVM 12.2.0.1.200114
- Correctif 29997937 : DSTv34 pour RDBMS (TZDATA2019G)
- Correctif 29997959 : DSTv34 pour OJVM (TZDATA2019G)
- PreUpgrade Jar : preupgrade_12201_cbuild_23_lf.zip
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS incluse dans CORRECTIF BASE DE DONNÉES 30138470

Mise à jour de version Oracle 12.2.0.1.200114, publiée en janvier 2020

Bogues corrigés :

```
30125995, 8480838, 8932139, 12763598, 13554903, 14221306, 14690846
15931756, 16002385, 16438495, 16727454, 16942578, 17027695, 17533661
17947871, 18308268, 18521691, 18594510, 18774543, 18878420, 19072655
19211433, 19285025, 19327292, 19526548, 19614243, 19647894, 19649997
19702201, 19721304, 20003668, 20087519, 20118035, 20120236, 20324049
20436508, 20532077, 20549013, 20588486, 20591151, 20617383, 20620169
20736227, 20756305, 20866970, 20976443, 21089435, 21095391, 21143725
21147908, 21159907, 21178363, 21186167, 21197098, 21216226, 21320338
21433452, 21479706, 21517767, 21520266, 21547051, 21638600, 21744603
21788462, 21837606, 21882528, 21935698, 21981529, 21985256, 22007324
22070473, 22070853, 22072543, 22087683, 22104866, 22107360, 22174392
22179537, 22282748, 22310426, 22347493, 22363790, 22364044, 22367053
22379010, 22446455, 22454940, 22495673, 22503283, 22503297, 22504793
22522515, 22530986, 22564336, 22568728, 22581771, 22594071, 22599050
22628825, 22645009, 22645496, 22654475, 22700845, 22726044, 22729345
22826067, 22843979, 22845846, 22864303, 22898198, 22921674, 22939829
22950945, 22970869, 22981722, 23019710, 23026585, 23035249, 23055900
23061453, 23065002, 23066146, 23080557, 23104033, 23105538, 23109325
23110523, 23125560, 23126545, 23127945, 23151677, 23169712, 23177923
23179662, 23184263, 23197730, 23234232, 23237091, 23249829, 23271203
23278750, 23300142, 23306590, 23308065, 23310101, 23312077, 23328639
23333567, 23336559, 23342170, 23481673, 23491861, 23499004, 23499160
23521523, 23527363, 23533647, 23548817, 23567857, 23572982, 23581777
23588722, 23599216, 23600861, 23602213, 23645516, 23665623, 23709062
23715460, 23715518, 23730961, 23733981, 23735292, 23738304, 23741944
23743596, 23746128, 23749454, 23761724, 24010030, 24289874, 24294174
24303148, 24307571, 24308349, 24326444, 24326846, 24328857, 24330708
24332831, 24334708, 24336249, 24337882, 24341675, 24343905, 24345420
24346821, 24348685, 24350620, 24352981, 24355111, 24357348, 24368004
24371491, 24373528, 24373756, 24374976, 24376875, 24376878, 24383086
24385983, 24401351, 24403922, 24409977, 24415926, 24416451, 24421668
24423416, 24425056, 24425998, 24435982, 24437162, 24440648, 24443539
24457597, 24460392, 24461826, 24467122, 24468470, 24470606, 24471079
24471473, 24473736, 24485034, 24485161, 24485174, 24486059, 24486237
24509056, 24516314, 24534401, 24554533, 24555417, 24556862, 24556967
24560906, 24563422, 24570214, 24570598, 24573817, 24578718, 24578797
24588377, 24589081, 24589590, 24591506, 24593740, 24595699, 24600330
24609592, 24609996, 24611527, 24616637, 24617969, 24623975, 24624166
24642495, 24654629, 24655717, 24664211, 24668398, 24669189, 24674197
24674955, 24676172, 24677696, 24680959, 24687075, 24689376, 24692973
24693010, 24693290, 24697323, 24699619, 24710696, 24713381, 24714096
24717183, 24717859, 24718260, 24719799, 24735430, 24737064, 24737403
24737581, 24737954, 24739791, 24744383, 24744686, 24752618, 24757934
24759556, 24760407, 24764085, 24766309, 24784414, 24786669, 24792678
24793511, 24796092, 24797119, 24800423, 24801152, 24802934, 24811725
24812047, 24818566, 24827228, 24827654, 24831514, 24835919, 24841671
24843188, 24844549, 24844841, 24845157, 24848746, 24848923, 24850622
24907917, 24908321, 24911709, 24912588, 24921478, 24922704, 24923080
24923215, 24923338, 24923790, 24924667, 24926999, 24929210, 24938784
24940060, 24942749, 24953434, 24957555, 24960044, 24960809, 24965426
24966594, 24966788, 24967993, 24968162, 24976007, 24978100, 25022574
25027852, 25028996, 25029022, 25029423, 25032818, 25034396, 25036006
25036474, 25042823, 25044977, 25045228, 25050160, 25051465, 25051628
25054064, 25057811, 25058080, 25060506, 25062592, 25063971, 25065563
25072986, 25077278, 25078611, 25086233, 25087436, 25092777, 25093872
25095982, 25098160, 25099339, 25099497, 25099758, 25100063, 25100579
25103996, 25107662, 25110233, 25114561, 25120284, 25120668, 25120742
25121089, 25123585, 25124363, 25129925, 25130312, 25140197, 25145163
25145215, 25150925, 25159176, 25162645, 25164293, 25166187, 25171041
25171084, 25175723, 25176408, 25178032, 25178101, 25178179, 25179774
25182817, 25184453, 25184555, 25186079, 25191872, 25192044, 25192528
25192729, 25195901, 25199585, 25201454, 25202355, 25203656, 25205954
25206864, 25207410, 25209912, 25210268, 25210499, 25210690, 25211628
25219450, 25223839, 25224242, 25225795, 25226665, 25227381, 25230870
25230945, 25237577, 25240188, 25240590, 25241448, 25241625, 25244807
25248384, 25250109, 25251648, 25257085, 25259611, 25262869, 25263960
```

```
25265499, 25269133, 25283790, 25287072, 25293659, 25296876, 25299227
25299807, 25300427, 25303284, 25303756, 25305405, 25307368, 25309116
25313154, 25313411, 25316758, 25317989, 25320555, 25323525, 25328518
25329664, 25335249, 25335360, 25335790, 25337332, 25337640, 25348956
25353983, 25356118, 25357142, 25360661, 25362958, 25367588, 25367721
25382812, 25383204, 25384462, 25386748, 25388896, 25392535, 25393714
25395696, 25397936, 25398306, 25404202, 25405100, 25405687, 25405813
25410017, 25410180, 25410802, 25410877, 25411036, 25415713, 25417050
25417056, 25417958, 25425451, 25425760, 25427662, 25429959, 25430120
25433696, 25435038, 25437699, 25440818, 25442559, 25444961, 25445168
25451531, 25455795, 25457409, 25459958, 25462714, 25463844, 25472112
25472885, 25476125, 25476149, 25477657, 25478885, 25479164, 25481087
25482971, 25489342, 25489367, 25489607, 25492379, 25498930, 25498994
25516250, 25524955, 25528838, 25530080, 25530814, 25535668, 25536819
25537470, 25539063, 25540738, 25546580, 25546608, 25547901, 25551676
25553616, 25554787, 25555252, 25557886, 25558986, 25560487, 25561296
25569149, 25570929, 25573623, 25575348, 25575369, 25575628, 25579458
25579761, 25591394, 25594901, 25597525, 25598473, 25599425, 25600342
25600421, 25602488, 25603923, 25606091, 25607726, 25612095, 25614866
25616268, 25616359, 25616417, 25616645, 25631933, 25633101, 25634317
25634348, 25635149, 25638456, 25639019, 25643818, 25643889, 25643931
25646373, 25647325, 25648731, 25653109, 25654459, 25654936, 25655390
25655966, 25659655, 25660847, 25661819, 25662088, 25662101, 25662524
25663488, 25669791, 25670786, 25671354, 25672640, 25674386, 25680221
25685152, 25686739, 25687460, 25691904, 25694206, 25695903, 25696520
25699321, 25700654, 25709368, 25710420, 25715167, 25717371, 25722055
25722608, 25722720, 25723158, 25728085, 25729507, 25730014, 25734963
25736747, 25739065, 25741955, 25743479, 25747569, 25749273, 25752755
25754606, 25756945, 25757748, 25760195, 25762221, 25764020, 25766822
25768681, 25772669, 25774077, 25775213, 25775444, 25780343, 25783447
25784002, 25785331, 25785441, 25788879, 25789041, 25789277, 25789579
25790353, 25792911, 25795865, 25797092, 25797124, 25797305, 25800464
25802510, 25803364, 25803545, 25807997, 25810263, 25810704, 25811650
25812390, 25813931, 25818707, 25822410, 25823754, 25825910, 25826740
25830492, 25832935, 25834581, 25835365, 25838361, 25838755, 25852885
25856821, 25858672, 25861398, 25865785, 25870579, 25871177, 25871639
25871753, 25872127, 25872389, 25873336, 25874050, 25874678, 25882264
25883438, 25885148, 25888073, 25888984, 25890056, 25890673, 25890782
25894239, 25895224, 25897615, 25898228, 25904273, 25904490, 25906117
25906886, 25908728, 25911724, 25914276, 25919622, 25932524, 25932728
25933494, 25941836, 25943271, 25945130, 25947799, 25951571, 25953857
25954022, 25954054, 25957038, 25963024, 25964954, 25967544, 25967985
25970731, 25971286, 25973152, 25975723, 25977302, 25980605, 25980770
25981498, 25982666, 25986062, 25990907, 25995938, 25997810, 26006257
26007010, 26019148, 26024732, 26024784, 26025681, 26029075, 26029777
26029780, 26032573, 26034119, 26036748, 26037215, 26038086, 26039623
26040483, 26045732, 26051656, 26078437, 26078493, 26080410, 26083298
26087754, 26088426, 26088836, 26090767, 26090893, 26091640, 26091786
26095327, 26095405, 26096382, 26108080, 26108337, 26110259, 26110632
26111842, 26112621, 26115103, 26121990, 26124078, 26130486, 26137367
26138085, 26145560, 26149904, 26153372, 26153977, 26168933, 26169341
26169345, 26170659, 26170715, 26176002, 26187943, 26189861, 26198757
26198926, 26201113, 26203182, 26223039, 26237338, 26237431, 26237773
26238195, 26242031, 26242677, 26243698, 26244115, 26245237, 26248143
26249718, 26256131, 26257953, 26259265, 26261327, 26263328, 26263721
26268756, 26269790, 26271001, 26274660, 26275023, 26275415, 26277439
26281476, 26285062, 26285933, 26308650, 26309047, 26317991, 26318627
26323308, 26324206, 26324769, 26325856, 26327418, 26327624, 26327775
26330994, 26331743, 26333141, 26336977, 26338953, 26351334, 26353617
26358670, 26359091, 26362155, 26362821, 26366517, 26367012, 26367460
26371725, 26373967, 26374791, 26375052, 26375250, 26380097, 26385189
26388538, 26396790, 26399626, 26399691, 26405036, 26406387, 26407408
26410240, 26412540, 26418088, 26420561, 26421667, 26422277, 26423085
26426526, 26426967, 26430323, 26430737, 26434436, 26434999, 26435073
26436168, 26438612, 26439748, 26440169, 26440749, 26442308, 26444601
26444887, 26446098, 26452606, 26474662, 26474703, 26475419, 26476244
```

```
26478970, 26479173, 26482376, 26486365, 26492866, 26493289, 26498354
26513067, 26513709, 26521043, 26522439, 26523432, 26526726, 26526799
26536320, 26537307, 26542135, 26542236, 26542835, 26544823, 26545688
26546070, 26546664, 26546754, 26548363, 26556014, 26558437, 26569225
26575788, 26580633, 26582460, 26584641, 26588069, 26597140, 26599395
26608137, 26608238, 26609942, 26615291, 26615690, 26617804, 26623652
26626879, 26629381, 26633355, 26633558, 26635897, 26637273, 26637824
26639167, 26641610, 26650226, 26650540, 26654363, 26658759, 26659182
26669550, 26680105, 26712331, 26714486, 26714910, 26717528, 26724511
26725687, 26727397, 26729494, 26729611, 26740700, 26744595, 26745002
26751106, 26751171, 26755171, 26758193, 26764561, 26765212, 26768025
26775602, 26784509, 26794786, 26797591, 26798411, 26798516, 26802503
26816582, 26820076, 26822620, 26824833, 26828994, 26829845, 26833932
26837702, 26840654, 26844406, 26844870, 26849779, 26871815, 26875822
26883456, 26895149, 26896659, 26898563, 26907236, 26907327, 26908788
26909100, 26909504, 26910716, 26911000, 26939314, 26943004, 26944190
26958896, 26963310, 26966616, 26966916, 26967713, 26968670, 26969321
26970175, 26970717, 26981902, 26983259, 26985002, 26986173, 26992964
27000158, 27006120, 27006664, 27009164, 27013146, 27028251, 27032785
27033520, 27034890, 27036163, 27037839, 27038986, 27039712, 27044169
27044297, 27045634, 27052607, 27056711, 27058530, 27060167, 27060859
27061736, 27072923, 27073314, 27079140, 27087426, 27090765, 27092508
27093423, 27097854, 27101105, 27105900, 27106179, 27110878, 27115422
27117822, 27119621, 27119861, 27122162, 27124624, 27125872, 27133662
27134734, 27135647, 27135993, 27138325, 27142373, 27142529, 27144928
27151826, 27153641, 27160922, 27161071, 27162390, 27162405, 27163928
27165231, 27169796, 27170305, 27181537, 27181897, 27185188, 27195935
27199245, 27200959, 27202015, 27203055, 27207110, 27208795, 27213224
27216046, 27223075, 27229389, 27231051, 27234962, 27236722, 27242226
27244337, 27244999, 27248917, 27249531, 27250547, 27251690, 27255377
27256000, 27258578, 27259307, 27262945, 27264464, 27266245, 27274456
27274536, 27275533, 27276231, 27283960, 27284499, 27285244, 27288638
27292213, 27293599, 27302711, 27302730, 27303287, 27304410, 27304906
27305039, 27308088, 27314206, 27314390, 27320576, 27321179, 27329612
27333106, 27334316, 27338912, 27338946, 27339115, 27345231, 27346709
27348081, 27349393, 27350267, 27351628, 27359178, 27364854, 27367194
27369515, 27370965, 27375542, 27381498, 27383281, 27386467, 27393570
27394703, 27395416, 27396624, 27396672, 27396813, 27397048, 27400416
27400598, 27404668, 27405645, 27416997, 27423251, 27424405, 27426363
27432062, 27432826, 27433385, 27433870, 27434193, 27439835, 27441326
27442041, 27445727, 27457891, 27459948, 27466597, 27468303, 27486805
27489107, 27493674, 27501373, 27501413, 27502420, 27504770, 27505229
27508985, 27510959, 27525909, 27529661, 27533780, 27533819, 27534509
27540613, 27544973, 27548131, 27554074, 27555481, 27558861, 27560602
27562488, 27565906, 27567477, 27576342, 27576354, 27587905, 27588271
27593501, 27595973, 27601118, 27601441, 27607563, 27611612, 27613080
27613530, 27617978, 27620808, 27623159, 27629756, 27632114, 27634676
27634991, 27657712, 27658186, 27666312, 27671633, 27680669, 27686599
27687880, 27688036, 27688099, 27688692, 27691920, 27691939, 27693416
27693713, 27695063, 27698953, 27700466, 27704237, 27709046, 27710072
27726780, 27729678, 27739006, 27740424, 27748954, 27751755, 27757567
27757888, 27758544, 27758653, 27758972, 27759077, 27769361, 27793533
27799032, 27801337, 27818389, 27819881, 27824540, 27824543, 27825241
27828794, 27829295, 27833672, 27834551, 27834569, 27835925, 27839353
27846298, 27846499, 27847259, 27850112, 27855490, 27861226, 27873412
27882176, 27886087, 27897759, 27898015, 27902561, 27909478, 27927431
27929287, 27931299, 27935493, 27940876, 27945870, 27951817, 27959048
27959594, 27966472, 27967484, 27983174, 27986817, 27994325, 27995215
27995248, 27997875, 27998003, 27999073, 27999638, 28000269, 28022101
28023081, 28023399, 28023482, 28026866, 28033429, 28040776, 28043157
28045903, 28067846, 28071549, 28072567, 28074713, 28079127, 28090453
28098160, 28099662, 28108003, 28111583, 28120036, 28120951, 28124631
28125947, 28129791, 28140658, 28164480, 28165439, 28171079, 28174827
28180464, 28181021, 28184554, 28188330, 28190796, 28194173, 28199085
28201419, 28209985, 28215510, 28218832, 28220398, 28223871, 28226179
28229360, 28236305, 28242712, 28256164, 28271119, 28279837, 28281094
```

```
28282606, 28290434, 28294563, 28302049, 28305001, 28305362, 28309406
28319114, 28320399, 28330971, 28354603, 28357401, 28361221, 28365111
28369092, 28371123, 28373960, 28375383, 28378446, 28384353, 28386259
28388910, 28390273, 28391210, 28396445, 28397317, 28401116, 28402823
28420042, 28420457, 28423598, 28432129, 28434028, 28435902, 28437315
28454215, 28454242, 28468312, 28468493, 28481149, 28483184, 28489150
28501075, 28502343, 28507324, 28508053, 28508557, 28512336, 28521330
28522441, 28528349, 28530171, 28535272, 28537715, 28538439, 28542455
28545134, 28546290, 28547068, 28571483, 28572407, 28572834, 28578164
28578945, 28585411, 28587723, 28589509, 28600233, 28612674, 28617631
28617959, 28621470, 28627255, 28636676, 28639299, 28642899, 28678804
28691965, 28692103, 28692275, 28697806, 28708023, 28714988, 28728272
28734355, 28742555, 28749289, 28749724, 28758090, 28758722, 28774416
28777174, 28791725, 28797711, 28803345, 28817449, 28819640, 28820669
28821847, 28830691, 28831971, 28838066, 28844866, 28849751, 28852691
28855922, 28856060, 28856172, 28863487, 28867992, 28887305, 28889730
28891984, 28927452, 28949888, 28951026, 28951382, 28956908, 28959493
28960211, 28965095, 28965787, 28986231, 28986257, 28987439, 28991884
28993590, 29002488, 29006527, 29007353, 29009513, 29013832, 29024054
29027694, 29032276, 29040739, 29050886, 29060216, 29061016, 29115857
29125374, 29158680, 29163567, 29170232, 29173817, 29182901, 29189889
29198092, 29200700, 29213320, 29224605, 29237575, 29250230, 29250317
29260956, 29278684, 29301463, 29339155, 29347943, 29353821, 29372069
29375355, 29375984, 29376346, 29378913, 29379978, 29383695, 29388020
29398488, 29399336, 29405462, 29409149, 29434301, 29436454, 29437712
29450812, 29452251, 29454978, 29464779, 29483626, 29483672, 29483723
29483771, 29500257, 29504682, 29511611, 29530515, 29536342, 29538631
29542449, 29549071, 29626154, 29629430, 29633753, 29637526, 29645349
29651520, 29667994, 29676089, 29678163, 29690625, 29703195, 29707896
29719146, 29724063, 29726695, 29767177, 29782211, 29791152, 29794462
29813494, 29817278, 29825525, 29836659, 29841687, 29846645, 29853485
29865188, 29869404, 29875459, 29884958, 29893132, 29902311, 29914449
29944035, 29944660, 29951620, 29962927, 29962939, 29991257, 30088912
30098251, 30150731, 30164714, 30189023, 30218044, 30223712, 30244787
30252098, 30252156, 30253255, 30281591, 30342878, 30365745, 30402386
30408515, 30453442, 30458593, 30485255
```

Version 12.2.0.1.ru-2019-10.rur-2019-10.r1

La version 12.2.0.1.ru-2019-10.rur-2019-10.r1 comprend ce qui suit :

- Correctif 30138470 : MISE À JOUR VERSION OCT 2019 BASE DE DONNÉES 12.2.0.1.191015
- Correctif 30133625 : MISE À JOUR VERSION OJVM 12.2.0.1.191015
- Correctif 29997937 : DSTv34 pour RDBMS (TZDATA2019G)
- Correctif 29997959 : DSTv34 pour OJVM (TZDATA2019G)
- PreUpgrade Jar : preupgrade_12201_cbuild_23_lf.zip
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS incluse dans CORRECTIF BASE DE DONNÉES 30138470
- Prise en charge de Redimensionnement de l'espace de table temporaire dans un réplica en lecture (p. 1128)

Mise à jour de version Oracle 12.2.0.1.191015, publiée en octobre 2019

Bogues corrigés :

```
29013832, 30244787, 30253255, 8480838, 8932139, 12763598, 13554903
```

```
14221306, 14690846, 15931756, 16002385, 16438495, 16727454, 16942578
17027695, 17533661, 17947871, 18308268, 18521691, 18594510, 18774543
18878420, 19072655, 19211433, 19285025, 19327292, 19526548, 19614243
19647894, 19649997, 19702201, 19721304, 20003668, 20087519, 20118035
20120236, 20324049, 20436508, 20532077, 20588486, 20591151, 20617383
20620169, 20736227, 20756305, 20866970, 20976443, 21089435, 21095391
21143725, 21147908, 21159907, 21178363, 21186167, 21197098, 21216226
21320338, 21433452, 21479706, 21517767, 21520266, 21547051, 21638600
21744603, 21882528, 21935698, 21981529, 21985256, 22007324, 22070473
22070853, 22072543, 22087683, 22104866, 22107360, 22179537, 22310426
22347493, 22364044, 22367053, 22379010, 22446455, 22495673, 22503283
22503297, 22504793, 22522515, 22530986, 22564336, 22568728, 22581771
22594071, 22599050, 22628825, 22645009, 22654475, 22700845, 22726044
22729345, 22826067, 22843979, 22845846, 22864303, 22898198, 22921674
22939829, 22950945, 22970869, 22981722, 23019710, 23026585, 23035249
23055900, 23061453, 23065002, 23066146, 23080557, 23104033, 23105538
23110523, 23125560, 23126545, 23127945, 23151677, 23169712, 23177923
23179662, 23184263, 23197730, 23234232, 23237091, 23249829, 23271203
23278750, 23300142, 23306590, 23310101, 23312077, 23328639, 23336559
23342170, 23481673, 23491861, 23499004, 23499160, 23521523, 23527363
23533647, 23548817, 23567857, 23572982, 23581777, 23588722, 23599216
23600861, 23602213, 23645516, 23665623, 23709062, 23715460, 23715518
23730961, 23733981, 23735292, 23741944, 23743596, 23746128, 23749454
23761724, 24010030, 24289874, 24294174, 24303148, 24307571, 24308349
24326444, 24326846, 24328857, 24332831, 24334708, 24336249, 24337882
24341675, 24343905, 24345420, 24346821, 24348685, 24350620, 24352981
24355111, 24357348, 24368004, 24371491, 24373528, 24373756, 24374976
24376875, 24376878, 24383086, 24385983, 24401351, 24403922, 24409977
24415926, 24416451, 24421668, 24423416, 24425056, 24425998, 24435982
24437162, 24440648, 24443539, 24457597, 24460392, 24461826, 24467122
24468470, 24470606, 24471079, 24471473, 24473736, 24485034, 24485161
24485174, 24486059, 24486237, 24509056, 24534401, 24554533, 24555417
24556967, 24560906, 24563422, 24570214, 24570598, 24573817, 24578718
24578797, 24589081, 24589590, 24591506, 24593740, 24595699, 24600330
24609592, 24609996, 24611527, 24616637, 24617969, 24623975, 24624166
24642495, 24654629, 24655717, 24664211, 24668398, 24669189, 24674197
24674955, 24676172, 24677696, 24680959, 24687075, 24689376, 24692973
24693290, 24697323, 24699619, 24710696, 24713381, 24714096, 24717183
24717859, 24718260, 24719799, 24735430, 24737064, 24737403, 24737581
24737954, 24739791, 24744383, 24744686, 24757934, 24759556, 24760407
24764085, 24766309, 24786669, 24792678, 24793511, 24796092, 24797119
24800423, 24801152, 24802934, 24811725, 24812047, 24818566, 24827228
24827654, 24831514, 24835919, 24841671, 24843188, 24844549, 24844841
24845157, 24848746, 24848923, 24850622, 24907917, 24908321, 24911709
24912588, 24922704, 24923080, 24923215, 24923338, 24923790, 24924667
24926999, 24929210, 24938784, 24940060, 24942749, 24953434, 24957555
24960044, 24965426, 24966594, 24966788, 24967993, 24968162, 24976007
24978100, 25022574, 25027852, 25028996, 25029022, 25029423, 25032818
25034396, 25036006, 25036474, 25042823, 25044977, 25045228, 25050160
25051465, 25051628, 25057811, 25058080, 25060506, 25062592, 25063971
25065563, 25072986, 25078611, 25086233, 25087436, 25092777, 25093872
25095982, 25098160, 25099339, 25099497, 25099758, 25100063, 25100579
25103996, 25107662, 25110233, 25114561, 25120284, 25120668, 25120742
25121089, 25123585, 25124363, 25129925, 25130312, 25140197, 25145163
25145215, 25150925, 25159176, 25162645, 25164293, 25166187, 25171041
25171084, 25175723, 25176408, 25178032, 25178101, 25178179, 25179774
25182817, 25184453, 25184555, 25186079, 25191872, 25192044, 25192528
25192729, 25195901, 25199585, 25201454, 25202355, 25203656, 25206864
25207410, 25209912, 25210268, 25210499, 25211628, 25223839, 25224242
25225795, 25226665, 25227381, 25230870, 25230945, 25237577, 25240188
25240590, 25241448, 25241625, 25244807, 25248384, 25251648, 25257085
25259611, 25262869, 25263960, 25265499, 25283790, 25287072, 25293659
25296876, 25299227, 25299807, 25300427, 25303284, 25303756, 25305405
25307368, 25309116, 25313154, 25313411, 25316758, 25317989, 25320555
25323525, 25328518, 25329664, 25335249, 25335360, 25335790, 25337332
25337640, 25348956, 25353983, 25356118, 25357142, 25360661, 25362958
```

```
25367588, 25367721, 25382812, 25383204, 25384462, 25386748, 25388896
25392535, 25393714, 25395696, 25397936, 25398306, 25404202, 25405100
25405687, 25405813, 25410017, 25410180, 25410802, 25410877, 25411036
25415713, 25417050, 25417056, 25417958, 25425451, 25425760, 25427662
25429959, 25430120, 25433696, 25435038, 25437699, 25440818, 25442559
25444961, 25445168, 25451531, 25455795, 25457409, 25459958, 25462714
25463844, 25472112, 25476149, 25477657, 25478885, 25479164, 25482971
25489342, 25489367, 25489607, 25492379, 25498930, 25498994, 25516250
25524955, 25528838, 25530080, 25530814, 25535668, 25536819, 25537470
25539063, 25540738, 25546580, 25546608, 25547901, 25551676, 25553616
25554787, 25555252, 25557886, 25558986, 25560487, 25561296, 25569149
25570929, 25575348, 25575369, 25575628, 25579458, 25579761, 25594901
25597525, 25598473, 25599425, 25600342, 25600421, 25602488, 25603923
25606091, 25607726, 25612095, 25614866, 25616268, 25616359, 25616417
25616645, 25631933, 25633101, 25634317, 25634348, 25635149, 25638456
25639019, 25643818, 25643889, 25643931, 25646373, 25647325, 25648731
25653109, 25654459, 25654936, 25655390, 25655966, 25659655, 25660847
25661819, 25662088, 25662101, 25662524, 25663488, 25669791, 25670786
25671354, 25672640, 25674386, 25680221, 25685152, 25686739, 25687460
25691904, 25694206, 25695903, 25696520, 25699321, 25700654, 25709368
25710420, 25715167, 25717371, 25722055, 25722608, 25722720, 25723158
25728085, 25729507, 25734963, 25736747, 25739065, 25741955, 25743479
25747569, 25749273, 25752755, 25754606, 25756945, 25757748, 25760195
25762221, 25764020, 25766822, 25768681, 25772669, 25774077, 25775213
25780343, 25783447, 25784002, 25785331, 25785441, 25788879, 25789041
25789277, 25789579, 25790353, 25792911, 25795865, 25797092, 25797124
25797305, 25800464, 25802510, 25803545, 25807997, 25810263, 25810704
25811650, 25813931, 25818707, 25822410, 25823754, 25825910, 25826740
25830492, 25832935, 25834581, 25835365, 25838361, 25838755, 25852885
25856821, 25858672, 25861398, 25865785, 25870579, 25871177, 25871639
25871753, 25872127, 25872389, 25873336, 25874050, 25874678, 25882264
25883438, 25885148, 25888073, 25888984, 25890056, 25890673, 25890782
25894239, 25895224, 25897615, 25904273, 25904490, 25906117, 25906886
25908728, 25911724, 25914276, 25919622, 25932524, 25932728, 25933494
25941836, 25943271, 25945130, 25947799, 25951571, 25953857, 25954022
25954054, 25957038, 25963024, 25964954, 25967544, 25967985, 25970731
25971286, 25973152, 25975723, 25977302, 25980605, 25980770, 25981498
25982666, 25986062, 25990907, 25995938, 25997810, 26006257, 26007010
26019148, 26024732, 26024784, 26025681, 26029075, 26029777, 26029780
26032573, 26034119, 26036748, 26037215, 26038086, 26039623, 26040483
26045732, 26051656, 26078437, 26078493, 26080410, 26083298, 26088426
26088836, 26090767, 26091640, 26091786, 26095327, 26095405, 26096382
26108080, 26108337, 26110259, 26110632, 26111842, 26112621, 26115103
26121990, 26124078, 26130486, 26137367, 26138085, 26149904, 26153372
26153977, 26168933, 26169341, 26169345, 26170659, 26170715, 26176002
26187943, 26189861, 26198757, 26198926, 26201113, 26203182, 26223039
26237338, 26237431, 26237773, 26238195, 26242031, 26242677, 26243698
26244115, 26245237, 26248143, 26249718, 26256131, 26257953, 26259265
26261327, 26263328, 26263721, 26268756, 26269790, 26271001, 26275023
26275415, 26277439, 26281476, 26285062, 26285933, 26308650, 26309047
26317991, 26318627, 26323308, 26324206, 26324769, 26327624, 26330994
26331743, 26333141, 26336977, 26338953, 26351334, 26353617, 26358670
26359091, 26362155, 26362821, 26366517, 26367012, 26367460, 26371725
26374791, 26375052, 26375250, 26380097, 26385189, 26388538, 26396790
26399626, 26399691, 26406387, 26407408, 26412540, 26418088, 26420561
26421667, 26422277, 26423085, 26426526, 26426967, 26430323, 26430737
26434436, 26434999, 26435073, 26436168, 26438612, 26439748, 26440169
26440749, 26442308, 26444601, 26444887, 26446098, 26452606, 26474662
26474703, 26475419, 26476244, 26478970, 26479173, 26482376, 26486365
26492866, 26493289, 26498354, 26513067, 26513709, 26521043, 26522439
26523432, 26526726, 26526799, 26536320, 26537307, 26542135, 26542236
26544823, 26545688, 26546070, 26546664, 26546754, 26548363, 26556014
26558437, 26569225, 26575788, 26580633, 26582460, 26584641, 26597140
26599395, 26608137, 26608238, 26609942, 26615291, 26615690, 26617804
26623652, 26626879, 26629381, 26633355, 26633558, 26635897, 26637273
26637824, 26639167, 26641610, 26650226, 26654363, 26658759, 26659182
```

```
26680105, 26712331, 26714486, 26714910, 26717528, 26724511, 26725687
26727397, 26729494, 26729611, 26740700, 26744595, 26745002, 26751106
26751171, 26755171, 26758193, 26764561, 26765212, 26768025, 26775602
26784509, 26794786, 26797591, 26798411, 26798516, 26802503, 26816582
26820076, 26822620, 26828994, 26829845, 26833932, 26837702, 26840654
26844406, 26844870, 26849779, 26871815, 26875822, 26883456, 26895149
26896659, 26898563, 26907327, 26908788, 26909100, 26909504, 26910716
26911000, 26939314, 26943004, 26944190, 26958896, 26963310, 26966616
26966916, 26967713, 26969321, 26970175, 26970717, 26981902, 26983259
26985002, 26986173, 26992964, 27000158, 27006120, 27006664, 27009164
27013146, 27028251, 27032785, 27033520, 27034890, 27037839, 27038986
27039712, 27044297, 27052607, 27058530, 27060167, 27060859, 27061736
27072923, 27073314, 27079140, 27087426, 27090765, 27092508, 27093423
27097854, 27101105, 27105900, 27106179, 27110878, 27115422, 27117822
27119621, 27122162, 27124624, 27125872, 27133662, 27134734, 27135647
27135993, 27138325, 27142373, 27142529, 27144928, 27151826, 27153641
27160922, 27161071, 27162390, 27162405, 27163928, 27165231, 27169796
27170305, 27181537, 27181897, 27185188, 27199245, 27200959, 27202015
27207110, 27208795, 27213224, 27216046, 27223075, 27229389, 27231051
27236722, 27242226, 27244337, 27248917, 27249531, 27250547, 27251690
27255377, 27256000, 27258578, 27259307, 27262945, 27264464, 27266245
27274456, 27274536, 27275533, 27276231, 27283960, 27284499, 27285244
27288638, 27292213, 27293599, 27302711, 27302730, 27303287, 27304410
27304906, 27305039, 27308088, 27314206, 27314390, 27320576, 27321179
27329612, 27333106, 27334316, 27338912, 27338946, 27339115, 27345231
27346709, 27348081, 27349393, 27350267, 27351628, 27359178, 27364854
27367194, 27369515, 27370965, 27375542, 27381498, 27383281, 27386467
27393570, 27394703, 27395416, 27396624, 27396672, 27396813, 27397048
27400416, 27400598, 27404668, 27405645, 27416997, 27423251, 27424405
27426363, 27432062, 27432826, 27433385, 27433870, 27434193, 27439835
27441326, 27442041, 27445727, 27457891, 27459948, 27466597, 27468303
27493674, 27501373, 27501413, 27502420, 27504770, 27505229, 27508985
27510959, 27525909, 27533780, 27533819, 27534509, 27540613, 27544973
27548131, 27554074, 27555481, 27558861, 27560602, 27562488, 27565906
27567477, 27576342, 27576354, 27588271, 27593501, 27595973, 27601118
27601441, 27607563, 27611612, 27613080, 27613530, 27617978, 27620808
27623159, 27629756, 27632114, 27634676, 27634991, 27658186, 27666312
27671633, 27680669, 27686599, 27687880, 27688036, 27688099, 27688692
27691920, 27691939, 27693416, 27693713, 27695063, 27698953, 27700466
27704237, 27709046, 27710072, 27726780, 27740424, 27748954, 27751755
27757567, 27757888, 27758544, 27758653, 27758972, 27759077, 27793533
27799032, 27801337, 27824540, 27824543, 27825241, 27829295, 27833672
27834551, 27834569, 27835925, 27839353, 27846298, 27846499, 27847259
27850112, 27855490, 27861226, 27873412, 27882176, 27886087, 27898015
27902561, 27931299, 27935493, 27940876, 27945870, 27951817, 27959048
27959594, 27966472, 27967484, 27983174, 27986817, 27994325, 27995215
27995248, 27997875, 27998003, 27999073, 27999638, 28000269, 28022101
28023081, 28023399, 28023482, 28026866, 28033429, 28040776, 28043157
28045903, 28067846, 28072567, 28074713, 28090453, 28099662, 28108003
28111583, 28120036, 28120951, 28124631, 28125947, 28129791, 28140658
28165439, 28171079, 28174827, 28180464, 28181021, 28184554, 28188330
28194173, 28199085, 28201419, 28215510, 28218832, 28220398, 28223871
28226179, 28229360, 28236305, 28242712, 28256164, 28271119, 28279837
28281094, 28282606, 28290434, 28294563, 28302049, 28305001, 28305362
28319114, 28320399, 28354603, 28357401, 28361221, 28365111, 28369092
28371123, 28378446, 28384353, 28390273, 28391210, 28396445, 28401116
28420042, 28420457, 28423598, 28432129, 28434028, 28435902, 28437315
28454242, 28468312, 28481149, 28483184, 28489150, 28501075, 28502343
28507324, 28508053, 28508557, 28521330, 28522441, 28528349, 28535272
28537715, 28542455, 28545134, 28547068, 28571483, 28572834, 28578164
28585411, 28587723, 28600233, 28612674, 28617631, 28617959, 28621470
28627255, 28636676, 28678804, 28691965, 28692103, 28692275, 28697806
28708023, 28714988, 28728272, 28742555, 28749289, 28749724, 28758722
28774416, 28791725, 28803345, 28817449, 28819640, 28820669, 28831971
28849751, 28852691, 28855922, 28856060, 28856172, 28867992, 28889730
28891984, 28951026, 28951382, 28956908, 28960211, 28965787, 28986231
```

```
28987439, 28991884, 28993590, 29002488, 29006527, 29009513, 29024054
29027694, 29032276, 29125374, 29158680, 29163567, 29189889, 29198092
29200700, 29213320, 29224605, 29250230, 29250317, 29301463, 29339155
29347943, 29353821, 29376346, 29378913, 29379978, 29388020, 29405462
29409149, 29436454, 29437712, 29483672, 29483723, 29500257, 29511611
29542449, 29633753, 29637526, 29645349, 29676089, 29690625, 29707896
29724063, 29767177, 29782211, 29813494, 29836659, 29893132, 29902311
30088912, 30189023
```

Version 12.2.0.1.ru-2019-07.rur-2019-07.r1

La version 12.2.0.1.ru-2019-07.rur-2019-07.r1 comprend ce qui suit :

- Correctif 29757449 : MISE À JOUR VERSION JUILLET 2019 BASE DE DONNÉES 12.2.0.1.190716
- Correctif 29774415 : MISE À JOUR VERSION OJVM 12.2.0.1.190716
- Correctif 28125601 : DSTv33 pour RDBMS (TZDATA2018G)
- Correctif 28127287 : DSTv33 pour OJVM (TZDATA2018G)
- PreUpgrade Jar : preupgrade_12201_cbuild_22_lf.zip
- Correctif 29213893 : DBMS_ÉCHEC DES STATS AVEC ERREUR ORA-01422 LORS DU REGROUPEMENT DES STATS POUR LA TABLE UTILIATEUR$
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS

Mise à jour de version Oracle 12.2.0.1.190716, publiée en juillet 2019

Bogues corrigés :

```
8480838, 8932139, 12763598, 13554903, 14221306, 14690846, 15931756
16002385, 16438495, 16727454, 16942578, 17027695, 17533661, 17947871
18308268, 18521691, 18594510, 18774543, 18878420, 19072655, 19211433
19285025, 19327292, 19526548, 19614243, 19647894, 19649997, 19702201
19721304, 20003668, 20087519, 20118035, 20120236, 20324049, 20436508
20532077, 20588486, 20591151, 20617383, 20620169, 20736227, 20756305
20866970, 20976443, 21089435, 21095391, 21143725, 21147908, 21159907
21178363, 21186167, 21197098, 21216226, 21320338, 21433452, 21479706
21517767, 21520266, 21547051, 21638600, 21744603, 21882528, 21981529
21985256, 22007324, 22070473, 22070853, 22072543, 22087683, 22104866
22179537, 22310426, 22347493, 22364044, 22367053, 22379010, 22446455
22495673, 22503283, 22503297, 22504793, 22522515, 22530986, 22564336
22568728, 22581771, 22594071, 22599050, 22628825, 22645009, 22654475
22700845, 22726044, 22729345, 22826067, 22843979, 22845846, 22864303
22898198, 22950945, 22970869, 22981722, 23019710, 23026585, 23035249
23055900, 23061453, 23065002, 23066146, 23080557, 23104033, 23105538
23110523, 23125560, 23126545, 23127945, 23151677, 23169712, 23177923
23179662, 23184263, 23197730, 23234232, 23237091, 23249829, 23271203
23278750, 23300142, 23306590, 23310101, 23312077, 23328639, 23336559
23481673, 23491861, 23499004, 23499160, 23521523, 23527363, 23533647
23548817, 23567857, 23572982, 23581777, 23588722, 23599216, 23600861
23602213, 23645516, 23665623, 23709062, 23715460, 23715518, 23730961
23733981, 23735292, 23741944, 23746128, 23749454, 23761724, 24010030
24289874, 24294174, 24303148, 24307571, 24308349, 24326444, 24326846
24328857, 24332831, 24334708, 24336249, 24337882, 24341675, 24343905
24345420, 24346821, 24348685, 24350620, 24352981, 24355111, 24357348
24368004, 24371491, 24373528, 24373756, 24374976, 24376875, 24376878
24385983, 24401351, 24403922, 24409977, 24415926, 24416451, 24421668
24423416, 24425056, 24425998, 24435982, 24437162, 24443539, 24457597
24460392, 24461826, 24467122, 24468470, 24470606, 24471079, 24471473
```

```
24473736, 24485034, 24485161, 24485174, 24486059, 24486237, 24509056
24534401, 24554533, 24555417, 24556967, 24560906, 24563422, 24570214
24570598, 24573817, 24578718, 24578797, 24589081, 24589590, 24591506
24593740, 24595699, 24600330, 24609592, 24609996, 24611527, 24616637
24617969, 24623975, 24624166, 24642495, 24654629, 24655717, 24664211
24668398, 24669189, 24674197, 24674955, 24676172, 24677696, 24680959
24689376, 24692973, 24693290, 24697323, 24699619, 24710696, 24713381
24714096, 24717183, 24717859, 24718260, 24719799, 24735430, 24737064
24737403, 24737581, 24744383, 24744686, 24757934, 24759556, 24760407
24764085, 24766309, 24786669, 24792678, 24793511, 24796092, 24797119
24800423, 24801152, 24802934, 24811725, 24812047, 24827228, 24827654
24831514, 24835919, 24841671, 24843188, 24844549, 24844841, 24845157
24848746, 24848923, 24850622, 24907917, 24908321, 24911709, 24912588
24922704, 24923080, 24923215, 24923338, 24923790, 24924667, 24926999
24929210, 24938784, 24940060, 24942749, 24953434, 24957555, 24960044
24965426, 24966594, 24966788, 24967993, 24968162, 24976007, 24978100
25022574, 25027852, 25028996, 25029022, 25029423, 25032818, 25034396
25036474, 25042823, 25044977, 25045228, 25050160, 25051465, 25051628
25057811, 25058080, 25062592, 25063971, 25065563, 25072986, 25078611
25086233, 25087436, 25092777, 25093872, 25098160, 25099339, 25099497
25099758, 25100063, 25100579, 25103996, 25107662, 25110233, 25114561
25120284, 25120668, 25120742, 25121089, 25123585, 25124363, 25129925
25140197, 25145163, 25145215, 25150925, 25159176, 25162645, 25164293
25166187, 25171041, 25171084, 25175723, 25176408, 25178032, 25178101
25178179, 25179774, 25182817, 25184555, 25186079, 25191872, 25192044
25192528, 25192729, 25199585, 25201454, 25202355, 25203656, 25206864
25207410, 25209912, 25210268, 25210499, 25211628, 25223839, 25224242
25225795, 25226665, 25227381, 25230870, 25230945, 25237577, 25240188
25240590, 25241448, 25241625, 25244807, 25248384, 25251648, 25257085
25259611, 25262869, 25263960, 25265499, 25283790, 25287072, 25293659
25296876, 25299227, 25299807, 25300427, 25303756, 25305405, 25307368
25309116, 25313154, 25313411, 25316758, 25317989, 25320555, 25323525
25328518, 25329664, 25335249, 25335360, 25335790, 25337332, 25337640
25348956, 25353983, 25356118, 25357142, 25360661, 25362958, 25367588
25367721, 25382812, 25383204, 25384462, 25386748, 25388896, 25392535
25395696, 25397936, 25398306, 25404202, 25405100, 25405687, 25405813
25410017, 25410180, 25410802, 25410877, 25411036, 25415713, 25417050
25417056, 25417958, 25425451, 25425760, 25427662, 25429959, 25430120
25433696, 25435038, 25437699, 25440818, 25442559, 25444961, 25445168
25451531, 25455795, 25457409, 25459958, 25462714, 25463844, 25472112
25476149, 25477657, 25478885, 25479164, 25482971, 25489342, 25489367
25489607, 25492379, 25498930, 25498994, 25516250, 25524955, 25528838
25530080, 25530814, 25535668, 25536819, 25537470, 25539063, 25540738
25546580, 25546608, 25547901, 25551676, 25553616, 25554787, 25555252
25557886, 25558986, 25560487, 25561296, 25569149, 25570929, 25575348
25575369, 25575628, 25579458, 25579761, 25594901, 25597525, 25598473
25599425, 25600342, 25600421, 25602488, 25603923, 25606091, 25607726
25612095, 25614866, 25616268, 25616359, 25616417, 25616645, 25631933
25633101, 25634317, 25634348, 25635149, 25638456, 25639019, 25643818
25643889, 25643931, 25646373, 25647325, 25648731, 25653109, 25654459
25654936, 25655390, 25655966, 25659655, 25660847, 25661819, 25662088
25662101, 25662524, 25663488, 25669791, 25670786, 25671354, 25672640
25674386, 25680221, 25685152, 25686739, 25687460, 25691904, 25694206
25695903, 25699321, 25700654, 25709368, 25710420, 25715167, 25717371
25722055, 25722608, 25722720, 25723158, 25728085, 25729507, 25734963
25736747, 25739065, 25741955, 25743479, 25747569, 25749273, 25752755
25754606, 25757748, 25760195, 25762221, 25764020, 25766822, 25768681
25772669, 25774077, 25775213, 25780343, 25783447, 25784002, 25785331
25785441, 25788879, 25789041, 25789277, 25789579, 25790353, 25792911
25795865, 25797092, 25797124, 25797305, 25800464, 25802510, 25803545
25807997, 25810263, 25810704, 25811650, 25813931, 25818707, 25822410
25823754, 25825910, 25826740, 25830492, 25832935, 25834581, 25835365
25838361, 25838755, 25852885, 25856821, 25858672, 25861398, 25865785
25870579, 25871177, 25871639, 25871753, 25872127, 25872389, 25873336
25874050, 25874678, 25882264, 25883438, 25885148, 25888073, 25888984
25890056, 25890673, 25894239, 25895224, 25897615, 25904273, 25904490
```

```
25906117, 25906886, 25908728, 25911724, 25914276, 25919622, 25932524
25932728, 25933494, 25941836, 25943271, 25945130, 25947799, 25951571
25953857, 25954022, 25954054, 25957038, 25963024, 25964954, 25967544
25967985, 25970731, 25971286, 25973152, 25975723, 25977302, 25980605
25980770, 25981498, 25982666, 25986062, 25990907, 25995938, 25997810
26006257, 26007010, 26019148, 26024732, 26024784, 26025681, 26029075
26029777, 26029780, 26032573, 26034119, 26036748, 26037215, 26038086
26039623, 26040483, 26045732, 26051656, 26078437, 26078493, 26080410
26083298, 26088426, 26088836, 26090767, 26091640, 26091786, 26095327
26095405, 26096382, 26108080, 26108337, 26110259, 26110632, 26111842
26112621, 26115103, 26121990, 26124078, 26137367, 26138085, 26149904
26153977, 26168933, 26169341, 26169345, 26170659, 26170715, 26176002
26187943, 26189861, 26198757, 26198926, 26201113, 26203182, 26223039
26237338, 26237431, 26237773, 26238195, 26242031, 26243698, 26244115
26245237, 26248143, 26249718, 26256131, 26257953, 26259265, 26261327
26263328, 26263721, 26268756, 26269790, 26271001, 26275023, 26275415
26277439, 26281476, 26285062, 26285933, 26308650, 26309047, 26317991
26318627, 26323308, 26324206, 26324769, 26327624, 26330994, 26331743
26333141, 26336977, 26338953, 26351334, 26353617, 26358670, 26359091
26362155, 26362821, 26366517, 26367012, 26367460, 26371725, 26374791
26375052, 26375250, 26380097, 26385189, 26388538, 26396790, 26399626
26399691, 26406387, 26407408, 26412540, 26418088, 26420561, 26421667
26422277, 26423085, 26426526, 26426967, 26430323, 26430737, 26434436
26434999, 26435073, 26436168, 26438612, 26439748, 26440169, 26440749
26442308, 26444601, 26444887, 26446098, 26452606, 26474662, 26474703
26475419, 26476244, 26478970, 26479173, 26482376, 26486365, 26492866
26493289, 26498354, 26513067, 26513709, 26521043, 26522439, 26523432
26526726, 26526799, 26536320, 26537307, 26542135, 26542236, 26544823
26545688, 26546070, 26546664, 26546754, 26548363, 26556014, 26569225
26575788, 26580633, 26582460, 26584641, 26597140, 26599395, 26608137
26608238, 26609942, 26615291, 26615690, 26617804, 26623652, 26626879
26629381, 26633355, 26633558, 26635897, 26637273, 26637824, 26639167
26641610, 26650226, 26654363, 26658759, 26659182, 26680105, 26712331
26714486, 26714910, 26717528, 26725687, 26727397, 26729494, 26729611
26740700, 26744595, 26745002, 26751106, 26751171, 26755171, 26758193
26764561, 26765212, 26775602, 26784509, 26794786, 26797591, 26798516
26802503, 26816582, 26820076, 26822620, 26828994, 26829845, 26833932
26837702, 26840654, 26844406, 26844870, 26849779, 26875822, 26883456
26895149, 26896659, 26898563, 26907327, 26908788, 26909100, 26909504
26911000, 26939314, 26943004, 26944190, 26958896, 26963310, 26966616
26966916, 26967713, 26969321, 26970175, 26970717, 26981902, 26983259
26985002, 26986173, 26992964, 27006120, 27006664, 27009164, 27013146
27028251, 27032785, 27034890, 27037839, 27038986, 27039712, 27044297
27052607, 27058530, 27060167, 27060859, 27061736, 27073314, 27079140
27087426, 27090765, 27092508, 27093423, 27097854, 27101105, 27105900
27106179, 27110878, 27115422, 27117822, 27119621, 27122162, 27124624
27125872, 27133662, 27134734, 27135647, 27135993, 27138325, 27142373
27142529, 27151826, 27153641, 27161071, 27162390, 27162405, 27163928
27165231, 27169796, 27170305, 27181537, 27181897, 27199245, 27200959
27207110, 27208795, 27213224, 27216046, 27223075, 27229389, 27231051
27236722, 27242226, 27244337, 27248917, 27249531, 27250547, 27251690
27255377, 27256000, 27258578, 27259307, 27262945, 27266245, 27274456
27274536, 27275533, 27276231, 27283960, 27284499, 27285244, 27288638
27292213, 27293599, 27302711, 27302730, 27303287, 27304410, 27305039
27308088, 27314206, 27314390, 27320576, 27321179, 27329612, 27333106
27334316, 27338912, 27338946, 27339115, 27345231, 27346709, 27348081
27349393, 27350267, 27351628, 27359178, 27364854, 27367194, 27370965
27375542, 27381498, 27386467, 27394703, 27395416, 27396624, 27396672
27396813, 27397048, 27400416, 27400598, 27404668, 27405645, 27416997
27423251, 27424405, 27426363, 27432062, 27433870, 27434193, 27439835
27441326, 27442041, 27445727, 27457891, 27466597, 27468303, 27493674
27501373, 27501413, 27502420, 27504770, 27505229, 27508985, 27510959
27525909, 27533819, 27534509, 27540613, 27544973, 27548131, 27554074
27555481, 27558861, 27560602, 27562488, 27565906, 27567477, 27576342
27593501, 27595973, 27607563, 27611612, 27613080, 27613530, 27617978
27620808, 27629756, 27634676, 27634991, 27658186, 27666312, 27671633
```

```
27680669, 27686599, 27687880, 27688036, 27688099, 27688692, 27691920
27691939, 27693416, 27693713, 27695063, 27698953, 27700466, 27704237
27709046, 27710072, 27726780, 27740424, 27748954, 27751755, 27757567
27757888, 27758972, 27759077, 27793533, 27799032, 27801337, 27824540
27824543, 27825241, 27829295, 27833672, 27834551, 27835925, 27846298
27846499, 27847259, 27855490, 27861226, 27882176, 27898015, 27931299
27940876, 27945870, 27951817, 27959048, 27959594, 27966472, 27986817
27994325, 27995215, 27995248, 27997875, 27998003, 27999073, 27999638
28000269, 28022101, 28023081, 28023399, 28023482, 28026866, 28033429
28040776, 28045903, 28067846, 28072567, 28074713, 28090453, 28099662
28108003, 28111583, 28120036, 28120951, 28124631, 28129791, 28140658
28165439, 28171079, 28174827, 28180464, 28181021, 28184554, 28188330
28194173, 28199085, 28201419, 28218832, 28220398, 28223871, 28226179
28229360, 28236305, 28271119, 28279837, 28282606, 28290434, 28302049
28305001, 28305362, 28320399, 28354603, 28357401, 28361221, 28365111
28378446, 28390273, 28396445, 28420042, 28420457, 28423598, 28432129
28434028, 28437315, 28454242, 28468312, 28483184, 28489150, 28501075
28502343, 28507324, 28508053, 28508557, 28522441, 28528349, 28535272
28545134, 28547068, 28571483, 28572834, 28578164, 28587723, 28600233
28612674, 28617631, 28617959, 28621470, 28627255, 28636676, 28691965
28692275, 28708023, 28728272, 28742555, 28749289, 28758722, 28774416
28803345, 28819640, 28849751, 28852691, 28856060, 28891984, 28951382
28956908, 28960211, 28965787, 28986231, 28987439, 28991884, 28993590
29006527, 29024054, 29027694, 29032276, 29125374, 29158680, 29189889
29200700, 29224605, 29250230, 29301463, 29339155, 29347943, 29376346
29378913, 29379978, 29388020, 29405462, 29436454, 29437712, 29511611
29542449, 29676089, 29690625, 29813494, 29836659
```

Version 12.2.0.1.ru-2019-04.rur-2019-04.r1

La version 12.2.0.1.ru-2019-04.rur-2019-04.r1 comprend ce qui suit :

- Correctif 29314339 : Mise à jour version base de données avril 2019 : 12.2.0.1.190416
- Correctif 29249637 : MISE À JOUR VERSION OJVM : 12.2.0.1.190416
- Correctif 28852325 : DSTv33 pour RDBMS (TZDATA2018G)
- Correctif 28852334 : DSTv33 pour OJVM (TZDATA2018G)
- PreUpgrade Jar : preupgrade_12201_cbuild_21_lf.zip
- Correctif 28423598 : L'AUTHENTIFICATION GOLDENGATE EMPÊCHE L'UTILISATION DE DG ACTIF JUSQU'AU REBOND
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS
- Prise en charge du package `rdsadmin_dbms_goldengate_auth`, qui fournit à `GRANT` les privilèges requis par un compte administrateur GoldenGate (voir Accorder des privilèges de compte sur la base de données source (p. 1195))

Mise à jour de version Oracle 12.2.0.1.190416, publiée en avril 2019

Bogues corrigés :

```
26362155, 28023399, 25741955, 25873336, 26966616, 27097854, 28617631
28742555, 29006527, 8480838, 8932139, 12763598, 13554903, 14221306
14690846, 15931756, 16002385, 16438495, 16727454, 16942578, 17027695
17533661, 17947871, 18308268, 18521691, 18594510, 18774543, 18878420
19072655, 19211433, 19285025, 19327292, 19526548, 19614243, 19647894
19649997, 19702201, 19721304, 20003668, 20087519, 20118035, 20120236
20324049, 20436508, 20532077, 20591151, 20617383, 20620169, 20736227
```

```
20756305, 20866970, 20976443, 21089435, 21095391, 21143725, 21147908
21159907, 21178363, 21186167, 21197098, 21216226, 21320338, 21433452
21479706, 21520266, 21547051, 21638600, 21744603, 21882528, 21981529
21985256, 22007324, 22070853, 22072543, 22087683, 22104866, 22179537
22347493, 22364044, 22367053, 22379010, 22446455, 22495673, 22503283
22503297, 22504793, 22530986, 22564336, 22568728, 22581771, 22594071
22599050, 22628825, 22645009, 22654475, 22700845, 22726044, 22729345
22826067, 22843979, 22845846, 22864303, 22898198, 22950945, 22970869
22981722, 23019710, 23026585, 23035249, 23055900, 23061453, 23065002
23066146, 23080557, 23104033, 23105538, 23110523, 23125560, 23126545
23127945, 23151677, 23179662, 23184263, 23197730, 23234232, 23237091
23249829, 23271203, 23278750, 23300142, 23310101, 23312077, 23328639
23336559, 23481673, 23491861, 23499004, 23499160, 23521523, 23527363
23533647, 23548817, 23567857, 23572982, 23581777, 23588722, 23599216
23600861, 23602213, 23645516, 23665623, 23709062, 23715460, 23715518
23730961, 23733981, 23735292, 23741944, 23746128, 23749454, 23761724
24010030, 24289874, 24294174, 24303148, 24307571, 24308349, 24326444
24326846, 24328857, 24332831, 24334708, 24336249, 24337882, 24341675
24343905, 24345420, 24346821, 24348685, 24350620, 24352981, 24368004
24371491, 24373756, 24374976, 24376875, 24376878, 24385983, 24401351
24403922, 24415926, 24421668, 24423416, 24425056, 24425998, 24435982
24437162, 24443539, 24457597, 24460392, 24461826, 24467122, 24468470
24470606, 24471473, 24473736, 24485034, 24485161, 24485174, 24486059
24486237, 24509056, 24534401, 24554533, 24555417, 24556967, 24560906
24563422, 24570214, 24570598, 24573817, 24578718, 24578797, 24589081
24589590, 24593740, 24595699, 24600330, 24609592, 24609996, 24611527
24616637, 24617969, 24623975, 24624166, 24642495, 24654629, 24655717
24664211, 24668398, 24669189, 24674197, 24674955, 24676172, 24677696
24680959, 24689376, 24692973, 24693290, 24697323, 24699619, 24710696
24713381, 24714096, 24717183, 24717859, 24718260, 24719799, 24735430
24737064, 24737403, 24737581, 24744383, 24744686, 24757934, 24759556
24760407, 24764085, 24766309, 24786669, 24792678, 24793511, 24796092
24797119, 24800423, 24801152, 24802934, 24811725, 24812047, 24827228
24827654, 24831514, 24835919, 24843188, 24844549, 24845157, 24848746
24848923, 24850622, 24907917, 24908321, 24911709, 24912588, 24922704
24923080, 24923215, 24923338, 24923790, 24924667, 24926999, 24929210
24938784, 24940060, 24942749, 24953434, 24957555, 24960044, 24966594
24966788, 24968162, 24976007, 24978100, 25022574, 25027852, 25028996
25029022, 25029423, 25032818, 25034396, 25036474, 25042823, 25044977
25045228, 25050160, 25051628, 25057811, 25058080, 25062592, 25063971
25065563, 25072986, 25078611, 25086233, 25087436, 25093872, 25098160
25099339, 25099497, 25099758, 25100063, 25100579, 25103996, 25107662
25110233, 25114561, 25120284, 25120668, 25120742, 25121089, 25123585
25124363, 25129925, 25140197, 25145163, 25145215, 25150925, 25159176
25162645, 25164293, 25166187, 25171084, 25175723, 25176408, 25178032
25178101, 25178179, 25179774, 25182817, 25184555, 25186079, 25191872
25192044, 25192729, 25199585, 25201454, 25202355, 25203656, 25206864
25207410, 25209912, 25210268, 25210499, 25211628, 25223839, 25224242
25225795, 25226665, 25227381, 25230870, 25230945, 25237577, 25240188
25240590, 25241448, 25241625, 25244807, 25248384, 25251648, 25257085
25259611, 25262869, 25263960, 25265499, 25283790, 25287072, 25293659
25296876, 25299227, 25299807, 25300427, 25303756, 25305405, 25307368
25309116, 25313154, 25313411, 25316758, 25317989, 25320555, 25323525
25328518, 25329664, 25335249, 25335360, 25335790, 25337332, 25337640
25348956, 25353983, 25356118, 25357142, 25362958, 25367588, 25367721
25382812, 25383204, 25384462, 25386748, 25388896, 25392535, 25395696
25397936, 25398306, 25404202, 25405100, 25405687, 25405813, 25410017
25410180, 25410802, 25410877, 25411036, 25417050, 25417056, 25417958
25425451, 25425760, 25427662, 25429959, 25430120, 25433696, 25435038
25437699, 25440818, 25442559, 25444961, 25445168, 25451531, 25455795
25457409, 25459958, 25462714, 25463844, 25472112, 25476149, 25477657
25478885, 25479164, 25489342, 25489367, 25489607, 25492379, 25498930
25498994, 25516250, 25524955, 25528838, 25530080, 25530814, 25535668
25536819, 25537470, 25539063, 25540738, 25546580, 25546608, 25547901
25551676, 25553616, 25554787, 25555252, 25557886, 25558986, 25560487
25561296, 25569149, 25570929, 25575348, 25575628, 25579458, 25579761
```

```
25594901, 25597525, 25598473, 25599425, 25600342, 25600421, 25602488
25603923, 25606091, 25607726, 25612095, 25614866, 25616268, 25616359
25616417, 25616645, 25631933, 25633101, 25634317, 25634348, 25635149
25638456, 25639019, 25643818, 25643931, 25646373, 25647325, 25648731
25653109, 25654459, 25654936, 25655390, 25655966, 25659655, 25660847
25661819, 25662088, 25662101, 25662524, 25663488, 25669791, 25670786
25671354, 25672640, 25674386, 25680221, 25685152, 25686739, 25687460
25691904, 25694206, 25695903, 25700654, 25710420, 25715167, 25717371
25722055, 25722608, 25722720, 25728085, 25729507, 25734963, 25736747
25739065, 25743479, 25754606, 25757748, 25760195, 25762221, 25764020
25766822, 25768681, 25772669, 25774077, 25775213, 25780343, 25783447
25784002, 25785331, 25785441, 25788879, 25789041, 25789277, 25789579
25790353, 25795865, 25797092, 25797124, 25797305, 25800464, 25802510
25803545, 25807997, 25810704, 25813931, 25818707, 25822410, 25823754
25825910, 25826740, 25830492, 25832935, 25834581, 25838361, 25852885
25856821, 25858672, 25861398, 25865785, 25870579, 25871177, 25871639
25871753, 25872127, 25872389, 25874050, 25874678, 25882264, 25883438
25885148, 25888073, 25890056, 25890673, 25894239, 25895224, 25897615
25904273, 25904490, 25906117, 25908728, 25911724, 25914276, 25919622
25932524, 25932728, 25933494, 25941836, 25943271, 25945130, 25947799
25953857, 25954022, 25954054, 25957038, 25963024, 25964954, 25967544
25967985, 25970731, 25971286, 25973152, 25975723, 25977302, 25980605
25980770, 25981498, 25982666, 25986062, 25990907, 25995938, 26006257
26007010, 26019148, 26024732, 26025681, 26029075, 26029777, 26029780
26032573, 26034119, 26036748, 26037215, 26038086, 26039623, 26040483
26045732, 26051656, 26078437, 26078493, 26080410, 26083298, 26088426
26088836, 26090767, 26091640, 26091786, 26095327, 26095405, 26096382
26108080, 26108337, 26110259, 26110632, 26111842, 26112621, 26115103
26121990, 26124078, 26137367, 26138085, 26149904, 26153977, 26169341
26169345, 26170715, 26176002, 26187943, 26189861, 26198757, 26198926
26201113, 26203182, 26223039, 26237431, 26237773, 26238195, 26242031
26243698, 26244115, 26245237, 26248143, 26249718, 26256131, 26259265
26261327, 26263328, 26263721, 26269790, 26271001, 26277439, 26285062
26285933, 26308650, 26309047, 26318627, 26323308, 26324206, 26324769
26327624, 26330994, 26331743, 26333141, 26336977, 26338953, 26351334
26353617, 26358670, 26359091, 26362821, 26366517, 26367012, 26367460
26371725, 26374791, 26375250, 26380097, 26385189, 26388538, 26396790
26399626, 26399691, 26406387, 26407408, 26412540, 26418088, 26420561
26421667, 26422277, 26423085, 26426526, 26426967, 26430323, 26430737
26434436, 26434999, 26435073, 26436168, 26438612, 26439748, 26440169
26440749, 26442308, 26444601, 26444887, 26446098, 26452606, 26474703
26475419, 26476244, 26478970, 26479173, 26486365, 26492866, 26493289
26498354, 26513709, 26521043, 26522439, 26523432, 26526726, 26526799
26536320, 26537307, 26542135, 26544823, 26545688, 26546070, 26546664
26546754, 26548363, 26556014, 26569225, 26575788, 26580633, 26582460
26584641, 26597140, 26599395, 26608137, 26608238, 26609942, 26615291
26615690, 26617804, 26623652, 26626879, 26629381, 26633355, 26633558
26635897, 26637273, 26637824, 26639167, 26641610, 26650226, 26654363
26658759, 26659182, 26680105, 26712331, 26714486, 26714910, 26717528
26725687, 26727397, 26729494, 26729611, 26740700, 26744595, 26745002
26751106, 26751171, 26755171, 26758193, 26764561, 26765212, 26775602
26784509, 26794786, 26797591, 26798516, 26802503, 26816582, 26820076
26822620, 26828994, 26829845, 26833932, 26837702, 26840654, 26844406
26844870, 26849779, 26875822, 26883456, 26895149, 26896659, 26898563
26907327, 26908788, 26909100, 26909504, 26911000, 26939314, 26944190
26958896, 26963310, 26966916, 26967713, 26969321, 26970175, 26970717
26981902, 26983259, 26986173, 26992964, 27006120, 27006664, 27009164
27013146, 27028251, 27034890, 27037839, 27038986, 27039712, 27044297
27052607, 27058530, 27060167, 27060859, 27061736, 27073314, 27079140
27087426, 27090765, 27093423, 27106179, 27110878, 27115422, 27117822
27119621, 27122162, 27124624, 27125872, 27133662, 27135647, 27135993
27138325, 27142373, 27142529, 27151826, 27153641, 27161071, 27162390
27162405, 27163928, 27165231, 27169796, 27170305, 27181537, 27181897
27199245, 27200959, 27207110, 27208795, 27213224, 27216046, 27223075
27229389, 27231051, 27236722, 27242226, 27244337, 27248917, 27250547
27251690, 27255377, 27256000, 27258578, 27259307, 27262945, 27266245
```

```
27274456, 27274536, 27275533, 27276231, 27283960, 27284499, 27285244
27288638, 27292213, 27293599, 27302711, 27302730, 27304410, 27305039
27314206, 27314390, 27320576, 27321179, 27329612, 27333106, 27334316
27338912, 27338946, 27339115, 27345231, 27346709, 27348081, 27349393
27350267, 27351628, 27359178, 27364854, 27367194, 27370965, 27375542
27381498, 27386467, 27394703, 27395416, 27396624, 27396672, 27396813
27397048, 27400416, 27400598, 27404668, 27405645, 27416997, 27423251
27424405, 27426363, 27432062, 27433870, 27434193, 27439835, 27441326
27442041, 27445727, 27457891, 27466597, 27493674, 27501373, 27501413
27502420, 27504770, 27505229, 27508985, 27510959, 27525909, 27534509
27540613, 27544973, 27548131, 27554074, 27555481, 27558861, 27560602
27562488, 27565906, 27567477, 27593501, 27595973, 27607563, 27611612
27613080, 27613530, 27617978, 27620808, 27634676, 27634991, 27658186
27666312, 27671633, 27680669, 27686599, 27687880, 27688036, 27688099
27688692, 27691920, 27691939, 27693713, 27695063, 27698953, 27700466
27704237, 27709046, 27726780, 27740424, 27748954, 27751755, 27757567
27757888, 27758972, 27759077, 27793533, 27799032, 27801337, 27824543
27825241, 27829295, 27833672, 27834551, 27835925, 27847259, 27855490
27882176, 27898015, 27931299, 27940876, 27945870, 27951817, 27959048
27966472, 27986817, 27994325, 27995215, 27995248, 27997875, 27998003
27999638, 28000269, 28022101, 28023081, 28023482, 28033429, 28040776
28045903, 28067846, 28072567, 28074713, 28090453, 28099662, 28108003
28111583, 28120036, 28120951, 28140658, 28171079, 28174827, 28180464
28184554, 28188330, 28194173, 28199085, 28218832, 28220398, 28223871
28226179, 28229360, 28279837, 28282606, 28290434, 28302049, 28305001
28305362, 28320399, 28354603, 28361221, 28365111, 28378446, 28390273
28396445, 28420042, 28420457, 28432129, 28434028, 28437315, 28454242
28468312, 28483184, 28489150, 28502343, 28507324, 28508053, 28508557
28522441, 28528349, 28535272, 28545134, 28571483, 28578164, 28587723
28600233, 28617959, 28621470, 28627255, 28636676, 28691965, 28708023
28728272, 28749289, 28803345, 28849751, 28852691, 28856060, 28891984
28951382, 28960211, 28987439, 28991884, 28993590, 29027694, 29189889
29250230
```

Version 12.2.0.1.ru-2019-01.rur-2019-01.r1

La version 12.2.0.1.ru-2019-01.rur-2019-01.r1 comprend ce qui suit :

- Correctif 28822515 : Mise à jour version base de données janvier 2019 : 12.2.0.1.190115
- Correctif 28790651 : MISE À JOUR VERSION OJVM : 12.2.0.1.190115
- Correctif 28125601 : DSTv32 pour RDBMS (TZDATA2018E)
- Correctif 28127287 : DSTv32 pour OJVM (TZDATA2018E)
- PreUpgrade Jar : preupgrade_12201_cbuild_21_lf.zip

Mise à jour de version Oracle 12.2.0.1.190115, publiée en janvier 2019

Bogues corrigés :

```
26285062, 8480838, 8932139, 13554903, 14221306, 14690846, 15931756
16002385, 16438495, 16727454, 16942578, 17027695, 17533661, 17947871
18308268, 18521691, 18594510, 18774543, 19072655, 19211433, 19285025
19327292, 19526548, 19614243, 19647894, 19649997, 19721304, 20003668
20087519, 20118035, 20120236, 20324049, 20436508, 20532077, 20591151
20620169, 20736227, 20756305, 20866970, 20976443, 21095391, 21143725
21147908, 21159907, 21178363, 21186167, 21197098, 21216226, 21320338
21433452, 21479706, 21520266, 21547051, 21744603, 21882528, 21981529
21985256, 22007324, 22070853, 22072543, 22087683, 22104866, 22179537
22347493, 22364044, 22367053, 22379010, 22446455, 22495673, 22503283
```

```
22503297, 22504793, 22530986, 22564336, 22568728, 22581771, 22594071
22599050, 22628825, 22645009, 22654475, 22700845, 22729345, 22826067
22843979, 22845846, 22864303, 22898198, 22950945, 22970869, 22981722
23019710, 23026585, 23035249, 23055900, 23061453, 23065002, 23066146
23080557, 23104033, 23105538, 23110523, 23125560, 23126545, 23127945
23151677, 23179662, 23184263, 23197730, 23234232, 23249829, 23271203
23300142, 23310101, 23312077, 23481673, 23491861, 23499004, 23499160
23521523, 23527363, 23533647, 23548817, 23567857, 23572982, 23581777
23588722, 23599216, 23600861, 23602213, 23645516, 23665623, 23709062
23715460, 23730961, 23733981, 23735292, 23741944, 23746128, 23749454
23761724, 24010030, 24289874, 24294174, 24303148, 24307571, 24308349
24326444, 24326846, 24332831, 24334708, 24336249, 24337882, 24341675
24343905, 24345420, 24346821, 24348685, 24350620, 24352981, 24368004
24371491, 24373756, 24374976, 24376875, 24376878, 24385983, 24401351
24403922, 24415926, 24421668, 24423416, 24425056, 24425998, 24435982
24437162, 24443539, 24457597, 24460392, 24461826, 24467122, 24468470
24470606, 24471473, 24473736, 24485034, 24485161, 24485174, 24486059
24486237, 24509056, 24534401, 24554533, 24555417, 24556967, 24560906
24563422, 24570214, 24570598, 24573817, 24578718, 24578797, 24589081
24589590, 24593740, 24595699, 24600330, 24609592, 24609996, 24616637
24617969, 24623975, 24624166, 24642495, 24654629, 24655717, 24664211
24668398, 24669189, 24674197, 24674955, 24676172, 24677696, 24680959
24689376, 24692973, 24693290, 24697323, 24699619, 24710696, 24713381
24714096, 24717183, 24717859, 24718260, 24719799, 24735430, 24737064
24737403, 24737581, 24744383, 24744686, 24757934, 24759556, 24760407
24764085, 24766309, 24786669, 24792678, 24793511, 24796092, 24797119
24800423, 24801152, 24802934, 24811725, 24812047, 24827228, 24827654
24831514, 24835919, 24843188, 24844549, 24845157, 24848746, 24848923
24850622, 24907917, 24908321, 24911709, 24912588, 24922704, 24923080
24923215, 24923338, 24923790, 24929210, 24938784, 24940060, 24942749
24953434, 24957555, 24960044, 24966594, 24966788, 24968162, 24976007
24978100, 25022574, 25027852, 25028996, 25029022, 25029423, 25034396
25036474, 25044977, 25045228, 25050160, 25051628, 25057811, 25058080
25062592, 25063971, 25065563, 25072986, 25078611, 25086233, 25087436
25093872, 25098160, 25099339, 25099497, 25099758, 25100063, 25100579
25103996, 25107662, 25110233, 25114561, 25120284, 25120668, 25120742
25121089, 25123585, 25124363, 25129925, 25140197, 25145163, 25145215
25150925, 25159176, 25162645, 25164293, 25166187, 25171084, 25175723
25176408, 25178032, 25178101, 25178179, 25179774, 25182817, 25184555
25186079, 25191872, 25192044, 25192729, 25199585, 25201454, 25202355
25203656, 25206864, 25207410, 25209912, 25210268, 25210499, 25211628
25223839, 25224242, 25225795, 25226665, 25227381, 25230870, 25230945
25237577, 25240188, 25240590, 25241448, 25241625, 25244807, 25248384
25251648, 25257085, 25259611, 25262869, 25263960, 25265499, 25283790
25287072, 25296876, 25299227, 25299807, 25300427, 25305405, 25307368
25309116, 25313154, 25313411, 25316758, 25317989, 25320555, 25323525
25328518, 25329664, 25335249, 25335360, 25335790, 25337332, 25337640
25348956, 25353983, 25356118, 25357142, 25362958, 25382812, 25383204
25384462, 25386748, 25388896, 25392535, 25395696, 25397936, 25405813
25410017, 25410180, 25410802, 25410877, 25411036, 25417050, 25417056
25417958, 25425451, 25425760, 25427662, 25429959, 25430120, 25433696
25435038, 25437699, 25440818, 25444961, 25445168, 25451531, 25455795
25457409, 25459958, 25462714, 25463844, 25472112, 25476149, 25478885
25479164, 25489342, 25489367, 25489607, 25492379, 25498930, 25498994
25516250, 25524955, 25528838, 25530080, 25530814, 25535668, 25536819
25537470, 25539063, 25540738, 25546580, 25546608, 25547901, 25551676
25553616, 25554787, 25555252, 25557886, 25558986, 25560487, 25561296
25569149, 25570929, 25575348, 25575628, 25579458, 25579761, 25594901
25597525, 25598473, 25599425, 25600342, 25600421, 25602488, 25603923
25606091, 25607726, 25612095, 25614866, 25616268, 25616359, 25616417
25616645, 25631933, 25633101, 25634317, 25634348, 25635149, 25638456
25639019, 25643818, 25643931, 25646373, 25647325, 25648731, 25653109
25654459, 25654936, 25655390, 25655966, 25659655, 25660847, 25661819
25662088, 25662101, 25662524, 25669791, 25670786, 25671354, 25672640
25674386, 25680221, 25685152, 25686739, 25687460, 25691904, 25694206
25695903, 25700654, 25710420, 25715167, 25717371, 25722055, 25722608
```

```
25722720, 25728085, 25729507, 25734963, 25736747, 25739065, 25754606
25757748, 25760195, 25762221, 25764020, 25766822, 25768681, 25772669
25774077, 25775213, 25780343, 25784002, 25785331, 25785441, 25788879
25789041, 25789277, 25789579, 25790353, 25797092, 25797124, 25797305
25800464, 25802510, 25803545, 25807997, 25810704, 25813931, 25818707
25822410, 25823754, 25825910, 25826740, 25830492, 25832935, 25834581
25838361, 25852885, 25856821, 25858672, 25861398, 25865785, 25870579
25871177, 25871639, 25871753, 25872127, 25872389, 25874050, 25874678
25882264, 25885148, 25888073, 25890056, 25890673, 25894239, 25895224
25897615, 25904273, 25904490, 25906117, 25911724, 25914276, 25919622
25932524, 25932728, 25933494, 25941836, 25943271, 25945130, 25947799
25953857, 25954022, 25954054, 25957038, 25963024, 25964954, 25967544
25967985, 25970731, 25973152, 25975723, 25977302, 25980605, 25980770
25981498, 25982666, 25990907, 25995938, 26006257, 26007010, 26019148
26024732, 26025681, 26029780, 26032573, 26034119, 26036748, 26037215
26038086, 26039623, 26040483, 26045732, 26078437, 26078493, 26080410
26083298, 26088426, 26088836, 26090767, 26091640, 26091786, 26095327
26095405, 26096382, 26108080, 26108337, 26110632, 26111842, 26112621
26115103, 26121990, 26124078, 26137367, 26138085, 26149904, 26153977
26169341, 26169345, 26170715, 26176002, 26187943, 26189861, 26198757
26198926, 26201113, 26203182, 26223039, 26237431, 26237773, 26238195
26242031, 26243698, 26244115, 26245237, 26248143, 26249718, 26256131
26259265, 26261327, 26263328, 26263721, 26269790, 26271001, 26277439
26285933, 26308650, 26309047, 26318627, 26323308, 26324769, 26327624
26330994, 26331743, 26333141, 26336977, 26338953, 26351334, 26353617
26358670, 26359091, 26362821, 26366517, 26367012, 26371725, 26374791
26375250, 26380097, 26385189, 26388538, 26396790, 26399626, 26399691
26406387, 26407408, 26412540, 26418088, 26420561, 26421667, 26422277
26423085, 26426526, 26426967, 26430737, 26434436, 26434999, 26435073
26436168, 26438612, 26440749, 26442308, 26444601, 26444887, 26446098
26452606, 26474703, 26475419, 26476244, 26478970, 26479173, 26486365
26492866, 26493289, 26498354, 26513709, 26521043, 26522439, 26523432
26526726, 26536320, 26537307, 26542135, 26544823, 26545688, 26546070
26546664, 26546754, 26548363, 26556014, 26569225, 26575788, 26580633
26582460, 26584641, 26597140, 26599395, 26608137, 26609942, 26615291
26615690, 26623652, 26626879, 26629381, 26633355, 26633558, 26635897
26637273, 26637824, 26639167, 26641610, 26650226, 26658759, 26659182
26680105, 26712331, 26714486, 26714910, 26717528, 26725687, 26727397
26729494, 26729611, 26740700, 26744595, 26745002, 26751106, 26751171
26755171, 26758193, 26764561, 26765212, 26775602, 26784509, 26794786
26797591, 26798516, 26802503, 26820076, 26822620, 26828994, 26840654
26844406, 26844870, 26849779, 26875822, 26883456, 26895149, 26896659
26898563, 26907327, 26908788, 26909100, 26909504, 26911000, 26939314
26944190, 26958896, 26963310, 26966916, 26967713, 26969321, 26970717
26981902, 26983259, 26986173, 26992964, 27006664, 27009164, 27013146
27028251, 27034890, 27037839, 27038986, 27039712, 27044297, 27052607
27058530, 27060167, 27060859, 27073314, 27079140, 27087426, 27090765
27093423, 27110878, 27117822, 27119621, 27122162, 27124624, 27125872
27133662, 27135647, 27135993, 27138325, 27142373, 27142529, 27151826
27153641, 27161071, 27162405, 27163928, 27165231, 27169796, 27170305
27181537, 27181897, 27199245, 27200959, 27207110, 27213224, 27223075
27229389, 27236722, 27244337, 27248917, 27250547, 27251690, 27255377
27256000, 27258578, 27259307, 27262945, 27266245, 27274456, 27274536
27276231, 27283960, 27285244, 27292213, 27293599, 27302711, 27302730
27304410, 27305039, 27314206, 27314390, 27320576, 27321179, 27329612
27333106, 27334316, 27338912, 27338946, 27339115, 27345231, 27346709
27348081, 27349393, 27351628, 27359178, 27367194, 27370965, 27375542
27381498, 27386467, 27394703, 27395416, 27396624, 27396813, 27397048
27400416, 27400598, 27404668, 27405645, 27416997, 27433870, 27434193
27439835, 27441326, 27442041, 27445727, 27466597, 27493674, 27501373
27501413, 27502420, 27504770, 27505229, 27508985, 27510959, 27525909
27534509, 27540613, 27544973, 27548131, 27555481, 27558861, 27560602
27567477, 27593501, 27595973, 27607563, 27611612, 27613080, 27613530
27617978, 27620808, 27634676, 27658186, 27687880, 27688036, 27688099
27688692, 27691920, 27691939, 27693713, 27695063, 27698953, 27700466
27709046, 27726780, 27740424, 27748954, 27757888, 27759077, 27793533
```

```
27799032, 27801337, 27835925, 27847259, 27855490, 27882176, 27898015
27931299, 27940876, 27945870, 27951817, 27959048, 27994325, 27995248
27997875, 27998003, 27999638, 28000269, 28022101, 28023081, 28023482
28033429, 28040776, 28067846, 28072567, 28074713, 28090453, 28099662
28111583, 28120951, 28140658, 28171079, 28174827, 28180464, 28184554
28188330, 28194173, 28218832, 28220398, 28226179, 28229360, 28282606
28290434, 28302049, 28305001, 28305362, 28320399, 28354603, 28361221
28365111, 28390273, 28396445, 28420042, 28420457, 28434028, 28437315
28454242, 28483184, 28489150, 28502343, 28508053, 28508557, 28522441
28528349, 28535272, 28571483, 28617959, 28621470, 28627255, 28636676
28691965, 28708023, 28728272, 28749289, 28960211, 28993590
```

Version 12.2.0.1.ru-2018-10.rur-2018-10.r1

La version 12.2.0.1.ru-2018-10.rur-2018-10.r1 comprend ce qui suit :

- Mise à jour de version d'octobre 2018 : 12.2.0.1.181016 (28662603)

Mise à jour de version Oracle 12.2.0.1.181016, publiée en octobre 2018

Bogues corrigés :

```
28390273, 28571483, 28483184, 8480838,  13554903, 14221306, 14690846
15931756, 16002385, 16438495, 16727454, 16942578, 17027695, 17533661
17947871, 18308268, 18521691, 18594510, 18774543, 19072655, 19211433
19285025, 19327292, 19526548, 19614243, 19647894, 19649997, 19721304
20003668, 20087519, 20118035, 20120236, 20324049, 20436508, 20532077
20591151, 20620169, 20736227, 20756305, 20866970, 20976443, 21143725
21147908, 21159907, 21178363, 21186167, 21216226, 21320338, 21433452
21479706, 21520266, 21547051, 21744603, 21882528, 21981529, 21985256
22007324, 22070853, 22072543, 22087683, 22104866, 22179537, 22347493
22364044, 22367053, 22379010, 22446455, 22495673, 22503283, 22503297
22504793, 22530986, 22564336, 22568728, 22581771, 22594071, 22599050
22628825, 22645009, 22654475, 22700845, 22729345, 22826067, 22843979
22845846, 22864303, 22898198, 22950945, 22970869, 22981722, 23019710
23026585, 23035249, 23055900, 23061453, 23065002, 23066146, 23080557
23105538, 23110523, 23125560, 23126545, 23127945, 23151677, 23179662
23184263, 23197730, 23234232, 23249829, 23271203, 23300142, 23310101
23312077, 23481673, 23491861, 23499160, 23521523, 23527363, 23533647
23548817, 23567857, 23572982, 23581777, 23588722, 23599216, 23600861
23602213, 23645516, 23665623, 23709062, 23715460, 23730961, 23733981
23735292, 23741944, 23746128, 23749454, 24010030, 24289874, 24294174
24303148, 24307571, 24308349, 24326444, 24326846, 24332831, 24334708

24336249, 24337882, 24341675, 24343905, 24345420, 24346821, 24348685
24350620, 24368004, 24371491, 24373756, 24374976, 24376875, 24376878
24385983, 24401351, 24403922, 24415926, 24421668, 24423416, 24425056
24425998, 24435982, 24437162, 24443539, 24457597, 24461826, 24467122
24468470, 24470606, 24473736, 24485034, 24485161, 24485174, 24486059
24486237, 24509056, 24534401, 24554533, 24555417, 24556967, 24560906
24563422, 24570598, 24573817, 24578718, 24578797, 24589081, 24589590
24593740, 24595699, 24600330, 24609592, 24609996, 24616637, 24617969
24623975, 24624166, 24642495, 24654629, 24655717, 24664211, 24668398
24674197, 24674955, 24676172, 24677696, 24680959, 24689376, 24692973
24693290, 24699619, 24710696, 24713381, 24714096, 24717183, 24717859
24718260, 24719799, 24735430, 24737064, 24737403, 24737581, 24744383
24744686, 24757934, 24759556, 24760407, 24766309, 24786669, 24792678
24793511, 24796092, 24797119, 24800423, 24801152, 24802934, 24811725
24812047, 24827228, 24827654, 24831514, 24835919, 24843188, 24844549
24845157, 24848746, 24848923, 24850622, 24907917, 24908321, 24911709
```

```
24912588, 24922704, 24923080, 24923215, 24923338, 24923790, 24929210
24938784, 24940060, 24942749, 24953434, 24957555, 24960044, 24966594
24966788, 24968162, 24976007, 24978100, 25027852, 25029022, 25029423
25034396, 25036474, 25044977, 25045228, 25050160, 25051628, 25057811
25058080, 25062592, 25063971, 25065563, 25072986, 25078611, 25086233
25087436, 25093872, 25098160, 25099339, 25099497, 25099758, 25100063
25100579, 25103996, 25107662, 25110233, 25120284, 25120742, 25121089
25123585, 25124363, 25129925, 25140197, 25145163, 25145215, 25150925
25159176, 25162645, 25164293, 25166187, 25171084, 25175723, 25176408
25178032, 25178101, 25178179, 25179774, 25182817, 25184555, 25186079
25191872, 25192044, 25192729, 25199585, 25201454, 25202355, 25203656
25206864, 25207410, 25209912, 25210268, 25210499, 25211628, 25223839
25224242, 25225795, 25226665, 25227381, 25230945, 25237577, 25240590
25241448, 25241625, 25244807, 25248384, 25251648, 25257085, 25259611
25262869, 25263960, 25265499, 25283790, 25287072, 25296876, 25299227
25299807, 25300427, 25305405, 25307368, 25309116, 25313154, 25313411
25316758, 25317989, 25320555, 25323525, 25328518, 25329664, 25335249
25335360, 25335790, 25337332, 25337640, 25348956, 25353983, 25357142
25362958, 25382812, 25383204, 25384462, 25386748, 25388896, 25392535
25395696, 25397936, 25405813, 25410017, 25410180, 25410802, 25410877
25411036, 25417050, 25417056, 25417958, 25425451, 25425760, 25427662
25429959, 25430120, 25433696, 25435038, 25437699, 25440818, 25444961
25451531, 25455795, 25457409, 25459958, 25462714, 25463844, 25472112
25476149, 25478885, 25479164, 25489342, 25489367, 25489607, 25492379
25498930, 25498994, 25516250, 25524955, 25528838, 25530080, 25530814

25535668, 25536819, 25537470, 25539063, 25540738, 25546580, 25546608
25547901, 25551676, 25553616, 25554787, 25555252, 25557886, 25558986
25560487, 25561296, 25569149, 25570929, 25575348, 25575628, 25579458
25579761, 25594901, 25597525, 25598473, 25600342, 25600421, 25602488
25603923, 25606091, 25607726, 25612095, 25614866, 25616268, 25616359
25616417, 25616645, 25631933, 25633101, 25634317, 25634348, 25635149
25638456, 25639019, 25643818, 25643931, 25646373, 25647325, 25648731
25653109, 25654459, 25654936, 25655390, 25655966, 25659655, 25660847
25661819, 25662088, 25662101, 25662524, 25669791, 25670786, 25672640
25674386, 25680221, 25685152, 25686739, 25687460, 25691904, 25694206
25695903, 25700654, 25710420, 25715167, 25717371, 25722055, 25722608
25722720, 25728085, 25729507, 25734963, 25736747, 25739065, 25754606
25757748, 25760195, 25762221, 25764020, 25766822, 25768681, 25772669
25774077, 25775213, 25780343, 25784002, 25785331, 25785441, 25788879
25789041, 25789277, 25789579, 25790353, 25797092, 25797124, 25797305
25800464, 25803545, 25807997, 25810704, 25813931, 25818707, 25822410
25823754, 25825910, 25826740, 25830492, 25832935, 25834581, 25838361
25852885, 25856821, 25858672, 25861398, 25865785, 25870579, 25871177
25871639, 25871753, 25872127, 25872389, 25874050, 25874678, 25882264
25885148, 25888073, 25890056, 25890673, 25894239, 25895224, 25897615
25904273, 25904490, 25906117, 25911724, 25914276, 25919622, 25932524
25932728, 25933494, 25941836, 25943271, 25945130, 25947799, 25953857
25954022, 25954054, 25957038, 25963024, 25964954, 25967544, 25967985
25970731, 25973152, 25975723, 25977302, 25980605, 25980770, 25981498
25982666, 25990907, 25995938, 26006257, 26007010, 26019148, 26024732
26025681, 26029780, 26032573, 26036748, 26037215, 26038086, 26039623
26040483, 26045732, 26078437, 26078493, 26080410, 26083298, 26088426
26088836, 26090767, 26091640, 26091786, 26095327, 26095405, 26096382
26108080, 26110632, 26111842, 26121990, 26137367, 26138085, 26149904
26153977, 26169341, 26169345, 26170715, 26176002, 26187943, 26189861
26198757, 26198926, 26201113, 26223039, 26237431, 26237773, 26242031
26243698, 26244115, 26245237, 26249718, 26256131, 26259265, 26261327
26263328, 26263721, 26269790, 26271001, 26277439, 26285933, 26308650
26309047, 26318627, 26323308, 26324769, 26327624, 26330994, 26331743
26333141, 26338953, 26351334, 26353617, 26358670, 26362821, 26366517
26367012, 26374791, 26375250, 26380097, 26385189, 26388538, 26396790
26399626, 26399691, 26406387, 26412540, 26418088, 26420561, 26421667
26422277, 26426526, 26430737, 26434999, 26435073, 26436168, 26438612
26440749, 26442308, 26444601, 26444887, 26446098, 26452606, 26475419
26476244, 26478970, 26479173, 26486365, 26492866, 26493289, 26498354
```

```
26513709, 26521043, 26522439, 26523432, 26526726, 26536320, 26537307
26542135, 26544823, 26545688, 26546070, 26546664, 26546754, 26548363
26556014, 26569225, 26575788, 26582460, 26584641, 26597140, 26599395
26608137, 26609942, 26615291, 26615690, 26623652, 26626879, 26629381
26633355, 26633558, 26635897, 26637273, 26637824, 26639167, 26641610
26650226, 26658759, 26659182, 26680105, 26712331, 26714910, 26717528
26727397, 26729494, 26729611, 26740700, 26744595, 26751106, 26751171
26758193, 26764561, 26765212, 26775602, 26784509, 26794786, 26797591
26802503, 26820076, 26822620, 26828994, 26840654, 26844870, 26849779
26875822, 26883456, 26896659, 26898563, 26907327, 26908788, 26909100
26909504, 26911000, 26939314, 26944190, 26963310, 26966916, 26967713
26969321, 26970717, 26981902, 26983259, 26986173, 26992964, 27006664
27009164, 27013146, 27028251, 27034890, 27038986, 27039712, 27044297
27052607, 27060167, 27060859, 27073314, 27079140, 27087426, 27090765
27093423, 27110878, 27117822, 27119621, 27124624, 27125872, 27133662
27135647, 27135993, 27138325, 27142373, 27153641, 27161071, 27162405
27163928, 27165231, 27169796, 27170305, 27181537, 27199245, 27207110
27213224, 27229389, 27244337, 27248917, 27250547, 27251690, 27255377
27256000, 27259307, 27262945, 27274536, 27276231, 27285244, 27292213
27293599, 27302711, 27302730, 27304410, 27305039, 27314206, 27314390
27321179, 27329612, 27333106, 27334316, 27338912, 27338946, 27339115
27345231, 27346709, 27348081, 27349393, 27351628, 27359178, 27367194
27370965, 27375542, 27394703, 27395416, 27396624, 27396813, 27400598
27405645, 27416997, 27433870, 27434193, 27439835, 27441326, 27442041
27466597, 27493674, 27501373, 27501413, 27502420, 27504770, 27505229
27508985, 27510959, 27534509, 27544973, 27548131, 27555481, 27558861
27560602, 27567477, 27595973, 27607563, 27611612, 27613080, 27620808
27687880, 27688036, 27688692, 27691920, 27691939, 27698953, 27700466
27709046, 27726780, 27740424, 27748954, 27757888, 27799032, 27835925
27847259, 27882176, 27898015, 27940876, 27945870, 27951817, 27959048
27994325, 27997875, 27998003, 28000269, 28033429, 28040776, 28074713
28090453, 28099662, 28140658, 28171079, 28174827, 28184554, 28188330
28218832, 28226179, 28290434, 28305001, 28320399, 28354603, 28437315
28454242, 28508557, 28522441
```

Moteur de base de données : 12.1.0.2

Les versions suivantes sont disponibles pour le moteur de base de données 12.1.0.2 :

- Version 12.1.0.2.v21 (p. 1278)
- Version 12.1.0.2.v20 (p. 1282)
- Version 12.1.0.2.v19 (p. 1285)
- Version 12.1.0.2.v18 (p. 1289)
- Version 12.1.0.2.v17 (p. 1292)
- Version 12.1.0.2.v16 (p. 1295)
- Version 12.1.0.2.v15 (p. 1297)
- Version 12.1.0.2.v14 (p. 1300)
- Version 12.1.0.2.v13 (p. 1302)
- Version 12.1.0.2.v12 (p. 1304)
- Version 12.1.0.2.v11 (p. 1306)
- Version 12.1.0.2.v10 (p. 1308)
- Version 12.1.0.2.v9 (p. 1310)
- Version 12.1.0.2.v8 (p. 1312)
- Version 12.1.0.2.v7 (p. 1314)
- Version 12.1.0.2.v6 (p. 1315)

- Version 12.1.0.2.v5 (p. 1316)
- Version 12.1.0.2.v4 (p. 1318)
- Version 12.1.0.2.v3 (p. 1319)
- Version 12.1.0.2.v2 (p. 1320)
- Version 12.1.0.2.v1 (p. 1320)

Version 12.1.0.2.v21

La version 12.1.0.2.v21 comprend les éléments suivants :

- Correctif 31113348 : mise à jour d'ensemble de correctifs de base de données : 12.1.0.2.200714
- Correctif 31219939 : PSU de base de données 12.1.0.2.200714, composant Oracle JavaVM (JUL2020)
- Correctif 31335037 : DSTV35 pour RDBMS (TZDATA2020A)
- Correctif 31335142 : DSTV35 pour OJVM (TZDATA2020A)
- Correctif 17969866 : Oracle GoldenGate – 46719 : ENH : PRISE EN CHARGE DE LA RÉPLICATION POUR LES INSERTIONS/MISES À JOUR COMPLÈTES AVEC DES VALEURS ÉLEVÉES
- Correctif 20394750 : Oracle GoldenGate – ÉCHEC DE L'APPLICATION DE LA RÉSOLUTION CDR POUR LES ÉLÉMENTS LOBS, XML, LONG et LES OBJETS
- Correctif 24835919 : Oracle GoldenGate – PANNE D'EXÉCUTION PAR IR DE TRANSACTIONS DEPENDANTES AVEC PARALLÉLISME DE TYPE SUPÉRIEUR À
- Correctif 20033733 : PART :IMC:HIT ORA 600 [KGL-HEAP-SIZE-EXCEEDED]
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS
- Correctif 23711335 : CDB_UPG:PDCDB:CDB UPGRADE AS WHOLE TAKES 1 MORE HOUR THAN PREVIOUS LABELS IN MAY
- Correctif 31579750 : ensemble de correctifs JSON
- Correctif 21091901 : LE DÉPLACEMENT EN LIGNE LA PARTITION PAR HACHAGE OU PAR RÉFÉRENCE PEUT EMPÊCHER LA COHÉRENCE DES INDEX LOCAUX
- Correctif 21171382 : Correctif DBMS_STATS AUTO DOP COMPUTES A HIGH DOP UNNECESSARILY
- Correctif 23262847 : Oracle GoldenGate – RÉEXÉCUTION MAL EFFECTUÉE AYANT PROVOQUÉ UNE FIN ANORMALE DE LA RÉPLICATION OGG
- PreUpgrade Jar : preupgrade_12.1.0.2.0_18_crlf.zip

Correctifs combinés pour la version 12.1.0.2.v21, publiée en juillet 2020

Bogues corrigés :

```
6194865, 6418158, 6599380, 13542050, 13787015, 14283239, 14643995
14705949, 16090440, 16354467, 16359751, 16439813, 16619249, 16756406
16777441, 16799735, 16863642, 16870214, 16875041, 16887946, 16923858
16938780, 16941434, 17008068, 17210525, 17258582, 17274537, 17319928
17365043, 17409174, 17414008, 17432124, 17495022, 17532729, 17532734
17533661, 17551063, 17655240, 17722075, 17760068, 17835294, 17867700
17890099, 17969866, 18007682, 18043064, 18051556, 18090142, 18110491
18122373, 18191823, 18202441, 18250893, 18254023, 18272672, 18288842
18306996, 18307021, 18308268, 18354830, 18371441, 18373438, 18382302
18411216, 18417036, 18419520, 18436647, 18440095, 18456643, 18475439
18492302, 18499088, 18510194, 18542562, 18548246, 18548433, 18549238
18604493, 18604692, 18607546, 18610915, 18618122, 18628388, 18648816
```

```
18662619, 18673090, 18674024, 18674047, 18681056, 18693124, 18700762
18705806, 18727933, 18733351, 18740837, 18742258, 18743542, 18758877
18759211, 18774543, 18775971, 18778801, 18791688, 18797519, 18798250
18799063, 18799993, 18801391, 18803726, 18810904, 18818069, 18819908
18840932, 18841764, 18845653, 18849537, 18849970, 18851894, 18856106
18856999, 18866977, 18868646, 18885870, 18886413, 18893947, 18895170
18899974, 18900107, 18904062, 18909599, 18913440, 18914624, 18921743
18940497, 18948177, 18952766, 18952989, 18964939, 18964978, 18966843
18967382, 18973548, 18974476, 18988834, 18990023, 18990693, 18999568
19001359, 19001390, 19012119, 19013183, 19016730, 19017309, 19018206
19018447, 19022470, 19023822, 19024808, 19028800, 19032777, 19035573
19044962, 19048007, 19050649, 19052488, 19054077, 19058490, 19060015
19065556, 19065677, 19067244, 19068380, 19068610, 19068970, 19074147
19075256, 19076343, 19077215, 19079752, 19081128, 19124336, 19124589
19130152, 19131386, 19131607, 19134173, 19141838, 19143550, 19146474
19149990, 19153980, 19154375, 19155797, 19157754, 19165673, 19168167
19171086, 19174430, 19174521, 19174942, 19176223, 19176326, 19176885
19178851, 19180394, 19180770, 19183343, 19185876, 19188927, 19189317
19189525, 19195895, 19197175, 19201867, 19207117, 19211433, 19213447
19223010, 19231857, 19238590, 19243521, 19245191, 19248279, 19248799
19258504, 19272708, 19279273, 19280225, 19284031, 19285025, 19289642
19291380, 19297917, 19303936, 19304354, 19306797, 19307662, 19308965
19309466, 19313563, 19315668, 19315691, 19317646, 19326908, 19327391
19329654, 19330795, 19332396, 19333670, 19335438, 19339555, 19347458
19354335, 19354794, 19358317, 19363645, 19364502, 19366375, 19370504
19371175, 19373893, 19375649, 19382851, 19383839, 19385656, 19390567
19390620, 19393542, 19396455, 19399918, 19402853, 19404068, 19409212
19430401, 19433930, 19434529, 19439759, 19440520, 19440586, 19445860
19448499, 19450116, 19450314, 19452434, 19461270, 19461428, 19468347
19468612, 19468991, 19469538, 19475971, 19487147, 19490948, 19501299
19503821, 19512341, 19516448, 19518079, 19520602, 19523462, 19524158
19524384, 19529868, 19532017, 19534363, 19536415, 19543384, 19547370
19547774, 19548064, 19550902, 19561643, 19562381, 19566592, 19571055
19571082, 19571367, 19577410, 19578247, 19578350, 19583624, 19587324
19590877, 19591608, 19593445, 19597439, 19597583, 19601762, 19604659
19606174, 19617921, 19619732, 19623450, 19627012, 19632912, 19637186
19639483, 19644859, 19647503, 19649152, 19658708, 19662635, 19663176
19670108, 19676012, 19676905, 19680796, 19684504, 19687159, 19689979
19693090, 19699191, 19699946, 19701015, 19703301, 19705781, 19706965
19708342, 19708632, 19718981, 19721304, 19723336, 19730508, 19769480
19769625, 19777862, 19781326, 19784751, 19790243, 19791273, 19791377
19799847, 19805359, 19809171, 19811709, 19817386, 19818513, 19824871
19831647, 19835133, 19841800, 19855285, 19859472, 19865345, 19869255
19871910, 19873610, 19877336, 19879746, 19880190, 19883092, 19886165
19888853, 19889230, 19891090, 19895326, 19895362, 19896336, 19902195
19908836, 19909862, 19915271, 19928926, 19930276, 19931367, 19931709
19932634, 19933147, 19941352, 19943771, 19952975, 19957298, 19978542
19982584, 19988852, 19989009, 19990037, 19995869, 20001168, 20009569
20009833, 20011515, 20011646, 20011897, 20017509, 20023340, 20031873
20043616, 20048359, 20052269, 20061399, 20074391, 20076781, 20078186
20087383, 20093776, 20101006, 20117253, 20118035, 20122715, 20124446
20134113, 20134339, 20139391, 20144019, 20144308, 20165574, 20169408
20171986, 20172151, 20173897, 20175161, 20181030, 20212067, 20217801
20228093, 20229001, 20233181, 20235511, 20245930, 20250147, 20267166
20273319, 20281121, 20284155, 20294666, 20296619, 20298413, 20302006
20308798, 20315311, 20318889, 20322560, 20324049, 20328248, 20331945
20347562, 20348653, 20354900, 20356733, 20361671, 20368850, 20373598
20374572, 20378086, 20382309, 20387265, 20394750, 20397490, 20401975
20402832, 20408829, 20408866, 20413820, 20415564, 20424183, 20424899
20425790, 20428621, 20432873, 20437153, 20440930, 20441797, 20446883
20447445, 20459944, 20464614, 20466322, 20466628, 20468401, 20468490
20470877, 20471920, 20474192, 20475845, 20476175, 20480209, 20493163
20505778, 20509482, 20513399, 20524085, 20528052, 20539050, 20543011
20544065, 20554364, 20557786, 20558005, 20560611, 20562898, 20564072
20565112, 20565133, 20569094, 20577490, 20581111, 20582405, 20588486
20588502, 20591183, 20596234, 20598042, 20603378, 20603431, 20613079
```

```
20618595, 20627866, 20635353, 20641666, 20657411, 20657441, 20669434
20671094, 20673810, 20677396, 20677974, 20684983, 20686773, 20688221
20703000, 20703629, 20704450, 20705577, 20707932, 20708701, 20711718
20717081, 20717091, 20717359, 20725343, 20734332, 20736227, 20746251
20757079, 20764012, 20766180, 20768076, 20778986, 20794034, 20798891
20800890, 20801783, 20803014, 20825533, 20828947, 20830459, 20831538
20832516, 20835241, 20839705, 20842388, 20844426, 20848335, 20856766
20859910, 20860659, 20862087, 20868862, 20869721, 20875898, 20877664
20878790, 20879709, 20879889, 20880215, 20882568, 20890311, 20897759
20898391, 20898997, 20899461, 20904530, 20907061, 20914870, 20919320
20920911, 20922010, 20925795, 20926021, 20929771, 20936731, 20936905
20938170, 20951038, 20952966, 20958816, 20977794, 20978259, 21037923
21047766, 21047803, 21052842, 21059919, 21060755, 21061354, 21063322
21068507, 21072646, 21080143, 21091431, 21091901, 21095391, 21097043
21099555, 21101873, 21106027, 21132297, 21133343, 21142837, 21147908
21153266, 21157728, 21159665, 21164318, 21171382, 21172913, 21174504
21184223, 21186167, 21188532, 21188537, 21188584, 21196809, 21197626
21220620, 21225209, 21239530, 21241052, 21241829, 21246723, 21260397
21260431, 21263635, 21266085, 21270823, 21273804, 21275255, 21281532
21281607, 21285458, 21291274, 21293600, 21294938, 21296029, 21297872
21299490, 21300341, 21308727, 21315084, 21322887, 21329301, 21354456
21373076, 21373473, 21380789, 21383171, 21385422, 21387128, 21387964
21419850, 21421886, 21422580, 21424824, 21425496, 21429602, 21442094
21450666, 21476308, 21479753, 21492036, 21502702, 21514877, 21516611
21517440, 21522582, 21526048, 21532755, 21534893, 21542577, 21555660
21560152, 21566639, 21566944, 21566993, 21575362, 21620471, 21623164
21625179, 21626377, 21629064, 21632821, 21641414, 21641760, 21644640
21649497, 21656630, 21659726, 21665897, 21668627, 21675340, 21695575
21698350, 21744290, 21756661, 21756677, 21756699, 21764119, 21773465
21780146, 21785691, 21787056, 21794615, 21795111, 21811517, 21820934
21821302, 21828126, 21837606, 21842017, 21842740, 21847223, 21856522
21863727, 21868720, 21875360, 21889720, 21893235, 21896069, 21899588
21911701, 21913183, 21915719, 21917884, 21924131, 21960504, 21967197
21977186, 21977392, 22007324, 22018363, 22022760, 22024071, 22037014
22046677, 22062026, 22062517, 22068305, 22070866, 22072818, 22075064
22077517, 22083366, 22087683, 22092979, 22118835, 22118851, 22139226
22146062, 22148226, 22160989, 22165897, 22168163, 22173980, 22175564
22176950, 22178855, 22179537, 22185234, 22205263, 22214989, 22223463
22228324, 22232606, 22233505, 22238921, 22243719, 22243983, 22250006
22256431, 22256560, 22258530, 22264489, 22268833, 22282748, 22294260
22296366, 22301880, 22305887, 22346829, 22347493, 22351572, 22353199
22353346, 22359063, 22364044, 22365117, 22366322, 22366558, 22374754
22380919, 22454326, 22458049, 22465352, 22468781, 22475617, 22492533
22495062, 22495673, 22496904, 22499356, 22501616, 22503297, 22507210
22507234, 22515353, 22517782, 22518784, 22519146, 22520320, 22528741
22529728, 22533631, 22536802, 22551446, 22568016, 22568177, 22568797
22606521, 22624709, 22645009, 22654475, 22657942, 22670385, 22670413
22674709, 22675136, 22686674, 22690648, 22695831, 22707244, 22707866
22721409, 22729345, 22730454, 22733141, 22734547, 22750215, 22757364
22760595, 22760679, 22762046, 22782647, 22806698, 22808310, 22809871
22815955, 22816287, 22820579, 22826718, 22836801, 22842151, 22855193
22862134, 22865673, 22873635, 22894949, 22897344, 22901797, 22905130
22916353, 22922076, 22923409, 22950945, 22961508, 22972770, 22977256
23002524, 23003979, 23007241, 23008056, 23019710, 23020270, 23025340
23026585, 23028781, 23029562, 23035249, 23053606, 23061453, 23061702
23065323, 23066146, 23068169, 23080557, 23084507, 23088803, 23089357
23096938, 23101501, 23104033, 23105538, 23108128, 23115139, 23124895
23125826, 23126410, 23140259, 23148260, 23149541, 23151677, 23168363
23170620, 23172924, 23177536, 23177923, 23184263, 23195445, 23197103
23209741, 23220453, 23229229, 23237313, 23240358, 23260854, 23262847
23265914, 23265965, 23266217, 23272045, 23294548, 23302839, 23314180
23315153, 23315889, 23324000, 23326313, 23328639, 23338911, 23342170
23492665, 23501901, 23514710, 23514911, 23521523, 23528412, 23533524
23533807, 23543183, 23548817, 23567857, 23571055, 23572982, 23602213
23614158, 23628685, 23642282, 23709062, 23711335, 23713236, 23717151
23725036, 23727148, 23731896, 23746128, 23854396, 24285405, 24300640
```

```
24303148, 24307571, 24308635, 24315824, 24316947, 24321547, 24326444
24341675, 24350620, 24350831, 24365589, 24385625, 24385983, 24386767
24393981, 24397438, 24401351, 24411921, 24413809, 24415926, 24416451
24421668, 24423416, 24425998, 24437510, 24448240, 24448282, 24457597
24461826, 24509056, 24523374, 24534298, 24555417, 24560906, 24563422
24570598, 24573817, 24577566, 24589081, 24600330, 24624166, 24642295
24652769, 24662775, 24674955, 24683149, 24690216, 24693382, 24701840
24713381, 24717859, 24718260, 24719736, 24737064, 24737403, 24737581
24737954, 24739928, 24752618, 24766121, 24790914, 24792678, 24796092
24801152, 24802934, 24808595, 24812585, 24825843, 24831514, 24835538
24835919, 24848928, 24907917, 24908321, 24917972, 24920582, 24929210
24966594, 25029423, 25031502, 25034396, 25042823, 25047724, 25051465
25056052, 25058080, 25060506, 25067795, 25076732, 25076756, 25079710
25091141, 25093739, 25093872, 25099339, 25107334, 25110233, 25123585
25150925, 25161298, 25165496, 25178179, 25192729, 25210690, 25240188
25248384, 25264559, 25300427, 25307368, 25313154, 25328093, 25330273
25353983, 25357142, 25377044, 25392535, 25405687, 25415713, 25417056
25417958, 25423453, 25427662, 25429959, 25437695, 25437699, 25459958
25472885, 25475853, 25476125, 25477657, 25482971, 25483815, 25484507
25486384, 25489342, 25489367, 25489607, 25490238, 25492379, 25494379
25494413, 25495682, 25539063, 25546608, 25547060, 25551676, 25555252
25575628, 25579761, 25599425, 25600342, 25600421, 25602488, 25606091
25612095, 25616268, 25633101, 25634317, 25635149, 25639019, 25643931
25649873, 25653109, 25654936, 25655390, 25669791, 25670786, 25695903
25699321, 25722055, 25733479, 25740844, 25743479, 25760195, 25764020
25766822, 25775213, 25780343, 25789277, 25790353, 25809524, 25822410
25823532, 25823754, 25856821, 25861398, 25879984, 25881255, 25885148
25897615, 25914276, 25919622, 25947799, 25957038, 25982666, 25986062
25997810, 26007010, 26023002, 26023025, 26024732, 26027162, 26029780
26039623, 26088426, 26089440, 26110259, 26110632, 26111842, 26121990
26153977, 26187943, 26198757, 26198926, 26203182, 26243698, 26245237
26248143, 26256131, 26262953, 26263721, 26318627, 26324206, 26325856
26336977, 26353617, 26366517, 26412540, 26430737, 26439748, 26444887
26446098, 26482376, 26513067, 26513709, 26544823, 26546664, 26546754
26556014, 26569225, 26570171, 26575788, 26633558, 26635845, 26637592
26637824, 26654363, 26658759, 26714910, 26758193, 26768025, 26784509
26822620, 26828994, 26832296, 26844406, 26875822, 26898563, 26968670
26999139, 27000663, 27000690, 27001733, 27012701, 27015449, 27033652
27034890, 27052607, 27060167, 27072923, 27086138, 27092508, 27097854
27101105, 27122162, 27133662, 27169796, 27199245, 27207110, 27207634
27213224, 27217412, 27223075, 27229389, 27255377, 27274536, 27276231
27303938, 27314206, 27314390, 27314697, 27337759, 27348081, 27351628
27370965, 27375542, 27397048, 27404573, 27424405, 27433385, 27441326
27445727, 27461789, 27461842, 27468303, 27475603, 27487919, 27534509
27548131, 27567477, 27611612, 27620950, 27623159, 27629756, 27634991
27642235, 27710072, 27726780, 27751755, 27829295, 27846298, 27847259
27897759, 27923320, 27929509, 27938623, 27952577, 27952584, 27986817
27995248, 27997875, 28000269, 28022101, 28023399, 28024793, 28025414
28026866, 28043157, 28079127, 28098160, 28125601, 28164480, 28174827
28199085, 28215510, 28250929, 28281094, 28302049, 28305362, 28357401
28369092, 28384353, 28390273, 28420042, 28423598, 28432129, 28440711
28501075, 28502113, 28502128, 28507324, 28542455, 28566241, 28578164
28587723, 28612674, 28636676, 28639299, 28683167, 28708023, 28714988
28730253, 28758090, 28774416, 28790654, 28797711, 28821847, 28849751
28852325, 28867992, 28891741, 28915933, 28950969, 28986231, 28993590
29006527, 29009513, 29027694, 29030780, 29142109, 29163567, 29189889
29200700, 29247712, 29250317, 29251241, 29254615, 29260956, 29343156
29372460, 29378913, 29379978, 29388020, 29408136, 29434301, 29437712
29464779, 29483626, 29483672, 29483723, 29483771, 29500257, 29500963
29511611, 29559723, 29621961, 29633753, 29637560, 29645349, 29707896
29719146, 29726695, 29774367, 29774383, 29782211, 29791152, 29817278
29828111, 29869404, 29869906, 29893132, 29944660, 29961353, 29962927
29962939, 29997937, 30116203, 30128197, 30160639, 30164714, 30179644
30200680, 30215130, 30218044, 30225443, 30252098, 30295478, 30305880
30365745, 30497057, 30499600, 30502041, 30522998, 30534664, 30624864
30659882, 30668407, 30698289, 30758943, 30803210, 30805558, 30816938
```

```
30855121, 30973003, 30987088, 31001455, 31013127, 31022858, 31031715
31113348, 31156383, 31219939, 31306274, 31335037, 31335142
```

Version 12.1.0.2.v20

La version 12.1.0.2.v20 inclut les éléments suivants :

- Correctif 30700212 : PSU de base de données 12.1.0.2.200414
- Correctif 30805558 : PSU de base de données de composant Oracle JVM 12.1.0.2.200414
- Correctif 29997937 : DSTv34 pour RDBMS (TZDATA2019G)
- Correctif 29997959 : DSTv34 pour OJVM (TZDATA2019G)
- Correctif 17969866 : Oracle GoldenGate – 46719 : ENH : PRISE EN CHARGE DE LA RÉPLICATION POUR LES INSERTIONS/MISES À JOUR COMPLÈTES AVEC DES VALEURS ÉLEVÉES
- Correctif 20394750 : Oracle GoldenGate – ÉCHEC DE L'APPLICATION DE LA RÉSOLUTION CDR POUR LES ÉLÉMENTS LOBS, XML, LONG et LES OBJETS
- Correctif 24835919 : Oracle GoldenGate – PANNE D'EXÉCUTION PAR IR DE TRANSACTIONS DEPENDANTES AVEC PARALLÉLISME DE TYPE SUPÉRIEUR À
- Correctif 23262847 : Oracle GoldenGate – RÉEXÉCUTION MAL EFFECTUÉE AYANT PROVOQUÉ UNE FIN ANORMALE DE LA RÉPLICATION OGG
- Correctif 21171382 : Correctif DBMS_STATS
- Correctif 21091901 : LE DÉPLACEMENT EN LIGNE LA PARTITION PAR HACHAGE OU PAR RÉFÉRENCE PEUT EMPÊCHER LA COHÉRENCE DES INDEX LOCAUX
- Correctif 31164857 : ensemble de correctifs JSON
- Correctif 20033733 : PART :IMC:HIT ORA 600 [KGL-HEAP-SIZE-EXCEEDED]
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS
- PreUpgrade Jar : preupgrade_12.1.0.2.0_18_crlf.zipn
- Prise en charge de Purge de la corbeille (p. 1129)
- Prise en charge de Génération de rapports de performance avec AWR (Automatic Workload Repository) (p. 1119) utilisant le package `rdsadmin.rdsadmin_diagnostic_util`.

Correctifs combinés pour la version 12.1.0.2, publiés en avril 2020

Bogues corrigés :

```
19309466, 19902195, 18250893, 25437699, 19383839, 19781326, 16756406
18456643, 26546664, 22364044, 29483723, 18913440, 18845653, 28774416
19915271, 20172151, 18417036, 19516448, 24907917, 23713236, 24796092
23140259, 21856522, 29434301, 23028781, 19243521, 19658708, 18272672
21153266, 19174430, 28250929, 18900107, 22243719, 19548064, 26556014
20493163, 20688221, 22346829, 21387964, 13542050, 25377044, 22072818
22250006, 22734547, 22243983, 21623164, 21534893, 19012119, 19932634
19869255, 22232606, 18681056, 23324000, 25427662, 22068305, 24589081
19439759, 19303936, 18856106, 22916353, 24835538, 22353346, 19790243
21106027, 20023340, 26444887, 23088803, 22529728, 26256131, 18492302
19134173, 24303148, 21101873, 20447445, 27122162, 21188584, 19390567
26513709, 25780343, 19769480, 21097043, 21225209, 27217412, 26245237
20677396, 19284031, 19450314, 23514911, 19016730, 27303938, 22205263
22517782, 20919320, 22075064, 29621961, 22551446, 29250317, 22721409
18440095, 22496904, 27611612, 16439813, 18354830, 20596234, 22022760
20936905, 22268833, 23197103, 23746128, 22515353, 27897759, 21514877
```

```
19809171, 21186167, 26111842, 18990023, 13787015, 22492533, 25405687
22233505, 20173897, 24624166, 17210525, 29707896, 21260431, 25579761
20181030, 25056052, 19370504, 21868720, 24423416, 23068169, 19124589
22690648, 21383171, 19402853, 19888853, 25107334, 24341675, 17722075
20882568, 25653109, 23026585, 18604692, 20717081, 25546608, 20768076
27370965, 19081128, 22173980, 25722055, 23514710, 29483771, 19178851
20951038, 22168163, 25161298, 20569094, 24308635, 28302049, 19791377
19050649, 20920911, 29962939, 30365745, 22475617, 19189525, 19060015
19469538, 27052607, 29633753, 20598042, 22458049, 18988834, 21159665
23302839, 25307368, 25699321, 21924131, 21837606, 17409174, 20588486
22729345, 22842151, 25051465, 19238590, 16941434, 20387265, 29378913
24397438, 20673810, 23108128, 20356733, 28215510, 22380919, 18436647
21764119, 23065323, 20825533, 19124336, 22294260, 20839705, 24790914
20284155, 23571055, 6194865, 25539063, 17365043, 25914276, 20952966
22961508, 19176223, 21300341, 23237313, 18288842, 27223075, 22353199
20011515, 22083366, 28305362, 27634991, 25670786, 21419850, 26898563
22495673, 27986817, 19577410, 26248143, 23294548, 25328093, 23101501
24737064, 19931709, 25423453, 25547060, 23533807, 27726780, 24600330
20635353, 28384353, 25600421, 18122373, 20043616, 23124895, 18856999
21450666, 24752618, 18893947, 26633558, 20076781, 20926021, 26029780
21196809, 21354456, 22533631, 23725036, 20464614, 19562381, 27375542
24808595, 19189317, 25669791, 18307021, 21917884, 19708632, 28423598
27213224, 25633101, 29006527, 20711718, 18973548, 25982666, 25472885
19718981, 20684983, 23567857, 22826718, 25655390, 21773465, 20250147
20144019, 19197175, 26263721, 19597439, 28867992, 21387128, 22007324
28797711, 18818069, 21566639, 19180770, 19879746, 21785691, 20539050
20424183, 24285405, 21425496, 26544823, 19957298, 20322560, 29962927
22228324, 23172924, 22520320, 29817278, 28164480, 30179644, 27751755
21575362, 25058080, 22365117, 22645009, 25165496, 28950969, 27133662
27433385, 18774543, 20124446, 21429602, 29189889, 26153977, 30659882
19371175, 21863727, 18940497, 19074147, 22923409, 25489342, 21380789
19154375, 25417056, 19044962, 19532017, 23080557, 19662635, 22374754
20560611, 25654936, 21492036, 18705806, 28420042, 19578247, 20705577
22024071, 22238921, 29645349, 22809871, 21184223, 19995869, 23089357
19404068, 18921743, 19065677, 19018447, 19018206, 18308268, 19777862
27314697, 29027694, 22223463, 19304354, 22519146, 23020270, 22214989
19445860, 26654363, 27199245, 22977256, 20890311, 27445727, 28281094
21142837, 20869721, 22258530, 24555417, 22179537, 21756699, 18801391
18648816, 20217801, 18819908, 19550902, 22760595, 25483815, 19543384
23628685, 25482971, 30252098, 23007241, 19593445, 21080143, 27351628
20582405, 24966594, 20031873, 29828111, 25489367, 20374572, 18618122
24737581, 21698350, 22501616, 26784509, 28043157, 19306797, 24739928
18966843, 19077215, 20704450, 19068970, 20543011, 19023822, 24713381
22836801, 20432873, 21756677, 23168363, 20328248, 18674047, 18849537
20087383, 25459958, 20315311, 29163567, 22897344, 27534509, 26768025
20686773, 25178179, 19308965, 18948177, 20764012, 27623159, 19468991
20868862, 21780146, 23315153, 20466628, 21756661, 20397490, 19706965
20302006, 24831514, 23240358, 22178855, 19032777, 20862087, 19329654
18974476, 20603378, 21275255, 20859910, 29500963, 19307662, 26203182
21847223, 20281121, 28079127, 22568797, 19075256, 19076343, 28026866
29511611, 18866977, 22808310, 25635149, 20844426, 20904530, 20441797
20175161, 20296619, 19831647, 18548246, 30497057, 21442094, 25079710
24674955, 18840932, 18740837, 20294666, 27404573, 21037923, 25602488
21517440, 22062517, 19180394, 27337759, 19174942, 27092508, 20671094
21889720, 19347458, 19450116, 18411216, 20117253, 24386767, 24737954
20641666, 19931367, 25264559, 19930276, 22092979, 25616268, 21625179
20879709, 23003979, 20165574, 28578164, 19272708, 19547370, 22624709
23084507, 23184263, 20228093, 21281532, 25093872, 19805359, 26324206
19461270, 18700762, 19434529, 18799063, 20354900, 29388020, 20378086
17008068, 21246723, 20831538, 20424899, 20361671, 18674024, 19689979
24411921, 19873610, 16619249, 20562898, 21641414, 21091431, 19440586
20001168, 22757364, 22175564, 22499356, 20725343, 21241052, 19561643
28199085, 21270823, 20736227, 19399918, 19195895, 20830459, 20017509
18475439, 25790353, 21828126, 21665897, 25555252, 20746251, 19315668
22568177, 25764020, 25612095, 25357142, 23096938, 19067244, 19943771
18043064, 19941352, 21329301, 18885870, 26243698, 26187943, 20324049
```

```
30164714, 19536415, 30305880, 23709062, 28174827, 20446883, 27314206
21299490, 25313154, 18628388, 21744290, 18254023, 27072923, 25047724
20591183, 27847259, 20459944, 19185876, 18548433, 27207110, 22465352
24385625, 24326444, 24920582, 20402832, 19627012, 22733141, 29200700
20468401, 27441326, 27620950, 16863642, 19639483, 19315691, 27567477
21479753, 19174521, 23177923, 20401975, 18306996, 18851894, 21424824
27034890, 20581111, 20318889, 20936731, 21060755, 25240188, 26828994
27629756, 22256560, 19188927, 23328639, 27229389, 20766180, 20229001
24570598, 25475853, 21172913, 17655240, 29379978, 21266085, 19028800
19035573, 19366375, 28821847, 24523374, 25599425, 25034396, 19289642
21502702, 21291274, 18007682, 23521523, 20475845, 29408136, 22148226
22528741, 25417958, 29500257, 24652769, 26088426, 19326908, 19597583
17414008, 23019710, 20897759, 26822620, 22046677, 19663176, 20938170
19891090, 24825843, 26318627, 21960504, 20524085, 24509056, 19054077
21385422, 26262953, 22657942, 20428621, 21899588, 23326313, 19723336
28891741, 19835133, 17532734, 17495022, 25300427, 19333670, 21842017
19285025, 21373473, 29483626, 23260854, 23061453, 19687159, 14643995
22146062, 20977794, 20734332, 16938780, 17551063, 27548131, 21977392
28612674, 24461826, 19676012, 20588502, 23315889, 19520602, 23053606
19841800, 20245930, 19001359, 21476308, 26546754, 19393542, 30215130
23533524, 21099555, 29961353, 17532729, 27995248, 25429959, 19141838
19644859, 21915719, 19908836, 21421886, 19358317, 27101105, 19524158
29869404, 28758090, 23548817, 25861398, 20803014, 23025340, 19335438
19058490, 23642282, 19207117, 18799993, 25919622, 26569225, 25986062
20835241, 24662775, 20958816, 19475971, 18967382, 20347562, 25740844
20348653, 29009513, 19896336, 24812585, 20048359, 21896069, 20468490
19524384, 25392535, 21147908, 21695575, 30295478, 20440930, 30973003
25789277, 19171086, 24718260, 17867700, 19791273, 26110632, 27397048
21241829, 19591608, 18662619, 22707244, 18419520, 22296366, 22654475
18914624, 19571367, 28636676, 21522582, 29893132, 19501299, 26007010
19529868, 20425790, 19708342, 27487919, 27997875, 26968670, 16870214
18202441, 24415926, 18743542, 19001390, 21157728, 20657411, 19332396
22606521, 21875360, 21821302, 25091141, 28000269, 19149990, 20382309
22855193, 16777441, 19606174, 28542455, 20848335, 25495682, 19382851
20528052, 22762046, 24563422, 27468303, 23125826, 22503297, 28993590
25192729, 23338911, 27274536, 22730454, 19354794, 20757079, 19176326
20298413, 19048007, 22018363, 24300640, 18849970, 21532755, 20860659
22905130, 26121990, 21263635, 23602213, 27710072, 23209741, 22160989
18499088, 18775971, 22894949, 21059919, 18952989, 27348081, 22518784
25856821, 24457597, 25885148, 25484507, 20794034, 20554364, 21061354
19468347, 17533661, 19883092, 20657441, 24401351, 21285458, 28023399
18051556, 25330273, 26412540, 24425998, 19699191, 24437510, 16875041
20669434, 18964978, 25415713, 23342170, 22972770, 28369092, 20828947
21373076, 25492379, 25551676, 14283239, 25766822, 21967197, 22922076
19601762, 25575628, 26110259, 20368850, 21239530, 20437153, 24848928
20880215, 20798891, 25606091, 19013183, 29782211, 21095391, 25042823
21133343, 22695831, 24365589, 25248384, 25634317, 20134113, 19587324
20273319, 28501075, 18542562, 19017309, 26758193, 21063322, 22062026
24802934, 27829295, 20134339, 22077517, 22815955, 23854396, 24690216
22507210, 16354467, 20101006, 21795111, 27938623, 23501901, 18797519
25997810, 23029562, 25879984, 26844406, 21260397, 25029423, 29726695
19354335, 19730508, 22366558, 19390620, 26658759, 25822410, 6599380
20717359, 24321547, 27097854, 21297872, 18964939, 19871910, 29437712
26366517, 21913183, 25695903, 22366322, 20171986, 20603431, 21132297
25957038, 21542577, 29791152, 22507234, 23170620, 24719736, 25600342
18868646, 28587723, 29142109, 26637824, 20627866, 18110491, 16923858
24642295, 19518079, 20914870, 19339555, 20466322, 25823754, 25110233
20169408, 24908321, 20842388, 17274537, 26575788, 20474192, 21644640
28849751, 21794615, 18899974, 20471920, 22806698, 19052488, 29944660
29260956, 26198757, 19503821, 23717151, 24350620, 23126410, 20074391
25823532, 19157754, 22495062, 21220620, 24316947, 19865345, 19065556
22816287, 25947799, 20878790, 23492665, 21322887, 22305887, 19617921
20879889, 24350831, 19578350, 28022101, 26439748, 21893235, 19363645
21072646, 20898391, 19291380, 27060167, 18382302, 27086138, 22536802
22087683, 21197626, 21656630, 20373598, 19248799, 22707866, 28432129
19155797, 19279273, 18886413, 25490238, 20922010, 19990037, 25150925
```

```
20509482, 20778986, 22282748, 27255377, 24717859, 20703000, 22862134
21526048, 28683167, 24929210, 24560906, 19079752, 25486384, 20144308
21620471, 19670108, 19068610, 20267166, 25123585, 20476175, 28639299
18549238, 19297917, 20564072, 22950945, 19385656, 23528412, 19684504
19330795, 21174504, 28357401, 20899461, 20557786, 21911701, 19143550
20118035, 19024808, 25809524, 25760195, 20009833, 19604659, 16359751
26039623, 22820579, 28024793, 19928926, 23314180, 20212067, 24737403
20480209, 18904062, 29030780, 26430737, 25476125, 20856766, 17258582
27169796, 21668627, 26325856, 23272045, 20877664, 29247712, 19487147
23149541, 24577566, 19430401, 19676905, 28025414, 20925795, 26482376
22760679, 21296029, 21629064, 24416451, 23229229, 22865673, 20708701
25353983, 19280225, 21315084, 20613079, 19375649, 19213447, 19989009
18191823, 27314390, 26336977, 25775213, 30803210, 24393981, 22568016
27033652, 25639019, 17319928, 14705949, 19703301, 20308798, 28390273
21626377, 20122715, 6418158, 23105538, 25743479, 26198926, 28714988
19258504, 21188532, 24792678, 23151677, 17890099, 21649497, 26446098
16887946, 19693090, 26024732, 18791688, 19721304, 27012701, 19490948
29483672, 19619732, 21164318, 29559723, 21516611, 23148260, 18090142
21641760, 19818513, 22468781, 23002524, 20139391, 21052842, 24693382
19978542, 25477657, 23543183, 22165897, 19373893, 22359063, 19409212
18373438, 23035249, 21820934, 20677974, 18990693, 20470877, 19452434
21422580, 21632821, 22351572, 20235511, 23220453, 18742258, 18604493
23008056, 22901797, 18610915, 20978259, 20832516, 24801152, 27276231
26089440, 20907061, 25733479, 19523462, 18733351, 20505778, 19183343
21675340, 21787056, 21273804, 22782647, 20544065, 29719146, 25093739
17835294, 25210690, 28708023, 24413809, 27846298, 18371441, 26714910
24385983, 20413820, 22176950, 28986231, 24421668, 25897615, 25643931
23195445, 21281607, 20513399, 18841764, 28098160, 20558005, 20093776
18909599, 20618595, 23572982, 23104033, 19211433, 20331945, 19512341
23066146, 22256431, 19637186, 19022470, 22686674, 18607546, 26875822
24573817, 23115139, 19649152, 19201867, 21294938, 20898997, 18510194
21293600, 30218044, 21842740, 22454326, 24683149, 19534363, 25489607
23061702, 30805558, 30855121, 30502041, 30534664, 30128197, 30160639
22070866, 29774383, 29774367, 29251241, 29254615, 19165673, 28790654
28915933, 28440711, 28502128, 28502113, 27923320, 27952584, 27952577
27642235, 27475603, 27461789, 27461842, 25649873, 27001733, 27000663
27000690, 26635845, 26637592, 26570171, 26027162, 26023002, 26023025
25437695, 25494413, 25494379, 24917972, 25067795, 24534298, 25076732
25076756, 24315824, 21659726, 24448240, 24448282, 23177536, 22675136
23265914, 23265965, 23727148, 22674709, 22670413, 22670385, 21188537
22139226, 22118835, 22118851, 21555660, 21811517, 19623450, 21566993
21566944, 19176885, 21068507, 21047803, 21047766, 20415564, 20408829
20408866, 19877336, 19855285, 19909862, 19895362, 19895326, 19153980
19231857, 19223010, 19245191, 19699946, 28730253, 16799735, 17432124
18759211, 19396455, 20875898, 22037014, 22873635, 23614158, 24701840
25881255, 27015449, 28125601, 28852325, 29997937, 29997959, 17969866
20394750, 24835919, 23262847, 21171382, 21091901, 18727933, 18758877
18778801, 18803726, 18810904, 18895170, 18952766, 18999568, 19130152
19131386, 19131607, 19146474, 19168167, 19248279, 19313563, 19317646
19327391, 19364502, 19440520, 19448499, 19461428, 19468612, 19547774
19566592, 19571055, 19571082, 19583624, 19590877, 19632912, 19647503
19680796, 19701015, 19705781, 19769625, 19784751, 19799847, 19811709
19817386, 19824871, 19859472, 19880190, 19886165, 19889230, 19933147
19952975, 19982584, 19988852, 20009569, 20011646, 20011897, 20052269
20061399, 20233181, 20565112, 20565133, 20577490, 20703629, 20707932
20717091, 20800890, 20801783, 25031502
```

Version 12.1.0.2.v19

La version 12.1.0.2.v19 inclut les éléments suivants :

- Correctif 30340202 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS DE BASE DE DONNÉES 12.1.0.2.200114

- Correctif 30502041 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS OJVM 12.1.0.2.200114
- Correctif 29997937 : DSTv34 pour RDBMS (TZDATA2019G)
- Correctif 29997959 : DSTv34 pour OJVM (TZDATA2019G)
- Correctif 17969866 : Oracle GoldenGate – 46719 : ENH : PRISE EN CHARGE DE LA RÉPLICATION POUR LES INSERTIONS/MISES À JOUR COMPLÈTES AVEC DES VALEURS ÉLEVÉES
- Correctif 20394750 : Oracle GoldenGate – ÉCHEC DE L'APPLICATION DE LA RÉSOLUTION CDR POUR LES ÉLÉMENTS LOBS, XML, LONG et LES OBJETS
- Correctif 24835919 : Oracle GoldenGate – PANNE D'EXÉCUTION PAR IR DE TRANSACTIONS DEPENDANTES AVEC PARALLÉLISME DE TYPE SUPÉRIEUR À
- Correctif 23262847 : Oracle GoldenGate – RÉEXÉCUTION MAL EFFECTUÉE AYANT PROVOQUÉ UNE FIN ANORMALE DE LA RÉPLICATION OGG
- Correctif 21171382 : Correctif DBMS_STATS
- Correctif 21091901 : LE DÉPLACEMENT EN LIGNE LA PARTITION PAR HACHAGE OU PAR RÉFÉRENCE PEUT EMPÊCHER LA COHÉRENCE DES INDEX LOCAUX
- Correctif 30708149 : ensemble de correctifs JSON
- Correctif 20033733 : PART :IMC:HIT ORA 600 [KGL-HEAP-SIZE-EXCEEDED]
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS
- PreUpgrade Jar : preupgrade_12.1.0.2.0_18_crlf.zip

Correctif Oracle 29918340, publié en janvier 2020

Bogues corrigés :

```
19309466, 19902195, 18250893, 25437699, 19383839, 19781326, 16756406
18456643, 26546664, 22364044, 29483723, 18913440, 18845653, 19915271
20172151, 18417036, 19516448, 24907917, 23713236, 24796092, 23140259
29434301, 19243521, 19658708, 18272672, 21153266, 19174430, 18900107
22243719, 19548064, 26556014, 20493163, 20688221, 22346829, 21387964
13542050, 22072818, 22250006, 22734547, 22243983, 21623164, 19012119
21534893, 19932634, 19869255, 22232606, 18681056, 23324000, 25427662
22068305, 24589081, 19439759, 19303936, 18856106, 22916353, 24835538
22353346, 19790243, 21106027, 26444887, 20023340, 23088803, 22529728
26256131, 19134173, 18492302, 24303148, 21101873, 20447445, 27122162
21188584, 19390567, 26513709, 25780343, 19769480, 21097043, 21225209
26245237, 20677396, 19284031, 19450314, 23514911, 19016730, 22205263
22517782, 20919320, 22075064, 22551446, 29250317, 22721409, 18440095
22496904, 16439813, 18354830, 20596234, 22022760, 20936905, 22268833
23197103, 23746128, 22515353, 27897759, 21514877, 19809171, 21186167
26111842, 18990023, 13787015, 22492533, 22233505, 20173897, 24624166
17210525, 29707896, 21260431, 25579761, 20181030, 25056052, 19370504
21868720, 23068169, 19124589, 22690648, 21383171, 19402853, 19888853
25107334, 24341675, 17722075, 20882568, 25653109, 23026585, 18604692
20717081, 25546608, 20768076, 27370965, 19081128, 22173980, 25722055
23514710, 29483771, 19178851, 20951038, 22168163, 25161298, 20569094
24308635, 19791377, 19050649, 20920911, 29962939, 30365745, 22475617
19189525, 19060015, 19469538, 27052607, 29633753, 20598042, 22458049
18988834, 21159665, 23302839, 25307368, 25699321, 21924131, 17409174
21837606, 22729345, 22842151, 25051465, 19238590, 16941434, 20387265
29378913, 24397438, 20673810, 23108128, 20356733, 22380919, 18436647
21764119, 23065323, 20825533, 19124336, 22294260, 20839705, 24790914
20284155, 23571055, 6194865, 25539063, 17365043, 25914276, 20952966
22961508, 19176223, 21300341, 23237313, 18288842, 27223075, 22353199
20011515, 22083366, 27634991, 25670786, 28305362, 21419850, 26898563
22495673, 27986817, 19577410, 26248143, 23294548, 23101501, 24737064
```

```
19931709, 25423453, 25547060, 23533807, 27726780, 24600330, 28384353
20635353, 25600421, 18122373, 20043616, 23124895, 18856999, 21450666
18893947, 24752618, 26633558, 20076781, 26029780, 20926021, 21196809
21354456, 22533631, 23725036, 20464614, 19562381, 27375542, 24808595
19189317, 25669791, 18307021, 21917884, 19708632, 27213224, 25633101
29006527, 20711718, 18973548, 25982666, 25472885, 19718981, 20684983
23567857, 22826718, 25655390, 21773465, 20250147, 20144019, 19197175
26263721, 19597439, 21387128, 28867992, 22007324, 18818069, 21566639
19180770, 19879746, 21785691, 20539050, 20424183, 24285405, 21425496
26544823, 19957298, 20322560, 22228324, 29962927, 23172924, 22520320
29817278, 27751755, 21575362, 25058080, 22365117, 22645009, 25165496
28950969, 27433385, 18774543, 20124446, 21429602, 29189889, 26153977
19371175, 21863727, 18940497, 19074147, 22923409, 25489342, 21380789
19154375, 25417056, 19044962, 19532017, 19662635, 23080557, 22374754
20560611, 25654936, 21492036, 18705806, 28420042, 19578247, 20705577
22024071, 22238921, 22809871, 29645349, 21184223, 19995869, 23089357
19404068, 18921743, 19065677, 19018447, 19018206, 18308268, 19777862
29027694, 22223463, 19304354, 22519146, 22214989, 19445860, 26654363
27199245, 22977256, 20890311, 27445727, 21142837, 20869721, 22258530
24555417, 22179537, 21756699, 18801391, 20217801, 18819908, 19550902
22760595, 25483815, 19543384, 23628685, 25482971, 23007241, 19593445
30252098, 21080143, 27351628, 20582405, 24966594, 20031873, 29828111
25489367, 18618122, 24737581, 21698350, 22501616, 26784509, 28043157
19306797, 24739928, 18966843, 19077215, 20704450, 19068970, 20543011
19023822, 24713381, 22836801, 20432873, 21756677, 20328248, 18674047
18849537, 20087383, 25459958, 20315311, 29163567, 22897344, 27534509
26768025, 25178179, 19308965, 20686773, 18948177, 20764012, 27623159
19468991, 20868862, 21780146, 23315153, 20466628, 21756661, 20397490
19706965, 20302006, 24831514, 23240358, 22178855, 19032777, 20862087
19329654, 18974476, 20603378, 21275255, 20859910, 19307662, 26203182
21847223, 20281121, 22568797, 19075256, 28079127, 19076343, 28026866
29511611, 18866977, 22808310, 25635149, 20844426, 20904530, 20441797
20296619, 19831647, 18548246, 21442094, 25079710, 24674955, 18840932
18740837, 20294666, 21037923, 25602488, 21517440, 22062517, 19180394
27337759, 19174942, 27092508, 20671094, 21889720, 19347458, 19450116
18411216, 20117253, 24386767, 20641666, 24737954, 19931367, 25264559
19930276, 22092979, 25616268, 21625179, 20879709, 23003979, 20165574
28578164, 19272708, 19547370, 22624709, 23084507, 23184263, 20228093
21281532, 25093872, 19805359, 26324206, 19461270, 19434529, 18799063
20354900, 29388020, 20378086, 17008068, 21246723, 20831538, 20424899
20361671, 18674024, 19689979, 24411921, 19873610, 16619249, 20562898
21641414, 21091431, 19440586, 20001168, 22757364, 22175564, 22499356
20725343, 21241052, 19561643, 28199085, 20736227, 19399918, 19195895
20830459, 20017509, 18475439, 25790353, 21828126, 21665897, 25555252
20746251, 19315668, 22568177, 25764020, 25612095, 25357142, 23096938
19067244, 19943771, 18043064, 19941352, 21329301, 18885870, 26243698
26187943, 20324049, 19536415, 30164714, 23709062, 28174827, 20446883
27314206, 21299490, 25313154, 18628388, 21744290, 18254023, 27072923
25047724, 20591183, 27847259, 20459944, 19185876, 18548433, 27207110
22465352, 24385625, 24326444, 20402832, 19627012, 22733141, 29200700
20468401, 27441326, 27620950, 16863642, 19639483, 19315691, 27567477
21479753, 19174521, 23177923, 20401975, 18306996, 18851894, 21424824
27034890, 20581111, 20318889, 20936731, 21060755, 25240188, 26828994
22256560, 19188927, 23328639, 27229389, 20766180, 20229001, 24570598
25475853, 21172913, 17655240, 29379978, 21266085, 19028800, 19035573
19366375, 24523374, 28821847, 25599425, 25034396, 19289642, 21502702
21291274, 18007682, 23521523, 20475845, 29408136, 22148226, 22528741
25417958, 29500257, 24652769, 26088426, 19326908, 19597583, 17414008
23019710, 20897759, 26822620, 22046677, 19663176, 20938170, 19891090
24825843, 26318627, 21960504, 24509056, 20524085, 19054077, 21385422
26262953, 22657942, 20428621, 21899588, 23326313, 19723336, 19835133
17532734, 17495022, 25300427, 19333670, 21842017, 19285025, 21373473
29483626, 23260854, 23061453, 19687159, 14643995, 22146062, 20977794
20734332, 16938780, 17551063, 27548131, 21977392, 28612674, 24461826
19676012, 20588502, 23315889, 19520602, 23053606, 19841800, 20245930
19001359, 21476308, 26546754, 19393542, 23533524, 21099555, 27995248
```

```
17532729, 25429959, 19141838, 19644859, 21915719, 19908836, 21421886
19358317, 19524158, 27101105, 29869404, 23548817, 25861398, 20803014
23025340, 19335438, 19058490, 23642282, 19207117, 18799993, 25919622
26569225, 25986062, 20835241, 24662775, 19475971, 18967382, 20347562
20348653, 29009513, 19896336, 24812585, 20048359, 21896069, 20468490
19524384, 25392535, 21147908, 21695575, 30295478, 20440930, 25789277
19171086, 24718260, 17867700, 19791273, 26110632, 27397048, 21241829
19591608, 22707244, 18662619, 18419520, 22296366, 22654475, 18914624
19571367, 28636676, 21522582, 29893132, 19501299, 26007010, 19529868
20425790, 19708342, 27997875, 26968670, 16870214, 18202441, 24415926
18743542, 19001390, 21157728, 20657411, 19332396, 22606521, 21875360
21821302, 25091141, 28000269, 19149990, 20382309, 22855193, 16777441
19606174, 28542455, 20848335, 25495682, 19382851, 20528052, 22762046
24563422, 27468303, 23125826, 22503297, 28993590, 25192729, 23338911
22730454, 27274536, 19354794, 20757079, 19176326, 20298413, 19048007
22018363, 24300640, 18849970, 21532755, 20860659, 22905130, 26121990
21263635, 27710072, 23209741, 22160989, 18499088, 18775971, 22894949
21059919, 18952989, 27348081, 22518784, 25856821, 24457597, 25484507
20794034, 25885148, 20554364, 21061354, 19468347, 17533661, 19883092
20657441, 24401351, 21285458, 28023399, 18051556, 25330273, 26412540
24425998, 19699191, 24437510, 16875041, 20669434, 18964978, 23342170
22972770, 20828947, 21373076, 25492379, 25551676, 14283239, 25766822
21967197, 22922076, 19601762, 25575628, 26110259, 20368850, 21239530
20437153, 24848928, 20880215, 20798891, 25606091, 19013183, 25042823
21133343, 22695831, 24365589, 25248384, 25634317, 20134113, 19587324
20273319, 28501075, 18542562, 19017309, 26758193, 21063322, 22062026
20134339, 22077517, 22815955, 23854396, 24690216, 22507210, 16354467
20101006, 21795111, 27938623, 23501901, 18797519, 25997810, 23029562
25879984, 26844406, 21260397, 25029423, 19354335, 29726695, 19730508
22366558, 19390620, 26658759, 25822410, 6599380, 20717359, 24321547
27097854, 21297872, 18964939, 19871910, 29437712, 26366517, 21913183
25695903, 22366322, 20171986, 20603431, 21132297, 25957038, 21542577
22507234, 23170620, 24719736, 25600342, 18868646, 28587723, 29142109
26637824, 20627866, 18110491, 16923858, 24642295, 19518079, 20914870
19339555, 20466322, 25823754, 25110233, 20169408, 24908321, 20842388
17274537, 26575788, 20474192, 21644640, 28849751, 21794615, 18899974
20471920, 22806698, 19052488, 29944660, 29260956, 26198757, 19503821
23717151, 24350620, 23126410, 20074391, 19157754, 22495062, 21220620
24316947, 19865345, 19065556, 22816287, 25947799, 20878790, 23492665
21322887, 22305887, 19617921, 20879889, 24350831, 19578350, 28022101
26439748, 21893235, 19363645, 21072646, 20898391, 19291380, 27060167
18382302, 27086138, 22536802, 22087683, 21197626, 21656630, 20373598
19248799, 22707866, 28432129, 19155797, 19279273, 18886413, 25490238
20922010, 19990037, 25150925, 20509482, 20778986, 27255377, 24717859
20703000, 22862134, 21526048, 28683167, 24929210, 24560906, 20144308
21620471, 19670108, 19068610, 20267166, 25123585, 20476175, 18549238
28639299, 19297917, 20564072, 22950945, 19385656, 23528412, 19684504
19330795, 21174504, 28357401, 20899461, 20557786, 21911701, 19143550
20118035, 19024808, 25760195, 20009833, 19604659, 16359751, 26039623
22820579, 19928926, 23314180, 20212067, 24737403, 20480209, 18904062
29030780, 26430737, 20856766, 25476125, 17258582, 27169796, 21668627
23272045, 20877664, 26325856, 19487147, 23149541, 24577566, 19430401
19676905, 20925795, 26482376, 21296029, 21629064, 23229229, 22865673
20708701, 25353983, 19280225, 21315084, 20613079, 19375649, 19213447
19989009, 18191823, 27314390, 26336977, 25775213, 24393981, 22568016
25639019, 17319928, 14705949, 19703301, 28390273, 20308798, 21626377
20122715, 6418158, 23105538, 26198926, 25743479, 19258504, 28714988
21188532, 24792678, 23151677, 17890099, 21649497, 26446098, 16887946
26024732, 18791688, 19721304, 27012701, 19490948, 29483672, 19619732
21164318, 29559723, 21516611, 23148260, 18090142, 21641760, 19818513
22468781, 23002524, 20139391, 24693382, 19978542, 25477657, 23543183
22165897, 19373893, 22359063, 19409212, 18373438, 23035249, 21820934
20677974, 18990693, 20470877, 19452434, 21422580, 21632821, 22351572
20235511, 23220453, 18742258, 18604493, 23008056, 22901797, 18610915
20978259, 20832516, 24801152, 26089440, 27276231, 20907061, 25733479
19523462, 18733351, 20505778, 19183343, 21787056, 21273804, 22782647
```

```
20544065, 25093739, 17835294, 29719146, 25210690, 28708023, 24413809
27846298, 18371441, 26714910, 24385983, 20413820, 28986231, 24421668
25897615, 25643931, 23195445, 21281607, 20513399, 18841764, 28098160
20558005, 20093776, 18909599, 20618595, 23572982, 23104033, 19211433
20331945, 19512341, 23066146, 22256431, 19637186, 19022470, 22686674
18607546, 26875822, 24573817, 23115139, 19649152, 19201867, 21294938
20898997, 18510194, 21293600, 21842740, 22454326, 24683149, 19534363
25489607, 23061702
```

Version 12.1.0.2.v18

La version 12.1.0.2.v18 comprend les éléments suivants :

- Correctif 29918340 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS DE BASE DE DONNÉES 12.1.0.2.191015
- Correctif 30128197 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS OJVM 12.1.0.2.191015
- Correctif 29997937 : DSTv34 pour RDBMS (TZDATA2019G)
- Correctif 29997959 : DSTv34 pour OJVM (TZDATA2019G)
- Correctif 17969866 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 20394750 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 24835919 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 21171382 : Correctif DBMS_STATS
- Correctif 21091901 : LE DÉPLACEMENT EN LIGNE LA PARTITION PAR HACHAGE OU PAR RÉFÉRENCE PEUT EMPÊCHER LA COHÉRENCE DES INDEX LOCAUX
- Correctif 30370890 : ensemble de correctifs JSON
- Correctif 20033733 : PART :IMC:HIT ORA 600 [KGL-HEAP-SIZE-EXCEEDED]
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS
- PreUpgrade Jar : preupgrade_12.1.0.2.0_18_crlf.zip
- Prise en charge de Redimensionnement de l'espace de table temporaire dans un réplica en lecture (p. 1128)

Correctif Oracle 29918340, publié en octobre 2019

Bogues corrigés :

```
19309466, 19902195, 18250893, 25437699, 19383839, 19781326, 16756406
18456643, 26546664, 22364044, 29483723, 18845653, 18913440, 19915271
20172151, 18417036, 19516448, 24907917, 23713236, 24796092, 23140259
19243521, 19658708, 18272672, 21153266, 19174430, 18900107, 22243719
19548064, 26556014, 20493163, 20688221, 22346829, 21387964, 13542050
22072818, 22250006, 22734547, 22243983, 21623164, 19012119, 19932634
19869255, 22232606, 18681056, 23324000, 25427662, 22068305, 24589081
19439759, 19303936, 22916353, 24835538, 22353346, 19790243, 21106027
26444887, 23088803, 22529728, 26256131, 19134173, 24303148, 21101873
20447445, 27122162, 21188584, 19390567, 26513709, 25780343, 19769480
21097043, 21225209, 26245237, 20677396, 19284031, 19450314, 19016730
23514911, 22205263, 22517782, 20919320, 22075064, 22551446, 29250317
22721409, 18440095, 22496904, 16439813, 18354830, 20596234, 22022760
20936905, 22268833, 23197103, 22515353, 23746128, 21514877, 19809171
21186167, 26111842, 18990023, 13787015, 22492533, 22233505, 20173897
24624166, 17210525, 21260431, 29707896, 25579761, 20181030, 25056052
```

```
19370504, 21868720, 23068169, 19124589, 22690648, 21383171, 19402853
19888853, 25107334, 24341675, 17722075, 20882568, 25653109, 23026585
18604692, 20717081, 25546608, 20768076, 27370965, 19081128, 22173980
25722055, 23514710, 19178851, 20951038, 22168163, 25161298, 20569094
24308635, 19791377, 19050649, 20920911, 22475617, 19189525, 19469538
27052607, 20598042, 29633753, 22458049, 18988834, 21159665, 23302839
25307368, 25699321, 21924131, 17409174, 22729345, 22842151, 25051465
19238590, 16941434, 20387265, 29378913, 24397438, 20673810, 23108128
20356733, 22380919, 18436647, 23065323, 20825533, 19124336, 22294260
24790914, 20284155, 23571055, 6194865, 25539063, 17365043, 25914276
20952966, 22961508, 19176223, 21300341, 23237313, 18288842, 27223075
22353199, 20011515, 22083366, 27634991, 25670786, 21419850, 26898563
27986817, 19577410, 22495673, 26248143, 23294548, 23101501, 24737064
19931709, 25423453, 25547060, 23533807, 27726780, 24600330, 28384353
25600421, 18122373, 20043616, 23124895, 18856999, 21450666, 18893947
26633558, 20076781, 26029780, 21196809, 21354456, 22533631, 23725036
20464614, 19562381, 27375542, 24808595, 19189317, 25669791, 18307021
21917884, 19708632, 27213224, 25633101, 29006527, 20711718, 18973548
25982666, 19718981, 20684983, 23567857, 22826718, 25655390, 21773465
20250147, 20144019, 19197175, 26263721, 19597439, 21387128, 22007324
18818069, 21566639, 19180770, 19879746, 21785691, 20424183, 20539050
24285405, 21425496, 26544823, 19957298, 20322560, 22228324, 23172924
22520320, 27751755, 21575362, 25058080, 22365117, 22645009, 25165496
28950969, 18774543, 20124446, 21429602, 29189889, 26153977, 19371175
21863727, 18940497, 19074147, 22923409, 25489342, 21380789, 19154375
25417056, 19044962, 19532017, 19662635, 22374754, 20560611, 25654936
21492036, 18705806, 28420042, 19578247, 22024071, 22238921, 22809871
21184223, 19995869, 23089357, 19404068, 18921743, 19065677, 19018447
19018206, 18308268, 19777862, 29027694, 22223463, 19304354, 22519146
22214989, 19445860, 26654363, 27199245, 22977256, 20890311, 27445727
21142837, 20869721, 24555417, 22258530, 22179537, 21756699, 18801391
20217801, 18819908, 22760595, 19550902, 25483815, 23628685, 19543384
25482971, 23007241, 19593445, 21080143, 27351628, 20582405, 24966594
20031873, 25489367, 29828111, 18618122, 24737581, 21698350, 22501616
26784509, 24739928, 18966843, 19077215, 20704450, 19068970, 20543011
19023822, 24713381, 22836801, 20432873, 21756677, 20328248, 18674047
18849537, 20087383, 25459958, 20315311, 22897344, 29163567, 27534509
26768025, 25178179, 19308965, 18948177, 20764012, 27623159, 19468991
20868862, 21780146, 23315153, 20466628, 21756661, 20397490, 19706965
20302006, 24831514, 23240358, 22178855, 19032777, 20862087, 19329654
18974476, 20603378, 20859910, 19307662, 26203182, 21847223, 20281121
22568797, 19075256, 19076343, 28026866, 29511611, 18866977, 22808310
25635149, 20844426, 20904530, 20441797, 20296619, 18548246, 21442094
25079710, 24674955, 18840932, 18740837, 20294666, 21037923, 25602488
21517440, 22062517, 19180394, 27337759, 19174942, 20671094, 21889720
19347458, 19450116, 18411216, 20117253, 24386767, 20641666, 19931367
25264559, 19930276, 22092979, 25616268, 21625179, 20879709, 23003979
20165574, 28578164, 19272708, 19547370, 22624709, 23084507, 23184263
20228093, 21281532, 25093872, 19805359, 26324206, 19461270, 19434529
18799063, 20354900, 29388020, 20378086, 17008068, 21246723, 20831538
20424899, 20361671, 18674024, 19689979, 24411921, 19873610, 16619249
20562898, 21641414, 21091431, 19440586, 20001168, 22757364, 22175564
22499356, 20725343, 21241052, 19561643, 28199085, 20736227, 19399918
19195895, 20830459, 20017509, 18475439, 25790353, 21828126, 21665897
25555252, 20746251, 22568177, 25764020, 25612095, 25357142, 23096938
19067244, 18043064, 19941352, 21329301, 18885870, 26243698, 26187943
20324049, 19536415, 23709062, 28174827, 20446883, 27314206, 21299490
25313154, 18628388, 21744290, 18254023, 27072923, 25047724, 20591183
27847259, 20459944, 19185876, 18548433, 27207110, 22465352, 24385625
24326444, 20402832, 19627012, 22733141, 29200700, 20468401, 27441326
27620950, 16863642, 19639483, 19315691, 27567477, 21479753, 19174521
23177923, 20401975, 18306996, 18851894, 27034890, 21424824, 20581111
20318889, 20936731, 21060755, 25240188, 26828994, 22256560, 19188927
23328639, 27229389, 20766180, 20229001, 24570598, 25475853, 21172913
17655240, 29379978, 21266085, 19028800, 19035573, 19366375, 24523374
25599425, 25034396, 19289642, 21502702, 21291274, 18007682, 23521523
```

```
20475845, 29408136, 22148226, 22528741, 25417958, 24652769, 26088426
19326908, 19597583, 29500257, 17414008, 23019710, 20897759, 26822620
22046677, 19663176, 20938170, 19891090, 24825843, 26318627, 21960504
24509056, 19054077, 21385422, 26262953, 22657942, 20428621, 21899588
23326313, 19723336, 19835133, 17532734, 17495022, 25300427, 19333670
21842017, 19285025, 21373473, 23260854, 23061453, 19687159, 14643995
22146062, 20977794, 20734332, 17551063, 16938780, 27548131, 21977392
28612674, 24461826, 19676012, 20588502, 23315889, 19520602, 23053606
19841800, 20245930, 19001359, 21476308, 26546754, 19393542, 23533524
21099555, 27995248, 25429959, 19141838, 19644859, 21915719, 19908836
21421886, 19358317, 19524158, 23548817, 25861398, 20803014, 23025340
19335438, 19058490, 23642282, 19207117, 18799993, 25919622, 26569225
25986062, 20835241, 24662775, 19475971, 18967382, 20347562, 20348653
19896336, 24812585, 20048359, 21896069, 20468490, 19524384, 25392535
21147908, 21695575, 20440930, 30295478, 25789277, 19171086, 24718260
17867700, 19791273, 27397048, 21241829, 19591608, 22707244, 18419520
22296366, 22654475, 18914624, 19571367, 28636676, 21522582, 19501299
29893132, 26007010, 19529868, 20425790, 19708342, 27997875, 16870214
18202441, 24415926, 18743542, 19001390, 21157728, 20657411, 19332396
22606521, 21875360, 25091141, 21821302, 28000269, 19149990, 20382309
22855193, 16777441, 19606174, 20848335, 28542455, 25495682, 19382851
20528052, 22762046, 24563422, 23125826, 22503297, 28993590, 25192729
23338911, 22730454, 19354794, 20757079, 19176326, 20298413, 19048007
22018363, 18849970, 21532755, 24300640, 20860659, 22905130, 26121990
21263635, 27710072, 23209741, 22160989, 18499088, 18775971, 22894949
21059919, 18952989, 27348081, 22518784, 25856821, 24457597, 25484507
20794034, 20554364, 21061354, 19468347, 17533661, 19883092, 20657441
24401351, 21285458, 28023399, 18051556, 25330273, 26412540, 24425998
19699191, 24437510, 16875041, 20669434, 18964978, 22972770, 23342170
20828947, 21373076, 25492379, 25551676, 14283239, 25766822, 21967197
22922076, 19601762, 25575628, 26110259, 20368850, 21239530, 20437153
24848928, 20880215, 20798891, 25606091, 19013183, 25042823, 21133343
22695831, 24365589, 25248384, 25634317, 20134113, 19587324, 20273319
28501075, 18542562, 19017309, 26758193, 21063322, 22062026, 20134339
22077517, 22815955, 23854396, 24690216, 22507210, 16354467, 20101006
21795111, 27938623, 23501901, 18797519, 25997810, 23029562, 25879984
21260397, 25029423, 26844406, 19354335, 19730508, 22366558, 19390620
26658759, 25822410, 6599380, 20717359, 24321547, 27097854, 21297872
18964939, 19871910, 29437712, 26366517, 21913183, 25695903, 22366322
20171986, 20603431, 21132297, 25957038, 21542577, 22507234, 23170620
24719736, 25600342, 18868646, 28587723, 29142109, 26637824, 20627866
18110491, 16923858, 24642295, 19518079, 19339555, 20466322, 25823754
25110233, 20169408, 24908321, 20842388, 17274537, 26575788, 20474192
21644640, 28849751, 21794615, 18899974, 20471920, 22806698, 19052488
26198757, 19503821, 23717151, 24350620, 23126410, 20074391, 19157754
22495062, 21220620, 24316947, 19865345, 19065556, 22816287, 25947799
20878790, 23492665, 21322887, 22305887, 20879889, 19617921, 24350831
19578350, 28022101, 26439748, 21893235, 19363645, 21072646, 20898391
19291380, 27060167, 18382302, 27086138, 22536802, 22087683, 21197626
21656630, 20373598, 19248799, 22707866, 28432129, 19155797, 19279273
18886413, 25490238, 20922010, 19990037, 25150925, 20509482, 20778986
27255377, 24717859, 20703000, 22862134, 21526048, 28683167, 24929210
24560906, 20144308, 21620471, 19670108, 19068610, 20267166, 25123585
20476175, 18549238, 19297917, 22950945, 19385656, 20564072, 23528412
19684504, 19330795, 21174504, 28357401, 20899461, 20557786, 21911701
19143550, 20118035, 19024808, 25760195, 20009833, 19604659, 16359751
26039623, 22820579, 19928926, 23314180, 20212067, 24737403, 20480209
18904062, 29030780, 26430737, 20856766, 17258582, 27169796, 21668627
23272045, 20877664, 19487147, 23149541, 24577566, 19430401, 19676905
20925795, 26482376, 21296029, 21629064, 23229229, 22865673, 20708701
25353983, 19280225, 21315084, 20613079, 19375649, 19213447, 19989009
18191823, 27314390, 26336977, 25775213, 24393981, 22568016, 25639019
17319928, 14705949, 19703301, 28390273, 21626377, 20122715, 6418158
23105538, 26198926, 19258504, 21188532, 24792678, 23151677, 17890099
21649497, 26446098, 16887946, 26024732, 18791688, 19721304, 27012701
19490948, 29483672, 19619732, 21164318, 29559723, 23148260, 18090142
```

```
21641760, 19818513, 23002524, 22468781, 20139391, 24693382, 19978542
25477657, 23543183, 22165897, 19373893, 22359063, 19409212, 18373438
23035249, 20677974, 18990693, 20470877, 21422580, 21632821, 22351572
20235511, 23220453, 18742258, 18604493, 23008056, 22901797, 18610915
20978259, 20832516, 24801152, 26089440, 20907061, 19523462, 25733479
20505778, 18733351, 19183343, 21787056, 21273804, 22782647, 20544065
25093739, 17835294, 28708023, 24413809, 27846298, 18371441, 26714910
24385983, 20413820, 28986231, 24421668, 25897615, 25643931, 23195445
21281607, 20513399, 18841764, 20558005, 20093776, 18909599, 20618595
23572982, 23104033, 19211433, 20331945, 19512341, 22256431, 19637186
23066146, 19022470, 22686674, 18607546, 26875822, 24573817, 23115139
19649152, 19201867, 21294938, 20898997, 18510194, 21293600, 21842740
22454326, 24683149, 19534363, 25489607, 23061702
```

Version 12.1.0.2.v17

La version 12.1.0.2.v17 comprend les éléments suivants :

- Correctif 29494060 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS DATABASE 12.1.0.2.190716
- Correctif 29774383 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS OJVM 12.1.0.2.190716
- Correctif 28852325 : DSTv33 pour RDBMS (TZDATA2018G)
- Correctif 28852334 : DSTv33 pour OJVM (TZDATA2018G)
- Correctif 17969866 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 20394750 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 24835919 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 21171382 : Correctif DBMS_STATS
- Correctif 21091901 : LE DÉPLACEMENT EN LIGNE LA PARTITION PAR HACHAGE OU PAR RÉFÉRENCE PEUT EMPÊCHER LA COHÉRENCE DES INDEX LOCAUX
- Correctif 29958796 : ensemble de correctifs JSON
- Correctif 20033733 : PART :IMC:HIT ORA 600 [KGL-HEAP-SIZE-EXCEEDED]
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS

Correctif Oracle 29494060, publié en juillet 2019

Bogues corrigés :

```
19309466, 19902195, 18250893, 25437699, 19383839, 19781326, 16756406
18456643, 26546664, 22364044, 18845653, 19915271, 20172151, 18417036
19516448, 23713236, 24907917, 24796092, 23140259, 19243521, 19658708
18272672, 21153266, 19174430, 22243719, 19548064, 26556014, 20493163
20688221, 21387964, 13542050, 22250006, 22734547, 22243983, 21623164
19012119, 19932634, 19869255, 22232606, 18681056, 23324000, 25427662
22068305, 24589081, 19439759, 19303936, 22916353, 24835538, 22353346
19790243, 21106027, 26444887, 23088803, 22529728, 26256131, 19134173
24303148, 20447445, 21101873, 21188584, 19390567, 26513709, 25780343
19769480, 21097043, 21225209, 26245237, 20677396, 19284031, 19450314
19016730, 22517782, 20919320, 22205263, 22075064, 22551446, 22721409
18440095, 22496904, 16439813, 18354830, 20596234, 22022760, 20936905
23197103, 22515353, 21514877, 19809171, 21186167, 26111842, 18990023
13787015, 22492533, 20173897, 24624166, 17210525, 21260431, 20181030
25056052, 19370504, 21868720, 23068169, 19124589, 21383171, 19402853
22690648, 19888853, 24341675, 17722075, 25107334, 20882568, 25653109
23026585, 18604692, 20717081, 25546608, 27370965, 19081128, 20768076
```

```
22173980, 25722055, 23514710, 19178851, 20951038, 22168163, 25161298
20569094, 24308635, 19791377, 19050649, 20920911, 22475617, 19189525
19469538, 27052607, 20598042, 22458049, 18988834, 21159665, 23302839
25307368, 25699321, 17409174, 22729345, 22842151, 19238590, 25051465
16941434, 20387265, 24397438, 29378913, 20673810, 23108128, 20356733
22380919, 18436647, 23065323, 20825533, 19124336, 22294260, 24790914
20284155, 23571055, 25539063, 17365043, 25914276, 20952966, 22961508
19176223, 21300341, 23237313, 18288842, 27223075, 22353199, 20011515
22083366, 27634991, 25670786, 21419850, 26898563, 27986817, 19577410
26248143, 23294548, 23101501, 24737064, 19931709, 25423453, 25547060
23533807, 27726780, 24600330, 25600421, 18122373, 20043616, 23124895
18856999, 21450666, 18893947, 26633558, 20076781, 26029780, 21196809
21354456, 22533631, 23725036, 20464614, 19562381, 27375542, 24808595
19189317, 25669791, 18307021, 21917884, 19708632, 27213224, 25633101
29006527, 20711718, 18973548, 25982666, 19718981, 23567857, 22826718
25655390, 20684983, 21773465, 20250147, 20144019, 19197175, 26263721
19597439, 21387128, 22007324, 19180770, 18818069, 21566639, 19879746
21785691, 20424183, 24285405, 21425496, 26544823, 20322560, 22228324
23172924, 22520320, 27751755, 21575362, 25058080, 22365117, 22645009
25165496, 28950969, 18774543, 20124446, 21429602, 26153977, 29189889
19371175, 21863727, 18940497, 19074147, 22923409, 25489342, 21380789
19154375, 19044962, 25417056, 19532017, 19662635, 22374754, 20560611
25654936, 21492036, 18705806, 28420042, 19578247, 22024071, 22238921
22809871, 21184223, 19995869, 23089357, 19404068, 18921743, 19065677
19018447, 19018206, 18308268, 19777862, 29027694, 22223463, 19304354
22519146, 19445860, 26654363, 27199245, 22977256, 20890311, 27445727
21142837, 20869721, 24555417, 22179537, 21756699, 20217801, 18819908
22760595, 25483815, 23628685, 23007241, 19593445, 21080143, 27351628
20582405, 24966594, 20031873, 25489367, 18618122, 24737581, 21698350
26784509, 24739928, 18966843, 19077215, 20704450, 19068970, 20543011
19023822, 24713381, 20432873, 21756677, 22836801, 20328248, 18674047
18849537, 20087383, 25459958, 20315311, 22897344, 27534509, 25178179
19308965, 18948177, 19468991, 20868862, 21780146, 23315153, 20466628
21756661, 20397490, 19706965, 20302006, 24831514, 23240358, 22178855
19032777, 20862087, 19329654, 18974476, 20603378, 20859910, 19307662
26203182, 21847223, 20281121, 22568797, 19075256, 19076343, 18866977
28026866, 29511611, 22808310, 25635149, 20844426, 20904530, 20441797
21442094, 25079710, 24674955, 18840932, 18740837, 20294666, 25602488
21517440, 22062517, 19180394, 27337759, 19174942, 20671094, 21889720
19450116, 18411216, 20117253, 24386767, 20641666, 19931367, 25264559
19930276, 22092979, 25616268, 21625179, 20879709, 23003979, 20165574
28578164, 19272708, 19547370, 22624709, 23084507, 23184263, 20228093
21281532, 25093872, 19805359, 26324206, 19461270, 19434529, 18799063
20354900, 20378086, 29388020, 17008068, 21246723, 20831538, 20424899
20361671, 18674024, 19689979, 24411921, 19873610, 16619249, 20562898
21641414, 21091431, 19440586, 20001168, 22757364, 22175564, 20725343
21241052, 19561643, 20736227, 19399918, 19195895, 20830459, 20017509
18475439, 25790353, 21828126, 21665897, 25555252, 20746251, 22568177
25764020, 25612095, 25357142, 23096938, 19067244, 18043064, 21329301
18885870, 26243698, 26187943, 20324049, 19536415, 23709062, 28174827
20446883, 27314206, 21299490, 25313154, 18628388, 21744290, 18254023
25047724, 20591183, 27847259, 19185876, 18548433, 27207110, 22465352
24385625, 24326444, 20402832, 19627012, 29200700, 20468401, 27441326
27620950, 16863642, 19639483, 19315691, 27567477, 21479753, 19174521
23177923, 20401975, 18306996, 18851894, 27034890, 20581111, 20318889
20936731, 21060755, 25240188, 26828994, 22256560, 19188927, 23328639
27229389, 20766180, 20229001, 24570598, 25475853, 21172913, 17655240
21266085, 19028800, 29379978, 19035573, 19366375, 24523374, 25599425
25034396, 19289642, 21502702, 21291274, 18007682, 23521523, 20475845
29408136, 22148226, 22528741, 25417958, 24652769, 26088426, 19326908
19597583, 17414008, 23019710, 20897759, 26822620, 22046677, 19663176
20938170, 19891090, 24825843, 26318627, 21960504, 24509056, 19054077
26262953, 22657942, 20428621, 21899588, 23326313, 19723336, 19835133
17532734, 25300427, 19333670, 17495022, 21842017, 19285025, 21373473
23260854, 23061453, 19687159, 14643995, 20977794, 20734332, 17551063
27548131, 21977392, 24461826, 28612674, 19676012, 20588502, 23315889
```

```
19520602, 23053606, 19841800, 20245930, 19001359, 21476308, 26546754
19393542, 23533524, 21099555, 27995248, 25429959, 19141838, 19644859
21915719, 19908836, 21421886, 19358317, 19524158, 23548817, 25861398
20803014, 23025340, 19335438, 19058490, 23642282, 19207117, 18799993
25919622, 26569225, 25986062, 20835241, 24662775, 19475971, 18967382
20347562, 20348653, 19896336, 24812585, 20048359, 21896069, 20468490
19524384, 25392535, 21147908, 21695575, 20440930, 25789277, 19171086
24718260, 17867700, 19791273, 27397048, 21241829, 19591608, 22707244
18419520, 22296366, 22654475, 18914624, 19571367, 28636676, 21522582
19501299, 26007010, 19529868, 20425790, 19708342, 27997875, 16870214
18202441, 24415926, 18743542, 19001390, 21157728, 20657411, 19332396
21875360, 22606521, 25091141, 28000269, 19149990, 20382309, 22855193
16777441, 19606174, 20848335, 25495682, 19382851, 20528052, 22762046
24563422, 23125826, 22503297, 28993590, 25192729, 23338911, 22730454
19354794, 20757079, 19176326, 20298413, 19048007, 22018363, 18849970
21532755, 20860659, 22905130, 26121990, 21263635, 27710072, 22160989
23209741, 18499088, 22894949, 21059919, 18952989, 27348081, 22518784
25856821, 24457597, 25484507, 20794034, 21061354, 20554364, 19468347
17533661, 19883092, 20657441, 24401351, 21285458, 28023399, 18051556
25330273, 26412540, 19699191, 24437510, 16875041, 20669434, 18964978
22972770, 20828947, 21373076, 25492379, 25551676, 14283239, 25766822
21967197, 22922076, 25575628, 19601762, 26110259, 20368850, 21239530
20437153, 24848928, 20880215, 20798891, 25606091, 19013183, 25042823
21133343, 22695831, 24365589, 25248384, 25634317, 20134113, 19587324
20273319, 28501075, 18542562, 19017309, 26758193, 21063322, 22062026
20134339, 22077517, 22815955, 23854396, 24690216, 22507210, 16354467
20101006, 21795111, 27938623, 23501901, 18797519, 25997810, 25879984
21260397, 25029423, 19354335, 19730508, 22366558, 26658759, 25822410
6599380, 20717359, 24321547, 27097854, 21297872, 18964939, 19871910
29437712, 26366517, 21913183, 22366322, 20171986, 25695903, 20603431
21132297, 25957038, 21542577, 22507234, 23170620, 24719736, 25600342
18868646, 28587723, 29142109, 26637824, 20627866, 18110491, 16923858
24642295, 19518079, 19339555, 20466322, 25823754, 25110233, 20169408
24908321, 20842388, 17274537, 26575788, 20474192, 21644640, 28849751
21794615, 18899974, 20471920, 22806698, 19052488, 26198757, 19503821
24350620, 20074391, 19157754, 21220620, 22495062, 24316947, 19865345
19065556, 22816287, 25947799, 20878790, 23492665, 21322887, 22305887
20879889, 24350831, 19578350, 28022101, 26439748, 21893235, 19363645
21072646, 20898391, 19291380, 27060167, 18382302, 27086138, 22536802
22087683, 21197626, 21656630, 20373598, 19248799, 22707866, 28432129
19155797, 19279273, 18886413, 25490238, 20922010, 19990037, 25150925
20509482, 27255377, 24717859, 20703000, 22862134, 21526048, 28683167
24929210, 24560906, 20144308, 21620471, 19670108, 19068610, 20267166
25123585, 20476175, 18549238, 19297917, 22950945, 19385656, 23528412
19684504, 19330795, 21174504, 28357401, 20899461, 20557786, 21911701
19143550, 20118035, 19024808, 25760195, 20009833, 19604659, 16359751
26039623, 22820579, 19928926, 23314180, 20212067, 24737403, 20480209
18904062, 29030780, 26430737, 20856766, 17258582, 27169796, 21668627
20877664, 23272045, 19487147, 23149541, 24577566, 19430401, 19676905
20925795, 26482376, 21296029, 21629064, 23229229, 22865673, 20708701
25353983, 19280225, 21315084, 20613079, 19375649, 19213447, 19989009
18191823, 27314390, 26336977, 25775213, 24393981, 25639019, 17319928
14705949, 19703301, 28390273, 21626377, 20122715, 6418158, 23105538
26198926, 19258504, 21188532, 23151677, 24792678, 17890099, 21649497
26446098, 16887946, 26024732, 18791688, 19721304, 27012701, 19490948
19619732, 21164318, 23148260, 18090142, 21641760, 19818513, 23002524
20139391, 24693382, 19978542, 23543183, 22165897, 19373893, 22359063
19409212, 18373438, 23035249, 20677974, 18990693, 20470877, 21422580
21632821, 22351572, 20235511, 23220453, 18742258, 18604493, 23008056
22901797, 18610915, 20978259, 20832516, 24801152, 26089440, 20907061
19523462, 20505778, 19183343, 21787056, 21273804, 22782647, 25093739
17835294, 28708023, 24413809, 27846298, 18371441, 26714910, 24385983
20413820, 24421668, 28986231, 25897615, 25643931, 23195445, 21281607
20513399, 20558005, 20093776, 18909599, 20618595, 23572982, 19211433
20331945, 19512341, 22256431, 19637186, 19022470, 18607546, 26875822
24573817, 23115139, 19649152, 19201867, 21294938, 20898997, 18510194
```

```
21842740, 22454326, 24683149, 19534363, 25489607, 23061702
```

Version 12.1.0.2.v16

La version 12.1.0.2.v16 comprend les éléments suivants :

- Correctif 29141015 : Mise à jour d'ensemble de correctifs de base de données : 12.1.0.2.190416
- Correctif 29251241 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS OJVM 12.1.0.2.190416
- Correctif 28852325 : DSTv33 pour RDBMS (TZDATA2018G)
- Correctif 28852334 : DSTv33 pour OJVM (TZDATA2018G)
- Correctif 17969866 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 20394750 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 24835919 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 21171382 : Correctif DBMS_STATS
- Correctif 21091901 : LE DÉPLACEMENT EN LIGNE LA PARTITION PAR HACHAGE OU PAR RÉFÉRENCE PEUT EMPÊCHER LA COHÉRENCE DES INDEX LOCAUX
- Correctif 29600862 : ensemble de correctifs JSON
- Correctif 20033733 : PART :IMC:HIT ORA 600 [KGL-HEAP-SIZE-EXCEEDED]
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS

Correctif Oracle 22785785, publié en avril 2019

Bogues corrigés :

```
19309466, 19902195, 18250893, 25437699, 19383839, 19781326, 16756406
18456643, 26546664, 22364044, 18845653, 19915271, 20172151, 18417036
19516448, 23713236, 24796092, 23140259, 19243521, 19658708, 18272672
21153266, 19174430, 22243719, 26556014, 20493163, 20688221, 21387964
13542050, 22734547, 22243983, 21623164, 19012119, 19932634, 19869255
22232606, 18681056, 23324000, 25427662, 22068305, 24589081, 19439759
19303936, 22916353, 24835538, 22353346, 21106027, 19790243, 26444887
23088803, 22529728, 26256131, 19134173, 20447445, 21188584, 19390567
26513709, 25780343, 19769480, 21097043, 21225209, 26245237, 20677396
19284031, 19450314, 19016730, 20919320, 22517782, 22075064, 22551446
22721409, 18440095, 22496904, 16439813, 18354830, 20596234, 22022760
20936905, 23197103, 21514877, 21186167, 26111842, 18990023, 13787015
22492533, 20173897, 24624166, 17210525, 21260431, 20181030, 25056052
19370504, 21868720, 23068169, 19124589, 21383171, 19402853, 19888853
24341675, 17722075, 20882568, 25653109, 23026585, 18604692, 20717081
25546608, 27370965, 19081128, 22173980, 23514710, 25722055, 19178851
20951038, 22168163, 25161298, 20569094, 24308635, 19791377, 19050649
20920911, 22475617, 19189525, 19469538, 27052607, 20598042, 22458049
18988834, 23302839, 25307368, 17409174, 22729345, 22842151, 19238590
16941434, 20387265, 24397438, 20673810, 23108128, 20356733, 22380919
18436647, 23065323, 20825533, 19124336, 22294260, 24790914, 20284155
23571055, 25539063, 17365043, 25914276, 20952966, 22961508, 19176223
21300341, 23237313, 18288842, 27223075, 22353199, 20011515, 22083366
25670786, 27634991, 21419850, 26898563, 19577410, 27986817, 26248143
23294548, 24737064, 23101501, 19931709, 25423453, 25547060, 23533807
27726780, 24600330, 25600421, 18122373, 20043616, 23124895, 18856999
21450666, 18893947, 26633558, 20076781, 26029780, 21196809, 21354456
23725036, 20464614, 22533631, 19562381, 27375542, 24808595, 19189317
```

```
25669791, 18307021, 21917884, 19708632, 27213224, 25633101, 20711718
29006527, 18973548, 25982666, 19718981, 23567857, 22826718, 25655390
21773465, 20250147, 20144019, 19197175, 26263721, 19597439, 21387128
22007324, 19180770, 19879746, 21785691, 20424183, 24285405, 26544823
20322560, 22228324, 23172924, 22520320, 21575362, 27751755, 25058080
22365117, 22645009, 25165496, 28950969, 18774543, 20124446, 21429602
26153977, 19371175, 21863727, 18940497, 19074147, 22923409, 25489342
21380789, 19154375, 19044962, 19532017, 19662635, 22374754, 20560611
25654936, 21492036, 18705806, 28420042, 19578247, 22024071, 22238921
22809871, 21184223, 19995869, 23089357, 19404068, 18921743, 19065677
19018447, 19018206, 18308268, 19777862, 22223463, 19304354, 29027694
22519146, 27199245, 19445860, 26654363, 22977256, 20890311, 27445727
21142837, 20869721, 24555417, 22179537, 21756699, 20217801, 18819908
22760595, 25483815, 23628685, 23007241, 19593445, 21080143, 27351628
20582405, 20031873, 25489367, 18618122, 24737581, 26784509, 24739928
18966843, 19077215, 20704450, 19068970, 20543011, 19023822, 24713381
20432873, 21756677, 20328248, 18674047, 18849537, 20087383, 25459958
20315311, 22897344, 27534509, 25178179, 19308965, 18948177, 19468991
20868862, 21780146, 23315153, 20466628, 21756661, 20397490, 19706965
20302006, 24831514, 23240358, 22178855, 19032777, 20862087, 19329654
18974476, 20603378, 20859910, 19307662, 21847223, 20281121, 22568797
19075256, 19076343, 18866977, 22808310, 25635149, 20844426, 20904530
20441797, 21442094, 25079710, 24674955, 18840932, 18740837, 20294666
25602488, 21517440, 22062517, 27337759, 19174942, 19180394, 20671094
21889720, 18411216, 20117253, 24386767, 20641666, 25264559, 22092979
25616268, 21625179, 20879709, 23003979, 20165574, 28578164, 19272708
19547370, 22624709, 23084507, 23184263, 20228093, 21281532, 25093872
19805359, 19461270, 26324206, 19434529, 18799063, 20378086, 17008068
21246723, 20831538, 20424899, 20361671, 18674024, 19689979, 24411921
19873610, 16619249, 20562898, 21641414, 21091431, 19440586, 22757364
20001168, 22175564, 20725343, 21241052, 19561643, 20736227, 19399918
19195895, 20830459, 20017509, 18475439, 25790353, 21828126, 21665897
25555252, 20746251, 22568177, 25764020, 25612095, 25357142, 23096938
19067244, 18043064, 21329301, 18885870, 26243698, 26187943, 20324049
19536415, 23709062, 28174827, 20446883, 27314206, 21299490, 25313154
18628388, 21744290, 18254023, 25047724, 20591183, 27847259, 19185876
27207110, 22465352, 24385625, 24326444, 20402832, 19627012, 20468401
27441326, 27620950, 16863642, 19639483, 19315691, 27567477, 21479753
19174521, 20401975, 18306996, 18851894, 27034890, 20581111, 20318889
20936731, 21060755, 25240188, 26828994, 22256560, 19188927, 27229389
20766180, 20229001, 24570598, 25475853, 21172913, 17655240, 21266085
19028800, 19035573, 19366375, 24523374, 25599425, 25034396, 19289642
21502702, 21291274, 18007682, 23521523, 20475845, 22148226, 22528741
29408136, 25417958, 24652769, 26088426, 19326908, 19597583, 17414008
23019710, 20897759, 26822620, 22046677, 19663176, 20938170, 19891090
24825843, 26318627, 21960504, 24509056, 19054077, 26262953, 22657942
20428621, 21899588, 23326313, 19723336, 19835133, 17532734, 19333670
25300427, 21842017, 19285025, 21373473, 23260854, 23061453, 19687159
14643995, 20977794, 20734332, 17551063, 27548131, 21977392, 24461826
19676012, 20588502, 23315889, 19520602, 23053606, 19841800, 20245930
19001359, 21476308, 26546754, 19393542, 23533524, 21099555, 27995248
25429959, 19141838, 19644859, 21915719, 19908836, 21421886, 19358317
19524158, 23548817, 25861398, 20803014, 23025340, 19335438, 19058490
23642282, 19207117, 18799993, 25919622, 26569225, 20835241, 25986062
24662775, 19475971, 18967382, 20347562, 20348653, 19896336, 24812585
20048359, 21896069, 20468490, 19524384, 25392535, 21147908, 20440930
25789277, 19171086, 24718260, 17867700, 19791273, 27397048, 21241829
19591608, 22707244, 18419520, 22296366, 22654475, 18914624, 19571367
28636676, 21522582, 19501299, 19529868, 20425790, 26007010, 19708342
27997875, 16870214, 18202441, 24415926, 18743542, 19001390, 21157728
19332396, 21875360, 25091141, 28000269, 19149990, 20382309, 22855193
16777441, 19606174, 20848335, 25495682, 19382851, 20528052, 22762046
24563422, 23125826, 22503297, 28993590, 25192729, 23338911, 22730454
19176326, 20298413, 19048007, 18849970, 21532755, 20860659, 22905130
26121990, 21263635, 22160989, 18499088, 22894949, 21059919, 18952989
22518784, 27348081, 25856821, 24457597, 25484507, 20794034, 21061354
```

```
19468347, 17533661, 19883092, 20657441, 24401351, 21285458, 18051556
25330273, 28023399, 26412540, 19699191, 24437510, 20669434, 16875041
18964978, 22972770, 20828947, 21373076, 25492379, 25551676, 14283239
25766822, 21967197, 22922076, 25575628, 26110259, 20368850, 21239530
20437153, 24848928, 20880215, 20798891, 25606091, 19013183, 21133343
22695831, 24365589, 25634317, 19587324, 20134113, 20273319, 18542562
26758193, 19017309, 21063322, 22062026, 20134339, 22077517, 22815955
23854396, 24690216, 22507210, 16354467, 20101006, 21795111, 27938623
23501901, 18797519, 25879984, 21260397, 25029423, 19354335, 19730508
22366558, 26658759, 25822410, 6599380, 20717359, 24321547, 27097854
21297872, 18964939, 26366517, 21913183, 22366322, 20171986, 20603431
21132297, 25957038, 21542577, 22507234, 23170620, 24719736, 25600342
18868646, 26637824, 20627866, 28587723, 29142109, 18110491, 16923858
24642295, 19518079, 20466322, 19339555, 25823754, 25110233, 24908321
20842388, 17274537, 26575788, 20474192, 21644640, 28849751, 21794615
18899974, 20471920, 22806698, 19052488, 19503821, 24350620, 20074391
19157754, 21220620, 24316947, 19865345, 19065556, 22816287, 25947799
20878790, 23492665, 21322887, 22305887, 20879889, 24350831, 19578350
28022101, 26439748, 21893235, 19363645, 21072646, 20898391, 19291380
27060167, 27086138, 18382302, 22536802, 22087683, 21197626, 21656630
20373598, 19248799, 22707866, 19155797, 19279273, 28432129, 18886413
25490238, 20922010, 19990037, 25150925, 20509482, 27255377, 24717859
20703000, 22862134, 21526048, 28683167, 24929210, 24560906, 20144308
21620471, 19670108, 19068610, 20267166, 25123585, 20476175, 18549238
22950945, 19385656, 23528412, 19684504, 21174504, 20899461, 20557786
21911701, 19143550, 20118035, 19024808, 25760195, 20009833, 19604659
16359751, 26039623, 19928926, 23314180, 20212067, 24737403, 20480209
18904062, 26430737, 29030780, 20856766, 27169796, 21668627, 17258582
20877664, 19487147, 23149541, 24577566, 19430401, 19676905, 20925795
21296029, 21629064, 23229229, 22865673, 20708701, 25353983, 19280225
21315084, 20613079, 19375649, 19213447, 19989009, 18191823, 27314390
26336977, 25775213, 24393981, 25639019, 17319928, 14705949, 19703301
21626377, 20122715, 6418158, 23105538, 26198926, 19258504, 21188532
23151677, 17890099, 21649497, 26446098, 16887946, 26024732, 18791688
19721304, 27012701, 19490948, 19619732, 21164318, 23148260, 18090142
21641760, 19818513, 23002524, 20139391, 24693382, 19978542, 23543183
22165897, 22359063, 19373893, 19409212, 18373438, 23035249, 18990693
20470877, 21422580, 21632821, 22351572, 20235511, 23220453, 18742258
18604493, 23008056, 22901797, 18610915, 20978259, 20832516, 24801152
26089440, 20907061, 19523462, 20505778, 19183343, 21787056, 21273804
22782647, 25093739, 17835294, 28708023, 24413809, 18371441, 26714910
24385983, 20413820, 24421668, 25897615, 25643931, 23195445, 21281607
20513399, 20558005, 20093776, 18909599, 20618595, 23572982, 19211433
20331945, 19512341, 22256431, 19637186, 19022470, 18607546, 26875822
24573817, 23115139, 19649152, 19201867, 21294938, 20898997, 18510194
21842740, 22454326, 24683149, 19534363, 25489607
```

Version 12.1.0.2.v15

La version 12.1.0.2.v15 inclut les éléments suivants :

- Correctif 28729169 : Mise à jour d'ensemble de correctifs Oracle Database 12.1.0.2.190115
- Correctif 28790654 : Mise à jour d'ensemble de correctifs Oracle JVM 12.1.0.2.190115
- Correctif 28125601 : DSTv32 pour RDBMS (TZDATA2018E)
- Correctif 28127287 : DSTv32 pour OJVM (TZDATA2018E)
- Correctif 17969866 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 20394750 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 21171382 : Correctif DBMS_STATS
- Correctif 29125200 : ensemble de correctifs JSON

- Correctif 20033733 : correctif sur la taille de tas KGL

Correctif Oracle 28729169, publié en janvier 2019

Bogues corrigés :

```
19309466, 19902195, 18250893, 25437699, 19383839, 16756406, 18456643
26546664, 22364044, 18845653, 19915271, 20172151, 18417036, 23713236
24796092, 23140259, 19243521, 19658708, 18272672, 21153266, 19174430
22243719, 20493163, 20688221, 21387964, 13542050, 22734547, 21623164
19012119, 19932634, 19869255, 22232606, 18681056, 23324000, 25427662
22068305, 24589081, 19439759, 19303936, 22916353, 24835538, 22353346
21106027, 26444887, 23088803, 22529728, 26256131, 19134173, 20447445
21188584, 19390567, 26513709, 25780343, 19769480, 21097043, 21225209
26245237, 20677396, 19284031, 19450314, 19016730, 20919320, 22075064
22551446, 22721409, 18440095, 22496904, 16439813, 18354830, 20596234
22022760, 20936905, 23197103, 21514877, 26111842, 18990023, 13787015
22492533, 20173897, 24624166, 17210525, 21260431, 20181030, 25056052
19370504, 21868720, 23068169, 19124589, 19402853, 21383171, 19888853
24341675, 17722075, 20882568, 25653109, 23026585, 18604692, 20717081
25546608, 27370965, 19081128, 22173980, 23514710, 19178851, 20951038
22168163, 25161298, 20569094, 24308635, 19791377, 19050649, 20920911
19189525, 22475617, 19469538, 27052607, 20598042, 22458049, 18988834
23302839, 25307368, 17409174, 22729345, 22842151, 19238590, 16941434
20387265, 24397438, 20673810, 23108128, 20356733, 22380919, 18436647
23065323, 20825533, 19124336, 22294260, 24790914, 20284155, 23571055
25539063, 17365043, 25914276, 20952966, 22961508, 19176223, 21300341
23237313, 18288842, 22353199, 27223075, 22083366, 25670786, 21419850
26898563, 19577410, 26248143, 23294548, 24737064, 19931709, 25423453
25547060, 23533807, 27726780, 24600330, 25600421, 18122373, 20043616
23124895, 18856999, 21450666, 18893947, 26633558, 20076781, 26029780
21196809, 21354456, 23725036, 20464614, 19562381, 27375542, 24808595
19189317, 25669791, 18307021, 21917884, 19708632, 27213224, 25633101
20711718, 18973548, 25982666, 19718981, 23567857, 22826718, 25655390
21773465, 20250147, 20144019, 19197175, 26263721, 19597439, 21387128
22007324, 19180770, 19879746, 21785691, 20424183, 24285405, 26544823
20322560, 22228324, 23172924, 22520320, 21575362, 25058080, 22365117
22645009, 25165496, 28950969, 18774543, 20124446, 21429602, 26153977
19371175, 21863727, 18940497, 19074147, 22923409, 25489342, 21380789
19154375, 19044962, 19532017, 19662635, 22374754, 20560611, 25654936
21492036, 18705806, 19578247, 22024071, 22238921, 22809871, 21184223
23089357, 19404068, 18921743, 19065677, 19018447, 19018206, 18308268
19777862, 22223463, 19304354, 22519146, 27199245, 22977256, 20890311
27445727, 21142837, 20869721, 24555417, 22179537, 21756699, 20217801
18819908, 22760595, 25483815, 23628685, 23007241, 19593445, 21080143
27351628, 20031873, 25489367, 18618122, 24737581, 26784509, 24739928
18966843, 19077215, 20704450, 19068970, 20543011, 19023822, 24713381
20432873, 21756677, 20328248, 18674047, 18849537, 20087383, 25459958
20315311, 22897344, 27534509, 25178179, 19308965, 18948177, 19468991
20868862, 21780146, 23315153, 20466628, 21756661, 20397490, 19706965
20302006, 24831514, 23240358, 22178855, 19032777, 20862087, 19329654
18974476, 20603378, 20859910, 19307662, 21847223, 20281121, 19075256
22568797, 19076343, 18866977, 22808310, 25635149, 20844426, 20904530
20441797, 21442094, 25079710, 24674955, 18840932, 18740837, 20294666
25602488, 21517440, 22062517, 27337759, 19174942, 20671094, 21889720
18411216, 20117253, 24386767, 20641666, 25264559, 22092979, 25616268
21625179, 20879709, 23003979, 20165574, 19272708, 19547370, 22624709
23084507, 20228093, 21281532, 25093872, 19805359, 19461270, 19434529
18799063, 20378086, 17008068, 21246723, 20831538, 20424899, 20361671
18674024, 19689979, 24411921, 19873610, 16619249, 20562898, 21641414
21091431, 19440586, 22757364, 22175564, 20725343, 21241052, 19561643
20736227, 19399918, 19195895, 20830459, 20017509, 18475439, 25790353
21828126, 21665897, 25555252, 20746251, 25764020, 25612095, 22568177
```

```
25357142, 23096938, 19067244, 18043064, 21329301, 18885870, 26243698
26187943, 20324049, 19536415, 23709062, 28174827, 20446883, 27314206
21299490, 25313154, 21744290, 18254023, 20591183, 25047724, 27847259
19185876, 27207110, 22465352, 24326444, 20402832, 19627012, 20468401
27441326, 27620950, 16863642, 19639483, 19315691, 27567477, 21479753
19174521, 20401975, 18306996, 18851894, 27034890, 20581111, 20318889
20936731, 21060755, 25240188, 26828994, 22256560, 19188927, 27229389
24570598, 20229001, 25475853, 21172913, 17655240, 21266085, 19028800
19035573, 19366375, 24523374, 25034396, 25599425, 19289642, 21291274
18007682, 23521523, 20475845, 22148226, 22528741, 25417958, 24652769
26088426, 19326908, 19597583, 17414008, 23019710, 20897759, 26822620
22046677, 20938170, 19891090, 24825843, 26318627, 21960504, 24509056
19054077, 26262953, 22657942, 20428621, 21899588, 23326313, 19723336
19835133, 17532734, 19333670, 21842017, 19285025, 21373473, 23260854
23061453, 19687159, 14643995, 20977794, 20734332, 17551063, 27548131
21977392, 24461826, 19676012, 20588502, 23315889, 19520602, 23053606
19841800, 20245930, 19001359, 21476308, 26546754, 19393542, 23533524
21099555, 27995248, 25429959, 19141838, 19644859, 21915719, 19908836
21421886, 19358317, 19524158, 23548817, 25861398, 20803014, 23025340
19335438, 19058490, 23642282, 19207117, 18799993, 25919622, 26569225
20835241, 24662775, 19475971, 18967382, 20347562, 20348653, 19896336
24812585, 20048359, 21896069, 19524384, 20468490, 25392535, 21147908
20440930, 25789277, 19171086, 24718260, 17867700, 19791273, 21241829
27397048, 19591608, 22707244, 18419520, 22296366, 22654475, 18914624
19571367, 28636676, 21522582, 19501299, 20425790, 19529868, 19708342
27997875, 16870214, 18202441, 24415926, 18743542, 19001390, 21875360
25091141, 28000269, 19149990, 20382309, 22855193, 16777441, 19606174
20848335, 25495682, 19382851, 20528052, 22762046, 24563422, 23125826
22503297, 28993590, 25192729, 23338911, 22730454, 19176326, 19048007
18849970, 21532755, 20860659, 22905130, 26121990, 21263635, 22160989
18499088, 22894949, 21059919, 18952989, 22518784, 25856821, 25484507
20794034, 19468347, 17533661, 19883092, 20657441, 24401351, 21285458
18051556, 25330273, 26412540, 19699191, 24437510, 20669434, 18964978
22972770, 20828947, 21373076, 25492379, 25551676, 14283239, 25766822
21967197, 22922076, 25575628, 26110259, 20368850, 21239530, 20437153
24848928, 20880215, 20798891, 25606091, 19013183, 21133343, 22695831
24365589, 25634317, 19587324, 20273319, 18542562, 26758193, 21063322
22062026, 20134339, 22077517, 22815955, 24690216, 22507210, 16354467
20101006, 21795111, 27938623, 23501901, 18797519, 25879984, 21260397
25029423, 19354335, 19730508, 22366558, 26658759, 25822410, 6599380
20717359, 24321547, 21297872, 27097854, 18964939, 26366517, 21913183
22366322, 20171986, 20603431, 21132297, 25957038, 21542577, 22507234
23170620, 24719736, 25600342, 18868646, 26637824, 20627866, 18110491
16923858, 24642295, 19518079, 20466322, 25823754, 25110233, 24908321
20842388, 17274537, 26575788, 20474192, 21644640, 21794615, 18899974
20471920, 22806698, 19052488, 19503821, 24350620, 20074391, 19157754
21220620, 24316947, 19865345, 19065556, 22816287, 25947799, 20878790
23492665, 21322887, 22305887, 20879889, 24350831, 19578350, 28022101
19363645, 21072646, 20898391, 19291380, 27060167, 27086138, 22536802
22087683, 21656630, 20373598, 19248799, 22707866, 19155797, 19279273
18886413, 25490238, 20922010, 19990037, 25150925, 20509482, 24717859
20703000, 22862134, 21526048, 24929210, 24560906, 28683167, 20144308
21620471, 19670108, 19068610, 20267166, 25123585, 20476175, 18549238
22950945, 19385656, 23528412, 19684504, 21174504, 20899461, 20557786
21911701, 19143550, 20118035, 19024808, 25760195, 20009833, 19604659
16359751, 26039623, 19928926, 23314180, 20212067, 24737403, 20480209
26430737, 20856766, 27169796, 21668627, 20877664, 19487147, 23149541
24577566, 19430401, 19676905, 20925795, 21296029, 21629064, 23229229
22865673, 20708701, 25353983, 19280225, 21315084, 20613079, 19375649
19213447, 19989009, 18191823, 27314390, 25775213, 26336977, 24393981
25639019, 17319928, 19703301, 21626377, 20122715, 6418158, 23105538
26198926, 19258504, 21188532, 23151677, 17890099, 21649497, 26446098
16887946, 26024732, 18791688, 19721304, 27012701, 19490948, 19619732
21164318, 23148260, 18090142, 21641760, 19818513, 20139391, 24693382
19978542, 23543183, 22165897, 22359063, 19409212, 23035249, 18990693
20470877, 21422580, 21632821, 22351572, 20235511, 23220453, 18604493
```

```
18742258, 23008056, 22901797, 18610915, 20978259, 20832516, 24801152
26089440, 20907061, 20505778, 19183343, 21787056, 21273804, 25093739
17835294, 24413809, 28708023, 18371441, 26714910, 24385983, 20413820
24421668, 25897615, 25643931, 23195445, 21281607, 20513399, 20558005
20093776, 18909599, 20618595, 23572982, 19211433, 20331945, 19512341
22256431, 19637186, 19022470, 18607546, 24573817, 23115139, 19649152
19201867, 21294938, 20898997, 18510194, 21842740, 22454326, 24683149
19534363, 25489607
```

Version 12.1.0.2.v14

La version 12.1.0.2.v14 comprend les éléments suivants :

- Correctif 28259833 : PSU Oracle Database 12.1.0.2.181016
- Correctif 28440711 : PSU Oracle JVM 12.1.0.2.181016
- Correctif 28125601 : DSTv32 pour RDBMS (TZDATA2018E)
- Correctif 28127287 : DSTv32 pour OJVM (TZDATA2018E)
- Correctif 17969866 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 20394750 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 21171382 : Correctif DBMS_STATS
- Correctif 28697469 : Correctif de base de données JSON
- Correctif 20033733 : correctif sur la taille de tas KGL

Correctif Oracle 28259833, publié en octobre 2018

Bogues corrigés :

```
19309466, 19902195, 18250893, 25437699, 19383839, 16756406, 18456643
26546664, 22364044, 18845653, 19915271, 20172151, 18417036, 23713236
24796092, 23140259, 19243521, 19658708, 18272672, 21153266, 19174430
22243719, 20688221, 20493163, 21387964, 13542050, 22734547, 21623164
19012119, 19932634, 19869255, 22232606, 18681056, 23324000, 25427662
22068305, 24589081, 19439759, 19303936, 22916353, 24835538, 22353346
21106027, 26444887, 23088803, 22529728, 26256131, 19134173, 20447445
21188584, 19390567, 26513709, 25780343, 19769480, 21097043, 21225209
26245237, 20677396, 19284031, 19450314, 19016730, 20919320, 22075064
22551446, 22721409, 18440095, 22496904, 16439813, 18354830, 20596234
22022760, 20936905, 23197103, 21514877, 26111842, 18990023, 22492533
20173897, 24624166, 17210525, 21260431, 20181030, 25056052, 19370504
21868720, 23068169, 19124589, 19402853, 19888853, 24341675, 17722075
20882568, 25653109, 23026585, 18604692, 20717081, 25546608, 27370965
19081128, 22173980, 23514710, 19178851, 20951038, 22168163, 25161298
20569094, 24308635, 19791377, 19050649, 20920911, 19189525, 19469538
27052607, 20598042, 22458049, 18988834, 23302839, 25307368, 17409174
22729345, 22842151, 19238590, 16941434, 20387265, 24397438, 20673810
23108128, 20356733, 22380919, 18436647, 23065323, 20825533, 19124336
22294260, 24790914, 20284155, 25539063, 17365043, 25914276, 20952966
22961508, 19176223, 21300341, 23237313, 18288842, 22353199, 22083366
25670786, 21419850, 26898563, 19577410, 23294548, 24737064, 19931709
25423453, 25547060, 23533807, 27726780, 24600330, 25600421, 18122373
20043616, 23124895, 18856999, 21450666, 18893947, 20076781, 26633558
26029780, 21196809, 21354456, 23725036, 20464614, 19562381, 24808595
27375542, 19189317, 25669791, 18307021, 21917884, 19708632, 27213224
25633101, 20711718, 18973548, 25982666, 19718981, 22826718, 25655390
23567857, 21773465, 20250147, 19197175, 26263721, 19597439, 21387128
```

```
22007324, 19180770, 19879746, 21785691, 20424183, 24285405, 26544823
20322560, 22228324, 23172924, 22520320, 21575362, 25058080, 22365117
22645009, 25165496, 18774543, 20124446, 21429602, 26153977, 19371175
21863727, 18940497, 19074147, 22923409, 25489342, 21380789, 19154375
19044962, 19532017, 19662635, 22374754, 20560611, 25654936, 21492036
18705806, 19578247, 22024071, 22238921, 22809871, 21184223, 23089357
19404068, 18921743, 19065677, 19018447, 19018206, 18308268, 19777862
22223463, 19304354, 22519146, 27199245, 20890311, 22977256, 21142837
20869721, 24555417, 22179537, 21756699, 20217801, 18819908, 22760595
25483815, 23007241, 19593445, 21080143, 27351628, 20031873, 18618122
24737581, 26784509, 24739928, 18966843, 19077215, 20704450, 19068970
20543011, 19023822, 24713381, 20432873, 21756677, 20328248, 18674047
18849537, 25459958, 20315311, 22897344, 27534509, 25178179, 19308965
18948177, 19468991, 20868862, 21780146, 20466628, 21756661, 20397490
23315153, 19706965, 20302006, 24831514, 23240358, 22178855, 19032777
20862087, 19329654, 18974476, 20603378, 20859910, 19307662, 21847223
20281121, 19075256, 19076343, 18866977, 22808310, 25635149, 20844426
20904530, 20441797, 21442094, 25079710, 24674955, 18840932, 18740837
20294666, 25602488, 21517440, 22062517, 27337759, 19174942, 20671094
21889720, 18411216, 20117253, 24386767, 20641666, 25264559, 22092979
21625179, 20879709, 23003979, 20165574, 19272708, 19547370, 22624709
23084507, 20228093, 21281532, 19805359, 19461270, 19434529, 18799063
20378086, 17008068, 21246723, 20831538, 20424899, 20361671, 18674024
19689979, 24411921, 19873610, 16619249, 20562898, 21641414, 21091431
19440586, 22757364, 22175564, 21241052, 20725343, 19561643, 20736227
19399918, 19195895, 20830459, 20017509, 25790353, 21828126, 21665897
25555252, 20746251, 25764020, 25612095, 25357142, 23096938, 19067244
18043064, 21329301, 18885870, 26243698, 26187943, 20324049, 19536415
23709062, 28174827, 20446883, 27314206, 21299490, 25313154, 21744290
18254023, 20591183, 27847259, 19185876, 27207110, 22465352, 24326444
20402832, 19627012, 27441326, 27620950, 16863642, 19639483, 19315691
21479753, 19174521, 20401975, 18306996, 18851894, 27034890, 20581111
20318889, 20936731, 21060755, 26828994, 22256560, 19188927, 27229389
24570598, 25475853, 21172913, 17655240, 21266085, 19028800, 19035573
19366375, 24523374, 25034396, 19289642, 21291274, 18007682, 23521523
20475845, 22148226, 22528741, 25417958, 24652769, 26088426, 19326908
19597583, 17414008, 23019710, 20897759, 26822620, 22046677, 20938170
24825843, 19891090, 21960504, 26318627, 24509056, 19054077, 26262953
22657942, 20428621, 21899588, 19723336, 19835133, 17532734, 19333670
21842017, 19285025, 21373473, 23260854, 19687159, 23061453, 14643995
20977794, 20734332, 17551063, 27548131, 21977392, 24461826, 19676012
20588502, 23315889, 19520602, 23053606, 19841800, 20245930, 19001359
21476308, 26546754, 19393542, 23533524, 21099555, 25429959, 19141838
19644859, 21915719, 19908836, 21421886, 19358317, 19524158, 23548817
25861398, 20803014, 23025340, 19335438, 19058490, 19207117, 23642282
18799993, 25919622, 26569225, 20835241, 24662775, 19475971, 18967382
20347562, 20348653, 19896336, 24812585, 20048359, 21896069, 19524384
25392535, 21147908, 20440930, 25789277, 19171086, 24718260, 17867700
19791273, 21241829, 19591608, 22707244, 18419520, 22296366, 18914624
19571367, 22654475, 21522582, 19501299, 20425790, 19708342, 27997875
16870214, 18202441, 24415926, 18743542, 19001390, 21875360, 25091141
28000269, 19149990, 20382309, 22855193, 16777441, 19606174, 20848335
25495682, 19382851, 20528052, 22762046, 24563422, 23125826, 22503297
25192729, 23338911, 22730454, 19176326, 19048007, 18849970, 21532755
20860659, 22905130, 21263635, 22160989, 18499088, 21059919, 18952989
22894949, 22518784, 25856821, 25484507, 20794034, 19468347, 17533661
19883092, 20657441, 24401351, 21285458, 18051556, 25330273, 19699191
24437510, 20669434, 18964978, 22972770, 20828947, 21373076, 25551676
25492379, 14283239, 25766822, 22922076, 25575628, 20368850, 21239530
20437153, 24848928, 20880215, 20798891, 25606091, 19013183, 21133343
22695831, 24365589, 25634317, 19587324, 20273319, 18542562, 26758193
21063322, 22062026, 20134339, 22077517, 22815955, 24690216, 22507210
20101006, 16354467, 21795111, 27938623, 23501901, 18797519, 25879984
21260397, 25029423, 19354335, 19730508, 22366558, 26658759, 6599380
20717359, 24321547, 21297872, 18964939, 26366517, 21913183, 22366322
20171986, 20603431, 21132297, 25957038, 21542577, 22507234, 23170620
```

```
24719736, 25600342, 18868646, 20627866, 26637824, 18110491, 16923858
24642295, 19518079, 20466322, 25823754, 25110233, 24908321, 20842388
17274537, 26575788, 20474192, 21644640, 21794615, 18899974, 20471920
22806698, 19052488, 19503821, 24350620, 20074391, 19157754, 21220620
24316947, 19865345, 19065556, 22816287, 25947799, 20878790, 23492665
21322887, 22305887, 20879889, 24350831, 19578350, 19363645, 21072646
20898391, 19291380, 27060167, 27086138, 22536802, 22087683, 21656630
20373598, 19248799, 22707866, 19155797, 19279273, 18886413, 25490238
20922010, 19990037, 25150925, 20509482, 24717859, 20703000, 22862134
21526048, 24929210, 24560906, 20144308, 21620471, 19670108, 19068610
20267166, 25123585, 20476175, 18549238, 22950945, 19385656, 23528412
19684504, 21174504, 20899461, 20557786, 21911701, 19143550, 20118035
19024808, 25760195, 20009833, 19604659, 16359751, 26039623, 19928926
23314180, 20212067, 24737403, 20480209, 26430737, 20856766, 27169796
21668627, 20877664, 19487147, 23149541, 24577566, 19430401, 19676905
20925795, 21296029, 21629064, 23229229, 22865673, 20708701, 25353983
19280225, 21315084, 19213447, 19989009, 18191823, 27314390, 25775213
24393981, 25639019, 17319928, 19703301, 21626377, 20122715, 6418158
23105538, 26198926, 19258504, 21188532, 23151677, 17890099, 21649497
26446098, 16887946, 26024732, 18791688, 19721304, 19490948, 27012701
19619732, 21164318, 18090142, 21641760, 19818513, 20139391, 24693382
19978542, 23543183, 22165897, 22359063, 19409212, 23035249, 18990693
20470877, 21422580, 21632821, 22351572, 20235511, 23220453, 18604493
23008056, 22901797, 18610915, 20832516, 24801152, 26089440, 20907061
20505778, 19183343, 21787056, 21273804, 25093739, 17835294, 24413809
18371441, 26714910, 24385983, 20413820, 24421668, 25897615, 25643931
23195445, 21281607, 20513399, 20558005, 20093776, 18909599, 20618595
23572982, 19211433, 20331945, 19512341, 22256431, 19637186, 19022470
18607546, 24573817, 19649152, 23115139, 19201867, 21294938, 20898997
18510194, 21842740, 22454326, 24683149, 19534363, 25489607
```

Version 12.1.0.2.v13

La version 12.1.0.2.v13 comprend les éléments suivants :

- Correctif 27547329 : PSU Oracle Database 12.1.0.2.180717
- Correctif 27923320 : PSU Oracle JVM 12.1.0.2.180717
- Correctif 28125601 : DSTv32 pour RDBMS (TZDATA2018E)
- Correctif 28127287 : DSTv32 pour OJVM (TZDATA2018E)
- Correctif 17969866 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 20394750 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 21171382 : Correctif DBMS_STATS
- Correctif 28307069 : Correctif de base de données JSON
- Correctif 20033733 : correctif sur la taille de tas KGL

Correctif Oracle 27547329, publié en juillet 2018

Bogues corrigés :

```
19309466, 19902195, 18250893, 25437699, 19383839, 16756406, 18456643
26546664, 18845653, 19915271, 20172151, 18417036, 23713236, 24796092
19243521, 19658708, 21153266, 19174430, 22243719, 20688221, 21387964
13542050, 22734547, 21623164, 19012119, 19932634, 19869255, 22232606
18681056, 23324000, 25427662, 22068305, 24589081, 19439759, 19303936
22916353, 24835538, 22353346, 21106027, 26444887, 23088803, 22529728
```

```
26256131, 19134173, 20447445, 21188584, 19390567, 26513709, 19769480
21097043, 21225209, 20677396, 19284031, 26245237, 19450314, 19016730
20919320, 22075064, 22551446, 22721409, 18440095, 22496904, 16439813
18354830, 20596234, 22022760, 20936905, 23197103, 21514877, 26111842
18990023, 22492533, 20173897, 24624166, 17210525, 21260431, 20181030
25056052, 19370504, 21868720, 23068169, 19124589, 19402853, 19888853
24341675, 17722075, 20882568, 23026585, 25653109, 20717081, 25546608
19081128, 27370965, 22173980, 19178851, 20951038, 22168163, 25161298
20569094, 24308635, 19791377, 19050649, 20920911, 19189525, 19469538
20598042, 22458049, 18988834, 17409174, 22729345, 22842151, 19238590
16941434, 20387265, 24397438, 20673810, 23108128, 20356733, 22380919
18436647, 23065323, 20825533, 19124336, 22294260, 24790914, 20284155
25539063, 17365043, 20952966, 22961508, 19176223, 21300341, 23237313
18288842, 22353199, 22083366, 21419850, 26898563, 19577410, 23294548
19931709, 25423453, 25547060, 23533807, 24600330, 25600421, 18122373
20043616, 23124895, 18856999, 21450666, 18893947, 20076781, 26029780
21196809, 21354456, 20464614, 23725036, 19562381, 24808595, 19189317
18307021, 25669791, 21917884, 19708632, 27213224, 25633101, 20711718
18973548, 25982666, 22826718, 25655390, 21773465, 20250147, 19197175
19597439, 26263721, 21387128, 19180770, 19879746, 21785691, 20424183
24285405, 26544823, 20322560, 22228324, 22520320, 23172924, 21575362
22365117, 22645009, 25165496, 18774543, 20124446, 21429602, 19371175
21863727, 18940497, 19074147, 22923409, 21380789, 19154375, 19044962
19532017, 19662635, 22374754, 20560611, 25654936, 21492036, 18705806
19578247, 22024071, 22238921, 22809871, 21184223, 23089357, 19404068
18921743, 19065677, 19018447, 19018206, 18308268, 19777862, 22223463
19304354, 22519146, 27199245, 20890311, 21142837, 20869721, 24555417
22179537, 21756699, 20217801, 18819908, 22760595, 25483815, 23007241
19593445, 21080143, 20031873, 18618122, 26784509, 24739928, 18966843
19077215, 20704450, 19068970, 20543011, 19023822, 24713381, 20432873
21756677, 20328248, 18674047, 18849537, 25459958, 20315311, 22897344
27534509, 25178179, 19308965, 18948177, 19468991, 20868862, 21780146
20466628, 21756661, 20397490, 19706965, 24831514, 23240358, 22178855
20302006, 19032777, 20862087, 19329654, 18974476, 20603378, 20859910
19307662, 21847223, 20281121, 19075256, 19076343, 18866977, 20844426
20904530, 20441797, 21442094, 25079710, 24674955, 18840932, 18740837
20294666, 25602488, 21517440, 22062517, 27337759, 19174942, 20671094
21889720, 18411216, 20117253, 24386767, 20641666, 25264559, 22092979
21625179, 20879709, 23003979, 20165574, 19272708, 19547370, 22624709
23084507, 20228093, 21281532, 19805359, 19461270, 19434529, 18799063
20378086, 17008068, 21246723, 20831538, 20424899, 20361671, 18674024
19689979, 24411921, 19873610, 16619249, 20562898, 21091431, 21641414
19440586, 22757364, 22175564, 21241052, 19561643, 19399918, 19195895
20830459, 20017509, 25790353, 21828126, 21665897, 20746251, 25764020
25612095, 25357142, 23096938, 19067244, 18043064, 21329301, 18885870
26187943, 20324049, 19536415, 20446883, 21299490, 27314206, 25313154
21744290, 18254023, 20591183, 27847259, 19185876, 22465352, 27207110
20402832, 19627012, 27441326, 27620950, 16863642, 19639483, 19315691
21479753, 19174521, 20401975, 18306996, 18851894, 27034890, 20581111
20318889, 20936731, 21060755, 22256560, 19188927, 24570598, 25475853
21172913, 17655240, 21266085, 19028800, 19035573, 19366375, 24523374
25034396, 19289642, 21291274, 18007682, 23521523, 20475845, 22148226
22528741, 25417958, 24652769, 26088426, 19326908, 19597583, 17414008
23019710, 20897759, 22046677, 20938170, 24825843, 21960504, 24509056
19054077, 22657942, 26262953, 20428621, 21899588, 19723336, 19835133
17532734, 19333670, 21842017, 19285025, 21373473, 23260854, 19687159
14643995, 20977794, 20734332, 17551063, 27548131, 21977392, 24461826
19676012, 20588502, 23315889, 19520602, 23053606, 19841800, 20245930
19001359, 21476308, 26546754, 19393542, 23533524, 21099555, 25429959
19141838, 19644859, 21915719, 19908836, 21421886, 19358317, 19524158
23548817, 25861398, 20803014, 23025340, 19335438, 19058490, 19207117
18799993, 26569225, 25919622, 20835241, 24662775, 19475971, 18967382
20347562, 20348653, 19896336, 24812585, 20048359, 21896069, 19524384
25392535, 20440930, 25789277, 19171086, 24718260, 17867700, 19791273
21241829, 19591608, 22707244, 18419520, 22296366, 18914624, 19571367
19501299, 20425790, 19708342, 27997875, 16870214, 18202441, 24415926
```

```
18743542, 19001390, 21875360, 25091141, 19149990, 20382309, 22855193
16777441, 19606174, 20848335, 25495682, 19382851, 20528052, 22762046
24563422, 23125826, 22503297, 25192729, 23338911, 22730454, 19176326
19048007, 18849970, 21532755, 20860659, 22905130, 21263635, 22160989
18499088, 21059919, 18952989, 22518784, 25856821, 25484507, 20794034
19468347, 17533661, 19883092, 20657441, 24401351, 21285458, 18051556
25330273, 19699191, 24437510, 20669434, 18964978, 20828947, 21373076
25551676, 14283239, 25766822, 22922076, 25575628, 20368850, 21239530
20437153, 20880215, 20798891, 25606091, 19013183, 21133343, 22695831
24365589, 19587324, 18542562, 26758193, 22062026, 20134339, 22077517
22815955, 24690216, 22507210, 20101006, 21795111, 27938623, 23501901
18797519, 21260397, 25029423, 19354335, 19730508, 22366558, 26658759
6599380, 20717359, 24321547, 21297872, 18964939, 26366517, 21913183
22366322, 20171986, 20603431, 21132297, 25957038, 21542577, 22507234
23170620, 24719736, 25600342, 18868646, 20627866, 18110491, 16923858
24642295, 19518079, 20466322, 25823754, 25110233, 24908321, 20842388
17274537, 26575788, 20474192, 21644640, 21794615, 18899974, 20471920
22806698, 19052488, 19503821, 24350620, 20074391, 19157754, 21220620
24316947, 19865345, 19065556, 22816287, 25947799, 20878790, 23492665
21322887, 20879889, 24350831, 19578350, 19363645, 21072646, 20898391
19291380, 27060167, 27086138, 22536802, 22087683, 20373598, 19248799
22707866, 19155797, 19279273, 18886413, 25490238, 20922010, 19990037
25150925, 20509482, 24717859, 20703000, 22862134, 21526048, 24929210
24560906, 20144308, 21620471, 19670108, 19068610, 20267166, 25123585
20476175, 18549238, 22950945, 19385656, 23528412, 19684504, 21174504
20899461, 20557786, 21911701, 19143550, 19024808, 20118035, 20009833
25760195, 19604659, 16359751, 26039623, 19928926, 23314180, 20212067
24737403, 20480209, 26430737, 27169796, 21668627, 20877664, 19487147
23149541, 24577566, 19430401, 19676905, 20925795, 21296029, 21629064
23229229, 22865673, 20708701, 19280225, 25353983, 21315084, 19213447
19989009, 18191823, 24393981, 25639019, 17319928, 19703301, 21626377
20122715, 6418158, 23105538, 26198926, 19258504, 21188532, 17890099
21649497, 26446098, 16887946, 26024732, 18791688, 19721304, 19490948
19619732, 21164318, 18090142, 21641760, 19818513, 20139391, 24693382
19978542, 23543183, 22165897, 22359063, 19409212, 23035249, 18990693
20470877, 21422580, 21632821, 22351572, 20235511, 23220453, 18604493
23008056, 18610915, 20832516, 24801152, 26089440, 20907061, 20505778
19183343, 21787056, 21273804, 25093739, 17835294, 24413809, 18371441
24385983, 20413820, 26714910, 24421668, 25897615, 25643931, 21281607
20513399, 23195445, 20558005, 20093776, 18909599, 20618595, 23572982
19211433, 20331945, 19512341, 22256431, 19637186, 19022470, 18607546
24573817, 19649152, 19201867, 21294938, 20898997, 18510194, 22454326
19534363, 24683149, 25489607
```

Version 12.1.0.2.v12

La version 12.1.0.2.v12 comprend les éléments suivants :

- Correctif 27338041 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS DATABASE 12.1.0.2.180417
- Correctif 27475603 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS OJVM 12.1.0.2.180417
- Correctif 27015449 : RDBMS - MISE À JOUR DSTV31 PROACTIVE - TZDATA2017C
- Correctif 27015468 : MISE À JOUR DSTV31 PROACTIVE - TZDATA2017C - CORRECTIF OJVM NÉCESSAIRE
- Correctif 17969866 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 20394750 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 21171382 : AUTO DOP COMPUTES A HIGH DOP UNNECESSARILY
- Correctif 27666699 : Correctif de base de données JSON
- Correctif 20033733 : PART :IMC:HIT ORA 600 [KGL-HEAP-SIZE-EXCEEDED]

Correctif Oracle 27338041, publié en avril 2018

Bogues corrigés :

```
19309466, 24570598, 25475853, 21172913, 19902195, 18250893, 17655240
25437699, 19383839, 21266085, 19028800, 19035573, 16756406, 19366375
18456643, 26546664, 24523374, 25034396, 19289642, 18845653, 19915271
21291274, 18007682, 20172151, 18417036, 23713236, 24796092, 23521523
20475845, 22148226, 22528741, 19243521, 19658708, 21153266, 24652769
26088426, 19326908, 19597583, 17414008, 20897759, 23019710, 19174430
22046677, 22243719, 20938170, 24825843, 21960504, 24509056, 19054077
22657942, 20688221, 20428621, 21899588, 21387964, 13542050, 19723336
19835133, 17532734, 19333670, 21842017, 19285025, 21373473, 22734547
23260854, 19687159, 14643995, 21623164, 20977794, 20734332, 19012119
19869255, 19932634, 17551063, 18681056, 22232606, 27548131, 21977392
23324000, 24461826, 19676012, 20588502, 25427662, 22068305, 23315889
19520602, 23053606, 19841800, 19439759, 20245930, 19303936, 19001359
21476308, 26546754, 22916353, 19393542, 23533524, 21099555, 24835538
22353346, 25429959, 19141838, 19644859, 21106027, 21915719, 26444887
23088803, 19908836, 21421886, 22529728, 26256131, 19358317, 19134173
19524158, 20447445, 23548817, 25861398, 20803014, 23025340, 21188584
19335438, 19390567, 19058490, 19207117, 26513709, 18799993, 26569225
20835241, 24662775, 19769480, 19475971, 21097043, 21225209, 20677396
19284031, 19450314, 19016730, 18967382, 20919320, 22075064, 20347562
20348653, 22551446, 19896336, 22721409, 24812585, 20048359, 21896069
18440095, 22496904, 19524384, 25392535, 16439813, 18354830, 20596234
20440930, 22022760, 20936905, 19171086, 23197103, 24718260, 17867700
19791273, 21514877, 26111842, 18990023, 21241829, 19591608, 22707244
18419520, 22492533, 22296366, 20173897, 24624166, 17210525, 18914624
19571367, 21260431, 19501299, 20181030, 25056052, 20425790, 19708342
19370504, 21868720, 23068169, 19124589, 19402853, 19888853, 16870214
24341675, 17722075, 18202441, 24415926, 18743542, 19001390, 20882568
23026585, 20717081, 25546608, 19081128, 22173980, 21875360, 25091141
19178851, 19149990, 20382309, 20951038, 22855193, 22168163, 16777441
25161298, 19606174, 20569094, 24308635, 20848335, 19791377, 19050649
19382851, 20920911, 20528052, 22762046, 19189525, 24563422, 23125826
22503297, 19469538, 25192729, 23338911, 20598042, 22458049, 18988834
22730454, 19176326, 19048007, 17409174, 22729345, 18849970, 21532755
20860659, 22842151, 22905130, 19238590, 16941434, 20387265, 21263635
24397438, 20673810, 23108128, 22160989, 20356733, 22380919, 18499088
18436647, 23065323, 21059919, 20825533, 18952989, 22518784, 19124336
25856821, 22294260, 25484507, 20794034, 19468347, 20284155, 17533661
19883092, 20657441, 24401351, 25539063, 17365043, 21285458, 20952966
22961508, 18051556, 25330273, 19176223, 21300341, 23237313, 18288842
19699191, 22353199, 24437510, 22083366, 21419850, 20669434, 18964978
26898563, 19577410, 23294548, 20828947, 21373076, 25551676, 14283239
25766822, 19931709, 22922076, 25423453, 25547060, 25575628, 23533807
20368850, 21239530, 20437153, 20880215, 25600421, 20798891, 25606091
18122373, 20043616, 23124895, 19013183, 18856999, 21450666, 21133343
22695831, 18893947, 24365589, 20076781, 21196809, 21354456, 19587324
20464614, 19562381, 18542562, 26758193, 24808595, 22062026, 19189317
18307021, 21917884, 19708632, 27213224, 25633101, 20711718, 20134339
22077517, 22815955, 24690216, 18973548, 25982666, 22507210, 22826718
25655390, 21773465, 20250147, 20101006, 21795111, 19197175, 23501901
18797519, 19597439, 21387128, 19180770, 19879746, 19354335, 21785691
19730508, 20424183, 22366558, 26658759, 24285405, 6599380, 20717359
26544823, 21297872, 20322560, 18964939, 22520320, 21575362, 26366517
21913183, 22366322, 20171986, 22365117, 22645009, 25165496, 20603431
21132297, 25957038, 21542577, 22507234, 18774543, 23170620, 24719736
25600342, 20627866, 20124446, 18110491, 21429602, 16923858, 24642295
19518079, 19371175, 20466322, 21863727, 18940497, 19074147, 22923409
25823754, 25110233, 24908321, 20842388, 17274537, 21380789, 26575788
19154375, 20474192, 19044962, 19532017, 21644640, 19662635, 22374754
20560611, 25654936, 21794615, 18899974, 21492036, 18705806, 20471920
```

```
22806698, 19052488, 22024071, 22238921, 19503821, 24350620, 22809871
20074391, 21184223, 23089357, 19157754, 21220620, 19404068, 24316947
18921743, 19865345, 19065677, 19065556, 22816287, 19018447, 19018206
19777862, 25947799, 22223463, 19304354, 20878790, 22519146, 23492665
21322887, 20879889, 24350831, 20890311, 19578350, 21142837, 20869721
24555417, 22179537, 21756699, 20217801, 18819908, 19363645, 25483815
21072646, 20898391, 19291380, 27060167, 27086138, 23007241, 19593445
21080143, 22536802, 22087683, 20373598, 19248799, 20031873, 22707866
19155797, 19279273, 18886413, 18618122, 25490238, 20922010, 19990037
25150925, 20509482, 24739928, 20703000, 18966843, 19077215, 22862134
21526048, 24929210, 24560906, 20704450, 20144308, 19068970, 20543011
21620471, 19023822, 19670108, 19068610, 20267166, 24713381, 20432873
21756677, 20476175, 25123585, 18549238, 20328248, 18674047, 22950945
19385656, 18849537, 23528412, 19684504, 25459958, 20315311, 22897344
20899461, 25178179, 20557786, 21911701, 19308965, 19143550, 19024808
18948177, 19468991, 20009833, 20868862, 21780146, 20466628, 21756661
20397490, 19706965, 24831514, 23240358, 22178855, 19604659, 16359751
19032777, 20862087, 19329654, 19928926, 18974476, 23314180, 20212067
20603378, 24737403, 20480209, 20859910, 26430737, 19307662, 21847223
21668627, 20281121, 27169796, 19075256, 20877664, 19487147, 19076343
23149541, 18866977, 24577566, 19430401, 19676905, 20844426, 20904530
20925795, 20441797, 21296029, 21629064, 21442094, 23229229, 25079710
22865673, 20708701, 19280225, 21315084, 24674955, 19213447, 18840932
18740837, 20294666, 19989009, 25602488, 18191823, 21517440, 22062517
19174942, 27337759, 17319928, 20671094, 21889720, 19703301, 21626377
20122715, 23105538, 18411216, 6418158, 26198926, 20117253, 19258504
21188532, 24386767, 17890099, 21649497, 26446098, 16887946, 26024732
25264559, 18791688, 19721304, 22092979, 19490948, 19619732, 21164318
21625179, 20879709, 23003979, 20165574, 18090142, 19272708, 21641760
19818513, 19547370, 22624709, 20139391, 23084507, 24693382, 20228093
21281532, 19978542, 23543183, 22165897, 22359063, 19409212, 19805359
19461270, 23035249, 19434529, 18799063, 18990693, 20470877, 20378086
17008068, 21246723, 21422580, 21632821, 20831538, 22351572, 20424899
20361671, 18674024, 19689979, 20235511, 23220453, 24411921, 19873610
16619249, 18604493, 20562898, 21091431, 19440586, 22757364, 18610915
22175564, 21241052, 19561643, 19399918, 19195895, 20832516, 20830459
20017509, 24801152, 21828126, 20907061, 21665897, 20746251, 20505778
19183343, 25764020, 25612095, 25357142, 23096938, 21787056, 21273804
19067244, 18043064, 21329301, 18885870, 20324049, 26187943, 19536415
25093739, 17835294, 20446883, 21299490, 25313154, 24413809, 21744290
18254023, 20591183, 18371441, 24385983, 20413820, 24421668, 25897615
19185876, 25643931, 21281607, 20513399, 22465352, 20558005, 20402832
19627012, 20093776, 18909599, 20618595, 27441326, 27620950, 23572982
16863642, 19639483, 19315691, 19211433, 20331945, 19512341, 22256431
21479753, 19637186, 19174521, 19022470, 18607546, 20401975, 18306996
24573817, 18851894, 19649152, 27034890, 20581111, 19201867, 20318889
20936731, 21060755, 21294938, 20898997, 18510194, 22256560, 22454326
19534363, 25489607, 19188927
```

Version 12.1.0.2.v11

La version 12.1.0.2.v11 comprend les éléments suivants :

- Correctif 26925311 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS DATABASE 12.1.0.2.180116
- Correctif 27001733 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS OJVM 12.1.0.2.180116
- Correctif 27015449 : RDBMS - MISE À JOUR DSTV31 PROACTIVE - TZDATA2017C
- Correctif 27015468 : MISE À JOUR DSTV31 PROACTIVE - TZDATA2017C - CORRECTIF OJVM NÉCESSAIRE
- Correctif 17969866 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 20394750 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS

- Correctif 21171382 : AUTO DOP COMPUTES A HIGH DOP UNNECESSARILY
- Correctif 27315904 : Correctif de base de données JSON
- Correctif 20033733 : ORA 600 [KGL-HEAP-SIZE-EXCEEDED]

Correctif Oracle 26925311, publié en janvier 2018

Bogues corrigés :

```
21099555, 22175564, 19141838, 22083366, 20842388, 19865345, 20117253
20830459, 19791273, 20671094, 21542577, 23105538, 19243521, 20951038
22165897, 19238590, 21281532, 17008068, 19908836, 24401351, 24577566
21184223, 25427662, 20717359, 19134173, 20569094, 20031873, 20387265
20322560, 21575362, 19149990, 21263635, 18886413, 17551063, 24719736
22160989, 22519146, 21623164, 22507210, 19703301, 23338911, 19366375
18007682, 19001390, 18202441, 24285405, 25655390, 20267166, 19358317
19706965, 19068970, 24739928, 18549238, 22148226, 18797519, 26544823
20825533, 23521523, 21196809, 18940497, 19670108, 19649152, 18866977
18948177, 19404068, 22496904, 22826718, 18964978, 19176326, 19035573
20413820, 20717081, 19176223, 21106027, 20904530, 20134339, 19074147
20868862, 18411216, 23035249, 25475853, 21072646, 21322887, 22507234
20425790, 20862087, 18966843, 25861398, 24929210, 24624166, 21329301
20562898, 19333670, 19468991, 20124446, 19883092, 23543183, 20878790
22855193, 18510194, 19658708, 19591608, 19402853, 23149541, 24796092
20618595, 22238921, 21795111, 21787056, 22380919, 19469538, 21266085
17835294, 19721304, 19068610, 19791377, 22178855, 16777441, 22173980
20746251, 20048359, 21896069, 19185876, 20898391, 20281121, 20907061
22950945, 21281607, 6599380, 19577410, 22092979, 19001359, 20603378
23089357, 23572982, 19490948, 21387964, 22294260, 20832516, 17532734
22351572, 18849970, 19309466, 19081128, 20627866, 20844426, 24908321
21188532, 18791688, 21442094, 20890311, 20596234, 20368850, 26366517
18973548, 19303936, 21296029, 22536802, 20882568, 21479753, 19461270
20235511, 20936905, 22077517, 21220620, 18964939, 19430401, 22806698
22296366, 21153266, 19409212, 20703000, 22657942, 20657441, 19879746
20557786, 26758193, 23237313, 26198926, 19684504, 26088426, 21294938
19024808, 24693382, 20528052, 20977794, 18799993, 20466322, 24642295
18740837, 19662635, 18440095, 21794615, 20382309, 20228093, 19065556
20212067, 25547060, 21868720, 22905130, 20938170, 19524384, 25459958
24350831, 17722075, 20446883, 20144308, 25056052, 18952989, 24523374
16870214, 21773465, 19928926, 19835133, 21629064, 21354456, 20466628
23007241, 24386767, 25490238, 19931709, 19730508, 18819908, 20250147
23124895, 25643931, 23220453, 19188927, 20074391, 18307021, 23533807
20356733, 14643995, 26430737, 18090142, 19065677, 19547370, 26024732
21225209, 21960504, 18371441, 20397490, 26575788, 23315889, 20172151
18967382, 22729345, 19174430, 22068305, 25654936, 18419520, 21241829
19536415, 26546664, 19171086, 21889720, 21132297, 20470877, 22465352
22168163, 19335438, 24397438, 20076781, 20447445, 18856999, 20471920
19869255, 21620471, 18990693, 23096938, 17890099, 19124336, 24812585
18990023, 20101006, 21300341, 20848335, 21744290, 21241052, 20897759
21668627, 19304354, 19052488, 20543011, 20794034, 23025340, 25606091
23260854, 18681056, 19562381, 24570598, 20952966, 19896336, 20828947
25539063, 18618122, 20328248, 24365589, 20440930, 18456643, 19699191
23065323, 22865673, 19201867, 22816287, 21514877, 22022760, 18743542
20798891, 20347562, 25161298, 23294548, 19777862, 24560906, 22551446
19687159, 21373076, 19174942, 20424899, 24461826, 21641760, 21899588
22862134, 18899974, 21476308, 20598042, 21297872, 24308635, 19058490
19032777, 20171986, 22815955, 25150925, 19399918, 24718260, 19434529
22492533, 19018447, 21273804, 18051556, 22757364, 18851894, 23125826
20424183, 21842017, 19022470, 19284031, 18043064, 26898563, 20173897
23713236, 22062026, 20475845, 17274537, 19440586, 16887946, 22374754
18974476, 22961508, 24825843, 17319928, 20401975, 20708701, 22062517
24674955, 17655240, 22809871, 19805359, 16439813, 19155797, 20859910
19393542, 17210525, 22024071, 19189525, 21847223, 21649497, 19075256
```

```
25079710, 25823754, 19370504, 20315311, 22762046, 22075064, 20936731
20437153, 25165496, 18845653, 19280225, 19248799, 20560611, 18988834
21756699, 22256431, 18921743, 20245930, 21532755, 18799063, 22454326
20373598, 20476175, 19571367, 20925795, 19018206, 25264559, 24385983
20509482, 20711718, 24509056, 20588502, 20181030, 21911701, 18849537
23501901, 25034396, 19183343, 22842151, 21917884, 21142837, 20603431
19189317, 23003979, 19644859, 19390567, 19279273, 26546754, 20669434
16863642, 22528741, 22707244, 25546608, 19619732, 20348653, 18607546
19315691, 19676905, 20165574, 17867700, 23528412, 20558005, 20734332
19532017, 20922010, 19818513, 19450314, 22353346, 16941434, 20361671
25423453, 20009833, 22366558, 20294666, 23197103, 18191823, 20860659
22707866, 19195895, 19371175, 19307662, 19154375, 20043616, 20324049
21977392, 18914624, 22529728, 22256560, 25330273, 19708342, 20139391
19593445, 21291274, 19382851, 19520602, 19174521, 21875360, 19676012
19326908, 20217801, 20093776, 18840932, 21097043, 21246723, 20803014
21665897, 19143550, 23026585, 20428621, 19627012, 24415926, 22087683
23548817, 14283239, 21422580, 19213447, 19518079, 26446098, 18610915
23492665, 18674024, 24831514, 21863727, 24413809, 18306996, 19915271
21626377, 19524158, 20122715, 20513399, 18110491, 22366322, 20284155
25091141, 21080143, 20017509, 22359063, 19363645, 19597439, 21239530
23108128, 19888853, 19383839, 20880215, 21756677, 22458049, 19534363
19354335, 19044962, 19639483, 25982666, 19475971, 22353199, 21060755
22243719, 22916353, 20378086, 21260431, 21756661, 24808595, 22923409
19028800, 20877664, 22518784, 21059919, 20879889, 21380789, 19723336
19077215, 21421886, 19604659, 21285458, 23533524, 26569225, 23170620
22365117, 18288842, 19048007, 19308965, 19689979, 17409174, 19503821
23068169, 24662775, 21526048, 25429959, 19197175, 19180770, 24555417
24573817, 19902195, 26444887, 25313154, 24835538, 23324000, 20318889
21492036, 19013183, 20591183, 19012119, 20464614, 22645009, 21625179
19067244, 25178179, 23053606, 21632821, 19841800, 19512341, 19211433
22695831, 20331945, 19587324, 24316947, 19578350, 19637186, 19054077
18674047, 19708632, 20898997, 21091431, 19285025, 19289642, 25947799
21133343, 20835241, 20869721, 21172913, 25602488, 19258504, 17365043
21419850, 21644640, 19468347, 21373473, 25093739, 22721409, 16359751
24421668, 21164318, 25484507, 25489607, 22520320, 19769480, 19439759
19272708, 23088803, 19978542, 19329654, 20402832, 19873610, 23229229
21517440, 13542050, 25897615, 19291380, 21915719, 25600342, 25192729
20879709, 20677396, 19076343, 19561643, 19990037, 18909599, 19487147
22897344, 20831538, 25600421, 19016730, 18250893, 23240358, 22179537
16619249, 18354830, 24411921, 25764020, 18254023, 16756406, 21188584
19989009, 25766822, 17414008, 20688221, 20441797, 20704450, 21780146
25612095, 25957038, 24652769, 25483815, 19157754, 19207117, 24437510
18885870, 21785691, 20673810, 24341675, 21450666, 18893947, 18705806
22223463, 18417036, 16923858, 23084507, 23314180, 20919320, 22503297
20474192, 22046677, 21299490, 19501299, 19385656, 20432873, 18542562
20920911, 20899461, 21315084, 21429602, 21387128, 18122373, 20581111
22624709, 26111842, 19606174, 24690216, 18436647, 19023822, 25110233
19124589, 19178851, 19597583, 20480209, 18499088, 19050649
```

Version 12.1.0.2.v10

La version 12.1.0.2.v10 comprend les éléments suivants :

- PSU Oracle d'octobre 2017, une combinaison de PSU de base de données (correctif 26713565) + PSU de composant OJVM (correctif 26635845)
- Oracle a recommandé les correctifs SGBDR pour Oracle GoldenGate (correctif 17969866)
- DBMS_STATS AUTO DOP COMPUTES A HIGH DOP UNNECESSARILY (correctif 21171382)
- Ensemble de correctifs JSON (correctif 26750145)
- Correctif sur la taille de tas KGL (correctif 20033733)
- Fichier de fuseau horaire DSTv30 (correctif 25881255, correctif OJVM 25881271)

Correctif Oracle 26713565, publié en octobre 2017

Bogues corrigés :

```
21099555, 22175564, 19141838, 22083366, 20842388, 19865345, 20117253
20830459, 19791273, 20671094, 21542577, 19243521, 20951038, 22165897
19238590, 21281532, 17008068, 19908836, 24577566, 21184223, 25427662
19134173, 20569094, 20031873, 20387265, 20322560, 21575362, 19149990
21263635, 17551063, 18886413, 24719736, 22160989, 22519146, 21623164
22507210, 23338911, 19703301, 19366375, 18007682, 19001390, 18202441
24285405, 25655390, 20267166, 19358317, 19706965, 19068970, 24739928
18549238, 22148226, 18797519, 26544823, 20825533, 23521523, 21196809
18940497, 19670108, 19649152, 18866977, 18948177, 22496904, 19404068
18964978, 19176326, 19035573, 20413820, 20717081, 19176223, 21106027
20904530, 20134339, 19074147, 20868862, 23035249, 18411216, 21072646
25475853, 21322887, 22507234, 20425790, 20862087, 18966843, 25861398
21329301, 20562898, 19333670, 19468991, 20124446, 19883092, 22855193
20878790, 18510194, 19658708, 19591608, 19402853, 23149541, 20618595
22238921, 21795111, 21787056, 22380919, 19469538, 21266085, 17835294
19721304, 19068610, 19791377, 22178855, 16777441, 22173980, 20746251
20048359, 21896069, 19185876, 20898391, 20281121, 20907061, 22950945
6599380, 19577410, 22092979, 19001359, 20603378, 23089357, 21387964
19490948, 22294260, 20832516, 17532734, 22351572, 19309466, 19081128
20627866, 20844426, 24908321, 21188532, 18791688, 21442094, 20890311
20596234, 20368850, 18973548, 19303936, 21296029, 20882568, 21479753
19461270, 20235511, 22077517, 20936905, 21220620, 18964939, 19430401
22806698, 22296366, 21153266, 19409212, 22657942, 20703000, 20657441
19879746, 20557786, 26198926, 26088426, 19684504, 21294938, 19024808
24693382, 20528052, 20977794, 18799993, 20466322, 24642295, 18740837
19662635, 18440095, 21794615, 20228093, 19065556, 20212067, 25547060
21868720, 20938170, 22905130, 19524384, 25459958, 24350831, 17722075
20144308, 20446883, 25056052, 18952989, 24523374, 16870214, 19928926
19835133, 21629064, 21354456, 20466628, 24386767, 25490238, 19931709
19730508, 18819908, 20250147, 23124895, 25643931, 23220453, 19188927
20074391, 18307021, 23533807, 20356733, 26430737, 14643995, 18090142
19065677, 19547370, 21225209, 21960504, 18371441, 20397490, 26575788
23315889, 20172151, 18967382, 19174430, 22068305, 25654936, 21241829
19536415, 19171086, 26546664, 21132297, 21889720, 22465352, 22168163
19335438, 24397438, 20076781, 20447445, 18856999, 20471920, 19869255
21620471, 18990693, 23096938, 19124336, 17890099, 24812585, 18990023
21300341, 20101006, 20848335, 21744290, 21241052, 20897759, 21668627
19304354, 19052488, 20543011, 20794034, 23025340, 25606091, 23260854
18681056, 19562381, 20952966, 19896336, 20828947, 25539063, 18618122
20328248, 20440930, 18456643, 19699191, 22865673, 19201867, 22816287
22022760, 21514877, 18743542, 20798891, 20347562, 25161298, 23294548
24560906, 22551446, 19777862, 19687159, 21373076, 19174942, 20424899
21899588, 22862134, 18899974, 21476308, 20598042, 24308635, 21297872
19058490, 19032777, 20171986, 22815955, 19399918, 19434529, 19018447
18051556, 21273804, 22757364, 18851894, 23125826, 20424183, 21842017
19022470, 19284031, 18043064, 23713236, 20173897, 22062026, 20475845
17274537, 19440586, 22961508, 24825843, 18974476, 22374754, 16887946
17319928, 20401975, 20708701, 24674955, 22062517, 22809871, 17655240
19805359, 16439813, 19155797, 20859910, 19393542, 17210525, 22024071
19189525, 21847223, 21649497, 19075256, 25823754, 25079710, 20315311
22762046, 22075064, 20936731, 20437153, 18845653, 19280225, 19248799
20560611, 18988834, 21756699, 22256431, 21532755, 18921743, 20245930
22454326, 18799063, 20373598, 20476175, 19571367, 20925795, 19018206
25264559, 20711718, 20509482, 20181030, 20588502, 21911701, 18849537
23501901, 25034396, 19183343, 22842151, 21917884, 21142837, 20603431
19189317, 23003979, 19644859, 19390567, 19279273, 26546754, 20669434
16863642, 22528741, 22707244, 25546608, 19619732, 20348653, 18607546
19315691, 19676905, 20165574, 17867700, 20558005, 20734332, 19532017
20922010, 19818513, 19450314, 22353346, 16941434, 20361671, 25423453
20009833, 22366558, 20294666, 23197103, 18191823, 20860659, 19195895
```

```
19371175, 19307662, 19154375, 20043616, 21977392, 18914624, 22529728
19708342, 20139391, 25330273, 19593445, 21291274, 19382851, 19520602
19174521, 21875360, 19676012, 19326908, 20217801, 20093776, 18840932
21097043, 21246723, 20803014, 21665897, 19143550, 23026585, 20428621
19627012, 22087683, 23548817, 14283239, 21422580, 19213447, 26446098
19518079, 23492665, 18610915, 18674024, 21863727, 24413809, 18306996
19915271, 21626377, 19524158, 20122715, 20513399, 18110491, 20284155
25091141, 21080143, 20017509, 22359063, 19363645, 19597439, 21239530
23108128, 19383839, 20880215, 21756677, 19888853, 22458049, 19534363
19354335, 19044962, 19639483, 25982666, 19475971, 22353199, 21060755
22243719, 22916353, 20378086, 24808595, 21756661, 21260431, 22923409
19028800, 20877664, 21059919, 20879889, 21380789, 19723336, 19077215
21421886, 19604659, 21285458, 23533524, 23170620, 22365117, 18288842
19048007, 19308965, 19689979, 17409174, 23068169, 19503821, 24662775
25429959, 21526048, 19197175, 19180770, 24555417, 24573817, 19902195
26444887, 24835538, 23324000, 20318889, 21492036, 19013183, 20591183
19012119, 20464614, 21625179, 19067244, 23053606, 21632821, 19841800
19512341, 22695831, 20331945, 19587324, 24316947, 19578350, 19637186
19054077, 18674047, 19708632, 20898997, 19285025, 21091431, 19289642
25947799, 21133343, 20835241, 20869721, 21172913, 25602488, 19258504
17365043, 21419850, 21644640, 19468347, 21373473, 25093739, 16359751
24421668, 21164318, 25489607, 25484507, 22520320, 19769480, 19439759
19272708, 19978542, 19329654, 20402832, 19873610, 23229229, 13542050
21517440, 25897615, 19291380, 21915719, 25600342, 20879709, 20677396
19076343, 19561643, 19990037, 22897344, 18909599, 19487147, 25600421
20831538, 19016730, 18250893, 23240358, 22179537, 16619249, 18354830
24411921, 18254023, 16756406, 21188584, 19989009, 25766822, 17414008
20688221, 20441797, 20704450, 21780146, 25612095, 25957038, 24652769
25483815, 19157754, 19207117, 24437510, 18885870, 21785691, 20673810
24341675, 21450666, 18893947, 18705806, 22223463, 18417036, 16923858
23084507, 23314180, 20919320, 22503297, 20474192, 22046677, 21299490
19501299, 19385656, 20432873, 18542562, 20920911, 20899461, 21429602
21387128, 21315084, 18122373, 20581111, 26111842, 22624709, 19606174
24690216, 18436647, 19023822, 25110233, 19124589, 19178851, 19597583
18499088, 19050649
```

Version 12.1.0.2.v9

La version 12.1.0.2.v9 comprend les éléments suivants :

- PSU Oracle de juillet 2017, une combinaison de PSU de base de données (correctif 26609783) + PSU de composant OJVM (correctif 26027162)
- Oracle a recommandé les correctifs SGBDR pour Oracle GoldenGate (correctif 17969866)
- DBMS_STATS AUTO DOP COMPUTES A HIGH DOP UNNECESSARILY (correctif 21171382)
- Ensemble de correctifs JSON (correctif 26083365)
- Correctif sur la taille de tas KGL (correctif 20033733 pour 12.1.0.2)
- Fichier de fuseau horaire DSTv30 (correctif 25881255, correctif OJVM 25881271)
- Prise en charge de Validation des fichiers d'instance de base de données (p. 1140) avec l'utilitaire de validation logique `RMAN`.
- Prise en charge de Définition de l'édition par défaut d'une instance de base de données (p. 1123)

Correctif Oracle 26609783, publié en juillet 2017

Bogues corrigés :

```
21099555, 22175564, 19141838, 22083366, 20842388, 19865345, 20117253
19791273, 20671094, 21542577, 20951038, 19243521, 22165897, 19238590
```

```
21281532, 17008068, 19908836, 24577566, 21184223, 25427662, 19134173
20569094, 20031873, 20387265, 20322560, 21575362, 19149990, 21263635
17551063, 18886413, 22160989, 22507210, 19703301, 19366375, 18007682
19001390, 18202441, 24285405, 25655390, 20267166, 19358317, 19706965
19068970, 24739928, 18549238, 22148226, 18797519, 26544823, 20825533
21196809, 18940497, 19670108, 19649152, 18866977, 18948177, 22496904
19404068, 18964978, 19176326, 19035573, 20413820, 20717081, 19176223
21106027, 20904530, 20134339, 19074147, 20868862, 18411216, 21072646
25475853, 21322887, 22507234, 20425790, 20862087, 18966843, 21329301
20562898, 19333670, 19468991, 20124446, 19883092, 20878790, 18510194
19658708, 19591608, 19402853, 20618595, 21787056, 22380919, 21266085
19469538, 17835294, 19721304, 19068610, 19791377, 22178855, 16777441
22173980, 20746251, 20048359, 21896069, 19185876, 20898391, 20281121
20907061, 6599380, 19577410, 22092979, 19001359, 20603378, 23089357
21387964, 19490948, 22294260, 20832516, 17532734, 22351572, 19309466
19081128, 20627866, 20844426, 24908321, 21188532, 18791688, 21442094
20890311, 20596234, 20368850, 18973548, 19303936, 21296029, 20882568
21479753, 19461270, 20235511, 22077517, 20936905, 21220620, 18964939
19430401, 22296366, 21153266, 19409212, 22657942, 20703000, 20657441
19879746, 20557786, 19684504, 21294938, 19024808, 24693382, 20528052
20977794, 18799993, 20466322, 18740837, 19662635, 18440095, 20228093
19065556, 20212067, 25547060, 21868720, 22905130, 19524384, 25459958
24350831, 17722075, 20446883, 25056052, 18952989, 24523374, 16870214
19928926, 19835133, 21629064, 21354456, 20466628, 24386767, 25490238
19931709, 19730508, 18819908, 20250147, 23124895, 25643931, 23220453
19188927, 20074391, 18307021, 23533807, 20356733, 14643995, 18090142
19065677, 19547370, 21225209, 21960504, 26575788, 20397490, 20172151
18967382, 19174430, 21241829, 19536415, 26546664, 19171086, 21132297
21889720, 22465352, 22168163, 19335438, 24397438, 20076781, 20447445
18856999, 20471920, 19869255, 21620471, 18990693, 23096938, 19124336
17890099, 24812585, 18990023, 21300341, 20101006, 20848335, 21744290
20897759, 21668627, 19304354, 19052488, 20543011, 20794034, 23025340
25606091, 23260854, 18681056, 19562381, 20952966, 19896336, 20828947
25539063, 18618122, 20328248, 20440930, 18456643, 19699191, 22865673
19201867, 22022760, 21514877, 18743542, 20798891, 20347562, 25161298
23294548, 24560906, 22551446, 19777862, 19687159, 21373076, 19174942
20424899, 21899588, 18899974, 21476308, 20598042, 24308635, 21297872
19058490, 19032777, 20171986, 22815955, 19399918, 19434529, 19018447
18051556, 21273804, 22757364, 18851894, 19022470, 19284031, 18043064
20173897, 22062026, 20475845, 17274537, 19440586, 24825843, 18974476
22374754, 16887946, 17319928, 20401975, 20708701, 24674955, 22062517
22809871, 17655240, 19805359, 16439813, 19155797, 20859910, 19393542
17210525, 22024071, 19189525, 21847223, 21649497, 19075256, 25823754
25079710, 20315311, 22762046, 22075064, 20936731, 20437153, 18845653
19280225, 19248799, 20560611, 18988834, 21756699, 18921743, 20245930
18799063, 20373598, 20476175, 19571367, 20925795, 19018206, 25264559
20711718, 20509482, 20181030, 20588502, 21911701, 18849537, 23501901
19183343, 21917884, 21142837, 20603431, 19189317, 19644859, 19390567
26546754, 19279273, 20669434, 16863642, 22528741, 25546608, 19619732
20348653, 18607546, 19315691, 19676905, 20165574, 17867700, 20558005
20734332, 19532017, 20922010, 19818513, 19450314, 22353346, 16941434
20361671, 25423453, 20009833, 22366558, 20294666, 23197103, 18191823
19195895, 19371175, 19307662, 19154375, 20043616, 21977392, 18914624
22529728, 20139391, 25330273, 19593445, 21291274, 19382851, 19520602
19174521, 21875360, 19676012, 19326908, 20217801, 20093776, 18840932
21097043, 21246723, 20803014, 21665897, 19143550, 23026585, 20428621
19627012, 14283239, 21422580, 19213447, 19518079, 18610915, 18674024
24413809, 18306996, 19915271, 21626377, 19524158, 20122715, 20513399
20284155, 25091141, 21080143, 20017509, 22359063, 19363645, 19597439
21239530, 19383839, 20880215, 21756677, 19888853, 22458049, 19534363
19354335, 19044962, 19639483, 25982666, 19475971, 22353199, 21060755
22243719, 22916353, 20378086, 24808595, 21756661, 21260431, 22923409
19028800, 20877664, 21059919, 20879889, 21380789, 19723336, 19077215
21421886, 19604659, 21285458, 23533524, 23170620, 22365117, 18288842
19048007, 19308965, 19689979, 17409174, 19503821, 21526048, 19197175
19180770, 24573817, 19902195, 24835538, 23324000, 20318889, 19013183
```

```
20591183, 19012119, 20464614, 19067244, 21632821, 19841800, 19512341
22695831, 20331945, 19587324, 24316947, 19578350, 19637186, 19054077
18674047, 19708632, 20898997, 21091431, 19289642, 21133343, 20835241
20869721, 21172913, 19258504, 17365043, 21419850, 21644640, 19468347
21373473, 25093739, 16359751, 21164318, 25484507, 22520320, 19769480
19439759, 19272708, 19978542, 19329654, 20402832, 19873610, 23229229
13542050, 21517440, 19291380, 21915719, 25600342, 20879709, 20677396
19076343, 19561643, 19990037, 18909599, 19487147, 25600421, 20831538
19016730, 18250893, 16619249, 18354830, 24411921, 16756406, 18254023
21188584, 19989009, 25766822, 17414008, 20688221, 20441797, 20704450
21780146, 25612095, 25957038, 25483815, 19157754, 19207117, 24437510
18885870, 21785691, 20673810, 21450666, 18893947, 18705806, 22223463
18417036, 16923858, 23314180, 20919320, 20474192, 22046677, 21299490
19501299, 19385656, 20432873, 20920911, 20899461, 21387128, 21315084
18122373, 20581111, 22624709, 19606174, 24690216, 18436647, 19023822
25110233, 19124589, 19178851, 19597583, 18499088, 19050649
```

Version 12.1.0.2.v8

La version 12.1.0.2.v8 comprend les éléments suivants :

- Correctif Oracle 25433980, une combinaison de PSU de base de données (correctif 25171037) + PSU de composant OJVM (correctif 25437695)
- Oracle a recommandé les correctifs SGBDR pour Oracle GoldenGate (correctif 17969866 pour 12.1.0.2)
- Correctif Formulaires Oracle 18307021 pour 12.1.0.2
- Correctif DBMS_STATS (correctif 21171382 pour 12.1.0.2)
- Ensemble de correctifs JSON (correctif 25531469 pour 12.1.0.2)
- Correctif sur la taille de tas KGL (correctif 20033733 pour 12.1.0.2)
- Correction d'un bogue qui affectait l'application d'une PSU après la mise à niveau vers 12.1.0.2.v5, v6 et v7
- Fichier de fuseau horaire DSTv28 (correctif 24701840)
- Prise en charge du package `DBMS_CHANGE_NOTIFICATION`
- Prise en charge des packages et vues `XSTREAM` (peut nécessiter des licences supplémentaires)

Correctif Oracle 25171037, publié en avril 2017

Bogues corrigés :

```
21099555, 22175564, 19141838, 22083366, 20842388, 20117253, 19865345
19791273, 21542577, 20951038, 19243521, 22165897, 17008068, 19908836
21281532, 19238590, 24577566, 21184223, 19134173, 20569094, 20031873
20322560, 20387265, 21575362, 19149990, 21263635, 17551063, 18886413
22160989, 22507210, 19366375, 19703301, 19001390, 24285405, 18202441
20267166, 19358317, 19706965, 19068970, 18549238, 24739928, 18797519
22148226, 20825533, 21196809, 19649152, 19670108, 18940497, 18948177
22496904, 18964978, 19176326, 19035573, 20413820, 19176223, 21106027
20904530, 20134339, 19074147, 20868862, 18411216, 25475853, 21322887
21072646, 22507234, 20425790, 20862087, 18966843, 21329301, 20562898
19333670, 20124446, 19468991, 19883092, 20878790, 18510194, 19658708
19591608, 19402853, 20618595, 21787056, 22380919, 19469538, 21266085
17835294, 19721304, 19068610, 19791377, 22178855, 16777441, 22173980
20048359, 20746251, 21896069, 19185876, 20898391, 20907061, 20281121
6599380, 19577410, 22092979, 19001359, 20603378, 23089357, 21387964
19490948, 22294260, 17532734, 20832516, 22351572, 19309466, 20627866
19081128, 20844426, 21188532, 18791688, 20890311, 21442094, 20596234
```

```
20368850, 18973548, 19303936, 21296029, 20882568, 19461270, 21479753
22077517, 20936905, 20235511, 21220620, 18964939, 19430401, 22296366
21153266, 19409212, 20703000, 22657942, 19879746, 20657441, 21294938
19684504, 19024808, 20528052, 24693382, 20977794, 18799993, 20466322
18740837, 19662635, 18440095, 20228093, 19065556, 20212067, 21868720
22905130, 19524384, 24350831, 17722075, 20446883, 25056052, 18952989
24523374, 16870214, 19928926, 19835133, 21629064, 21354456, 20466628
24386767, 25490238, 19931709, 19730508, 18819908, 20250147, 23124895
23220453, 19188927, 20074391, 18307021, 20356733, 14643995, 19065677
19547370, 21960504, 21225209, 20397490, 18967382, 19174430, 21241829
19536415, 19171086, 21889720, 22465352, 22168163, 19335438, 24397438
20447445, 18856999, 19869255, 20471920, 21620471, 23096938, 18990693
19124336, 17890099, 24812585, 18990023, 21300341, 20101006, 20848335
21744290, 20897759, 21668627, 19304354, 20543011, 19052488, 20794034
23025340, 23260854, 18681056, 20952966, 19896336, 25539063, 18618122
20328248, 20440930, 18456643, 19699191, 19201867, 22865673, 22022760
20798891, 18743542, 25161298, 20347562, 22551446, 19777862, 19687159
21373076, 19174942, 20424899, 21899588, 18899974, 21476308, 20598042
21297872, 24308635, 20171986, 19058490, 19032777, 22815955, 19399918
19434529, 21273804, 19018447, 22757364, 18851894, 19022470, 19284031
18043064, 20173897, 22062026, 20475845, 17274537, 19440586, 18974476
24825843, 22374754, 16887946, 17319928, 20401975, 20708701, 22062517
22809871, 17655240, 16439813, 19805359, 19155797, 20859910, 19393542
22024071, 17210525, 19189525, 21847223, 21649497, 25079710, 19075256
20315311, 22762046, 22075064, 20936731, 18845653, 19280225, 19248799
20560611, 18988834, 21756699, 18921743, 20245930, 18799063, 20373598
19571367, 20476175, 20925795, 19018206, 25264559, 20711718, 20509482
20181030, 20588502, 21911701, 18849537, 23501901, 19183343, 21917884
21142837, 19189317, 19644859, 19390567, 19279273, 20669434, 16863642
22528741, 25546608, 19619732, 18607546, 20348653, 19315691, 19676905
20165574, 17867700, 20558005, 20734332, 19532017, 20922010, 19818513
19450314, 22353346, 16941434, 20361671, 20009833, 22366558, 20294666
18191823, 23197103, 19195895, 19371175, 19307662, 19154375, 20043616
21977392, 18914624, 22529728, 25330273, 20139391, 19593445, 21291274
19382851, 19520602, 19174521, 21875360, 19676012, 19326908, 20217801
20093776, 18840932, 21097043, 21246723, 20803014, 21665897, 19143550
20428621, 19627012, 14283239, 21422580, 19213447, 19518079, 18610915
18674024, 24413809, 18306996, 19915271, 19524158, 20122715, 20284155
20017509, 22359063, 19363645, 19597439, 21239530, 19383839, 20880215
21756677, 19888853, 22458049, 19534363, 19354335, 19044962, 19639483
19475971, 22353199, 22243719, 21060755, 22916353, 20378086, 24808595
21756661, 21260431, 22923409, 19028800, 20877664, 21059919, 20879889
21380789, 19723336, 19077215, 19604659, 21421886, 21285458, 23533524
23170620, 22365117, 18288842, 19048007, 19308965, 19689979, 19503821
21526048, 19197175, 19180770, 19902195, 23324000, 20318889, 19013183
20591183, 19012119, 20464614, 19067244, 21632821, 19841800, 19512341
22695831, 20331945, 19587324, 24316947, 19578350, 19637186, 19054077
18674047, 19708632, 20898997, 21091431, 19289642, 21133343, 20869721
21172913, 19258504, 17365043, 21419850, 19468347, 21373473, 25093739
16359751, 21164318, 22520320, 19769480, 19439759, 19272708, 19978542
19329654, 20402832, 19873610, 23229229, 13542050, 21517440, 19291380
21915719, 20879709, 20677396, 19076343, 19561643, 19990037, 19487147
18909599, 20831538, 19016730, 18250893, 16619249, 18354830, 24411921
16756406, 18254023, 21188584, 19989009, 17414008, 20688221, 20704450
20441797, 25483815, 19157754, 24437510, 18885870, 21785691, 20673810
21450666, 18893947, 18705806, 22223463, 16923858, 18417036, 23314180
20919320, 20474192, 22046677, 21299490, 19501299, 19385656, 20920911
20899461, 21387128, 21315084, 18122373, 20581111, 19606174, 24690216
18436647, 19023822, 19124589, 19178851, 19597583, 18499088, 19050649
```

Version 12.1.0.2.v7

La version 12.1.0.2.v7 comprend les éléments suivants :

- Correctif Oracle 24917069, une combinaison de PSU de base de données (correctif 24732082) + PSU de composant OJVM (correctif 24917972)
- Oracle a recommandé les correctifs SGBDR pour Oracle GoldenGate (correctif 17969866 pour 12.1.0.2)
- Correctif Formulaires Oracle 18307021 pour 12.1.0.2
- Correctif DBMS_STATS (correctif 21171382 pour 12.1.0.2)
- Ensemble de correctifs JSON (correctif 25089615 pour 12.1.0.2)
- Correctif sur la taille de tas KGL (correctif 20033733 pour 12.1.0.2)

Correctif Oracle 24917069, publié en janvier 2017

Bogues corrigés :

```
24917972, 25067795, 24534298, 25076732, 25076756, 24315824, 21659726
24448240, 24448282, 23177536, 22675136, 23265914, 23265965, 23727148
22674709, 22670413, 22670385, 21188537, 22139226, 22118835, 22118851
21555660, 21811517, 19623450, 21566993, 21566944, 19176885, 21068507
21047803, 21047766, 20415564, 20408829, 20408866, 19877336, 19855285
19909862, 19895362, 19895326, 19153980, 19231857, 19223010, 19245191,
19699946,
21099555, 22175564, 19141838, 22083366, 20842388, 20117253, 19865345
19791273, 21542577, 20951038, 19243521, 22165897, 19908836, 21281532
19238590, 24577566, 21184223, 19134173, 20031873, 20387265, 21575362
19149990, 21263635, 17551063, 18886413, 22160989, 22507210, 19366375
19703301, 19001390, 24285405, 18202441, 20267166, 19358317, 19706965
24739928, 19068970, 18549238, 18797519, 22148226, 20825533, 21196809
19649152, 19670108, 18940497, 18948177, 22496904, 18964978, 19035573
19176326, 20413820, 19176223, 21106027, 20904530, 20134339, 19074147
20868862, 18411216, 21072646, 21322887, 22507234, 20425790, 18966843
21329301, 20562898, 19333670, 20124446, 19468991, 19883092, 18510194
19658708, 19591608, 19402853, 20618595, 21787056, 22380919, 19469538
21266085, 17835294, 19721304, 19791377, 19068610, 22178855, 16777441
22173980, 20048359, 20746251, 21896069, 20898391, 19185876, 20907061
20281121, 6599380, 19577410, 22092979, 19001359, 20603378, 23089357
19490948, 21387964, 22294260, 20832516, 17532734, 19309466, 20627866
19081128, 20844426, 21188532, 18791688, 20890311, 21442094, 20596234
18973548, 21296029, 19303936, 20882568, 19461270, 21479753, 22077517
20936905, 20235511, 21220620, 18964939, 19430401, 22296366, 21153266
19409212, 22657942, 19879746, 20657441, 21294938, 19684504, 24693382
20528052, 19024808, 20977794, 18799993, 20466322, 18740837, 19662635
20228093, 20212067, 19065556, 19524384, 17722075, 20446883, 25056052
24523374, 18952989, 16870214, 19928926, 19835133, 21629064, 21354456
20466628, 24386767, 19931709, 19730508, 18819908, 23124895, 23220453
19188927, 20074391, 18307021, 20356733, 14643995, 19547370, 19065677
21960504, 21225209, 20397490, 18967382, 19174430, 21241829, 19536415
19171086, 22465352, 22168163, 19335438, 24397438, 20447445, 18856999
19869255, 20471920, 21620471, 18990693, 17890099, 24812585, 18990023
21300341, 20101006, 20848335, 21744290, 20897759, 21668627, 19304354
19052488, 20794034, 23025340, 23260854, 18681056, 20952966, 19896336
20328248, 18618122, 20440930, 18456643, 19699191, 19201867, 22865673
22022760, 20798891, 18743542, 25161298, 20347562, 19777862, 22551446
19687159, 21373076, 19174942, 20424899, 21899588, 18899974, 21476308
20598042, 24308635, 19032777, 19058490, 22815955, 19399918, 19434529
21273804, 19018447, 22757364, 18851894, 19022470, 19284031, 18043064
20173897, 22062026, 20475845, 17274537, 19440586, 24825843, 18974476
22374754, 16887946, 17319928, 20401975, 20708701, 22809871, 17655240
16439813, 19805359, 19155797, 20859910, 19393542, 17210525, 22024071
```

```
21847223, 19189525, 21649497, 19075256, 20315311, 22762046, 22075064
20936731, 19280225, 18845653, 20560611, 19248799, 21756699, 18988834
20245930, 18921743, 18799063, 20373598, 19571367, 20476175, 20925795
25264559, 19018206, 20711718, 20509482, 20181030, 20588502, 18849537
23501901, 19183343, 21917884, 19189317, 19644859, 19390567, 19279273
20669434, 22528741, 16863642, 19619732, 18607546, 20348653, 19315691
19676905, 20165574, 17867700, 20558005, 20734332, 19532017, 20922010
19818513, 19450314, 22353346, 20361671, 20009833, 22366558, 20294666
23197103, 18191823, 19195895, 19307662, 19371175, 20043616, 19154375
18914624, 22529728, 20139391, 21291274, 19382851, 19520602, 19174521
21875360, 19676012, 19326908, 20217801, 20093776, 18840932, 21097043
21246723, 20803014, 21665897, 19143550, 20428621, 19627012, 14283239
19518079, 18610915, 18674024, 24413809, 18306996, 19524158, 19915271
20122715, 20284155, 20017509, 22359063, 19363645, 19597439, 21239530
19888853, 21756677, 20880215, 22458049, 19534363, 19354335, 19044962
19639483, 19475971, 22353199, 21060755, 22243719, 22916353, 20378086
24808595, 21260431, 21756661, 22923409, 20877664, 19028800, 21059919
20879889, 21380789, 19723336, 19077215, 19604659, 21421886, 21285458
23533524, 23170620, 22365117, 18288842, 19308965, 19048007, 19689979
21526048, 19197175, 19180770, 19902195, 23324000, 20318889, 19013183
20591183, 19012119, 20464614, 19067244, 21632821, 19512341, 19841800
22695831, 20331945, 19587324, 24316947, 19578350, 19637186, 18674047
19054077, 20898997, 19708632, 21091431, 19289642, 21133343, 20869721
21172913, 19258504, 17365043, 19468347, 21373473, 16359751, 19769480
19439759, 19272708, 19978542, 20402832, 19329654, 19873610, 23229229
21517440, 13542050, 19291380, 21915719, 20879709, 20677396, 19076343
19561643, 19990037, 19487147, 18909599, 20831538, 18250893, 19016730
16619249, 18354830, 18254023, 21188584, 19989009, 17414008, 20688221
20704450, 20441797, 19157754, 24437510, 18885870, 21785691, 18893947
21450666, 18705806, 22223463, 16923858, 18417036, 23314180, 20919320
20474192, 22046677, 19385656, 19501299, 20920911, 20899461, 21315084
21387128, 18122373, 20581111, 19606174, 24690216, 18436647, 19023822
19178851, 19124589, 19597583, 18499088, 19050649
```

Version 12.1.0.2.v6

La version 12.1.0.2.v6 inclut les éléments suivants :

- Correctif Oracle 24433133, une combinaison de PSU de base de données (correctif 24006101) + PSU de composant OJVM (correctif 24315824)
- Oracle a recommandé les correctifs SGBDR pour Oracle GoldenGate (correctif 17969866 pour 12.1.0.2)
- Correctif Formulaires Oracle 18307021 pour 12.1.0.2
- Correctif DBMS_STATS (correctif 21171382 pour 12.1.0.2)
- Ensemble de correctifs JSON (correctif 24568656 pour 12.1.0.2)
- Correction d'un bogue qui provoquait la suppression des répertoires clients par les scripts de mise à niveau 12c
- Mise à disposition du répertoire des journaux DIAG aux clients

Référence : mise à jour d'ensemble de correctifs Oracle Database 12.1.0.2.161018 (correctif 24006101, publié en octobre 2016)

Bogues corrigés :

```
21099555, 22175564, 19141838, 22083366, 20842388, 20117253, 19865345
19791273, 19243521, 20951038, 19908836, 21281532, 19238590, 24577566
21184223, 19134173, 20387265, 19149990, 21263635, 18886413, 17551063
22160989, 22507210, 19703301, 19366375, 19001390, 18202441, 20267166
```

```
19358317, 19706965, 18549238, 19068970, 18797519, 22148226, 20825533
19649152, 19670108, 18940497, 18948177, 18964978, 19035573, 19176326
20413820, 19176223, 20904530, 20134339, 19074147, 20868862, 18411216
21322887, 22507234, 20425790, 18966843, 21329301, 19333670, 19468991
20124446, 19883092, 19658708, 19591608, 19402853, 20618595, 21787056
22380919, 21266085, 17835294, 19721304, 19791377, 19068610, 22178855
22173980, 20746251, 20048359, 20898391, 19185876, 20281121, 20907061
6599380, 19577410, 22092979, 20603378, 19001359, 19490948, 21387964
20832516, 17532734, 19309466, 19081128, 20627866, 20844426, 21188532
18791688, 21442094, 20890311, 20596234, 18973548, 21296029, 19303936
19461270, 21479753, 20936905, 20235511, 21220620, 18964939, 19430401
22296366, 21153266, 19409212, 22657942, 20657441, 19879746, 19684504
20528052, 19024808, 20977794, 18799993, 20466322, 18740837, 19662635
20228093, 19065556, 20212067, 19524384, 17722075, 20446883, 18952989
16870214, 19928926, 19835133, 21629064, 20466628, 24386767, 19931709
19730508, 18819908, 23124895, 19188927, 20074391, 20356733, 14643995
19547370, 19065677, 21960504, 21225209, 20397490, 18967382, 19174430
21241829, 19536415, 19171086, 22465352, 22168163, 19335438, 20447445
18856999, 20471920, 19869255, 21620471, 18990693, 17890099, 18990023
20101006, 21300341, 20848335, 21744290, 20897759, 21668627, 19304354
19052488, 20794034, 23260854, 18681056, 20952966, 19896336, 18618122
20328248, 20440930, 18456643, 19699191, 19201867, 22865673, 18743542
20798891, 20347562, 22551446, 19777862, 19687159, 21373076, 19174942
20424899, 21899588, 18899974, 20598042, 19032777, 19058490, 22815955
19399918, 19434529, 21273804, 19018447, 22757364, 18851894, 19284031
19022470, 18043064, 20173897, 22062026, 20475845, 17274537, 19440586
16887946, 22374754, 17319928, 20708701, 17655240, 16439813, 19805359
19155797, 20859910, 19393542, 22024071, 17210525, 21847223, 19189525
21649497, 19075256, 22762046, 22075064, 19280225, 18845653, 20560611
19248799, 21756699, 18988834, 20245930, 18921743, 18799063, 20373598
20476175, 19571367, 20925795, 19018206, 20509482, 20711718, 20588502
18849537, 19183343, 21917884, 19189317, 19644859, 19390567, 19279273
20669434, 16863642, 22528741, 19619732, 18607546, 20348653, 19315691
19676905, 20165574, 17867700, 20558005, 20734332, 19532017, 20922010
19450314, 22353346, 20361671, 20009833, 22366558, 20294666, 18191823
19307662, 19371175, 19195895, 20043616, 19154375, 18914624, 20139391
21291274, 19174521, 19520602, 19382851, 21875360, 19676012, 19326908
20217801, 20093776, 21097043, 21246723, 21665897, 19143550, 20428621
19627012, 14283239, 19518079, 18610915, 18674024, 18306996, 19524158
19915271, 20122715, 20284155, 20017509, 19363645, 19597439, 21239530
19888853, 20880215, 21756677, 19534363, 19354335, 19044962, 19639483
22353199, 22243719, 22916353, 20378086, 21756661, 21260431, 22923409
20877664, 19028800, 20879889, 19723336, 19077215, 21421886, 19604659
19308965, 19048007, 18288842, 19689979, 21526048, 19180770, 19197175
19902195, 20318889, 19013183, 19012119, 20464614, 19067244, 21632821
19512341, 19841800, 20331945, 19587324, 24316947, 19578350, 19637186
18674047, 19054077, 20898997, 19708632, 21091431, 19289642, 20869721
19258504, 17365043, 19468347, 21373473, 16359751, 19439759, 19769480
19272708, 19978542, 20402832, 19329654, 19873610, 23229229, 21517440
13542050, 19291380, 21915719, 19076343, 19561643, 19990037, 19487147
18909599, 20831538, 18250893, 19016730, 16619249, 18354830, 21188584
19989009, 17414008, 20688221, 20704450, 20441797, 19157754, 18885870
21785691, 21450666, 18893947, 18705806, 22223463, 16923858, 18417036
20919320, 20474192, 22046677, 19385656, 19501299, 20920911, 20899461
21387128, 21315084, 18122373, 20581111, 19606174, 18436647, 19023822
19178851, 19124589, 19597583, 18499088, 19050649
```

Version 12.1.0.2.v5

La version 12.1.0.2.v5 comprend les éléments suivants :

- Correctif Oracle 23615289, une combinaison de PSU de base de données (correctif 23054246) + PSU de composant OJVM (correctif 23177536)

- Fichier de fuseau horaire DSTv26 (correctif 22873635 pour 12.1.0.2)
- Oracle a recommandé les correctifs SGBDR pour Oracle GoldenGate (correctif 17969866 pour 12.1.0.2)
- Correctif Formulaires Oracle 18307021 pour 12.1.0.2
- Possibilité de créer des fonctions personnalisées de vérification de mot de passe (voir Création de fonctions personnalisées pour vérifier les mots de passe (p. 1110))
- Correction d'un bogue qui empêchait la recompilation implicite de vues détenues par SYS

Référence : mise à jour d'ensemble de correctifs Oracle Database 12.1.0.2.160719 (correctif 23054246, publié en juillet 2016)

Bogues corrigés :

```
19189525, 21847223, 21099555, 21649497, 19075256, 19141838, 22762046
22075064, 20117253, 19865345, 19791273, 18845653, 19280225, 19248799
19243521, 20951038, 18988834, 21756699, 21281532, 19238590, 21184223
18921743, 20245930, 18799063, 19134173, 20373598, 19571367, 20476175
20925795, 19018206, 20509482, 20711718, 20387265, 20588502, 19149990
21263635, 18849537, 18886413, 17551063, 22507210, 19183343, 19366375
19703301, 21917884, 19001390, 18202441, 19189317, 20267166, 19644859
19390567, 19358317, 19279273, 19706965, 18549238, 16863642, 19068970
22528741, 18797519, 20825533, 19619732, 18607546, 20348653, 19649152
19670108, 18940497, 18948177, 19315691, 19676905, 18964978, 19176326
20165574, 19035573, 20413820, 17867700, 20558005, 19176223, 19532017
20904530, 20134339, 19450314, 19074147, 22353346, 20868862, 18411216
22507234, 20361671, 20425790, 18966843, 20009833, 22366558, 21329301
20294666, 18191823, 19333670, 19195895, 19371175, 19307662, 19154375
20043616, 20124446, 18914624, 19468991, 19883092, 21291274, 19382851
19520602, 19174521, 21875360, 19676012, 19326908, 19658708, 19591608
19402853, 20093776, 20618595, 21787056, 22380919, 21246723, 17835294
19721304, 19068610, 19791377, 21665897, 22178855, 22173980, 20048359
20746251, 19143550, 20898391, 19185876, 19627012, 20281121, 19577410
22092979, 19001359, 14283239, 19518079, 18610915, 19490948, 17532734
18674024, 18306996, 19309466, 19081128, 19524158, 19915271, 20122715
21188532, 18791688, 20284155, 20890311, 21442094, 20596234, 18973548
21296029, 19303936, 19597439, 20936905, 20235511, 21220620, 20880215
18964939, 21756677, 19888853, 19534363, 19430401, 19354335, 19044962
19639483, 22296366, 22353199, 21153266, 19409212, 19879746, 20657441
19684504, 20528052, 19024808, 20977794, 20378086, 18799993, 21756661
21260431, 18740837, 22923409, 19028800, 20877664, 20228093, 20879889
19065556, 19723336, 19077215, 19604659, 21421886, 19524384, 17722075
19308965, 18288842, 19048007, 19689979, 20446883, 18952989, 16870214
19928926, 19835133, 21629064, 21526048, 19197175, 19180770, 20466628
19902195, 19931709, 20318889, 19013183, 19730508, 19012119, 19067244
20074391, 20356733, 14643995, 19512341, 19841800, 20331945, 19587324
19065677, 19547370, 19578350, 21225209, 19637186, 20397490, 18967382
19174430, 21241829, 19054077, 18674047, 20898997, 19708632, 19536415
21091431, 19289642, 20869721, 22168163, 19335438, 19258504, 20447445
17365043, 18856999, 19468347, 19869255, 20471920, 21373473, 21620471
16359751, 18990693, 17890099, 19769480, 19439759, 19272708, 18990023
19978542, 19329654, 20101006, 21300341, 20402832, 19873610, 20848335
23229229, 21744290, 21668627, 21517440, 13542050, 19304354, 19052488
20794034, 19291380, 21915719, 23260854, 18681056, 20952966, 19896336
19076343, 19561643, 18618122, 19990037, 20440930, 18456643, 19699191
19201867, 19487147, 18909599, 20831538, 19016730, 18250893, 20798891
18743542, 20347562, 16619249, 18354830, 22551446, 19777862, 19687159
21373076, 19174942, 20424899, 21188584, 19989009, 17414008, 20688221
21899588, 20441797, 19157754, 19058490, 19032777, 22815955, 19399918
18885870, 19434529, 21273804, 19018447, 21450666, 18893947, 18851894
16923858, 18417036, 20919320, 19022470, 19284031, 20474192, 20173897
22046677, 22062026, 19501299, 19385656, 20920911, 17274537, 20899461
```

```
21315084, 19440586, 16887946, 22374754, 17319928, 19606174, 20708701
18436647, 17655240, 19023822, 19124589, 19178851, 16439813, 19805359
19597583, 18499088, 19155797, 19050649, 19393542
```

Version 12.1.0.2.v4

La version 12.1.0.2.v4 comprend les éléments suivants :

- PSU Oracle 12.1.0.2.160419 (22291127)
- Fichier de fuseau horaire DSTv25 (correctif 22037014)
- Oracle a recommandé les correctifs SGBDR pour Oracle GoldenGate (correctif 17969866)
- Ajoute la possibilité pour l'utilisateur principal d'accorder les rôles EM_EXPRESS_BASIC et EM_EXPRESS_ALL
- Ajoute la possibilité pour l'utilisateur principal d'accorder des privilèges sur les objets SYS avec l'option appropriée à l'aide de la procédure RDSADMIN.RDSADMIN_UTIL.GRANT_SYS_OBJECT
- Ajoute des privilèges d'utilisateur principal pour prendre en charge les schémas les plus courants créés par l'utilitaire Oracle Fusion Middleware Repository Creation Utility (RCU)

Référence : mise à jour d'ensemble de correctifs Oracle Database 12.1.0.2.160419 (correctif 22291127, publié en avril 2016)

Bogues corrigés :

```
21847223, 19189525, 19075256, 19141838, 22762046, 20117253, 19865345
19791273, 19280225, 18845653, 19248799, 20951038, 19243521, 21756699
18988834, 21281532, 19238590, 18921743, 20245930, 18799063, 19134173
20373598, 19571367, 20476175, 20925795, 19018206, 20711718, 20387265
20509482, 20588502, 19149990, 18849537, 17551063, 18886413, 19183343
19703301, 21917884, 19001390, 18202441, 19189317, 19644859, 19358317
19390567, 19279273, 19706965, 22528741, 19068970, 20825533, 19619732
18607546, 20348653, 19649152, 19670108, 18940497, 18948177, 19315691
19676905, 18964978, 19035573, 20165574, 19176326, 20413820, 20558005
19176223, 19532017, 20904530, 20134339, 19450314, 22353346, 19074147
18411216, 20361671, 20425790, 18966843, 21329301, 20294666, 19333670
19195895, 19307662, 19371175, 20043616, 19154375, 20124446, 18914624
19468991, 19883092, 19382851, 19520602, 19174521, 21875360, 19676012
19326908, 19658708, 19591608, 20093776, 20618595, 21787056, 17835294
19721304, 19791377, 19068610, 22173980, 20746251, 20048359, 19143550
19185876, 19627012, 20281121, 19577410, 22092979, 19001359, 19518079
18610915, 19490948, 18674024, 18306996, 19309466, 19081128, 19915271
20122715, 21188532, 18791688, 20284155, 20890311, 21442094, 20596234
18973548, 19303936, 19597439, 20936905, 20235511, 19888853, 21756677
18964939, 19354335, 19430401, 19044962, 19639483, 21153266, 22353199
19409212, 20657441, 19879746, 19684504, 19024808, 21260431, 21756661
18799993, 20877664, 19028800, 20879889, 19065556, 19723336, 19077215
19604659, 21421886, 19524384, 18288842, 19048007, 19689979, 20446883
18952989, 16870214, 19928926, 19835133, 21526048, 20466628, 19197175
19180770, 19902195, 20318889, 19730508, 19012119, 19067244, 20074391
20356733, 14643995, 19512341, 19841800, 20331945, 19587324, 19547370
19065677, 21225209, 19637186, 20397490, 18967382, 19174430, 19054077
18674047, 19536415, 19708632, 21091431, 19289642, 22168163, 20869721
19335438, 19258504, 20447445, 17365043, 18856999, 19468347, 20471920
19869255, 21620471, 16359751, 18990693, 17890099, 19769480, 19439759
19272708, 18990023, 19978542, 20402832, 20101006, 21300341, 19329654
19873610, 21744290, 13542050, 21517440, 21668627, 19304354, 19052488
20794034, 19291380, 21915719, 18681056, 20952966, 19896336, 19076343
```

```
19561643, 19990037, 18618122, 20440930, 18456643, 19699191, 19487147
18909599, 20831538, 18250893, 19016730, 18743542, 20347562, 16619249
18354830, 19777862, 19687159, 19174942, 20424899, 19989009, 20688221
21899588, 20441797, 19157754, 19032777, 19058490, 19399918, 18885870
19434529, 21273804, 19018447, 18893947, 16923858, 18417036, 20919320
19022470, 19284031, 20474192, 22046677, 20173897, 22062026, 19385656
19501299, 17274537, 20899461, 21315084, 19440586, 22374754, 16887946
19606174, 18436647, 17655240, 19023822, 19178851, 19124589, 16439813
19805359, 19597583, 18499088, 19155797, 19050649, 19393542
```

Version 12.1.0.2.v3

La version 12.1.0.2.v3 inclut les éléments suivants :

- PSU Oracle 12.1.0.2.160119 (21948354).
- Fichier de fuseau horaire DSTv25 (correctif 22037014 pour 12.1.0.2). 12.1.0.1 inclut DSTv24, correctif 20875898 (inchangé depuis 12.1.0.1.v3), car un rétroportage de DSTv25 n'était pas disponible au moment de la génération.
- Correction d'un problème qui empêchait les clients de créer plus de 10 objets de répertoire dans la base de données.
- Correction d'un problème qui empêchait les clients de réaccorder des privilèges de lecture sur les objets de répertoire ADUMP et BDUMP.

Référence : mise à jour d'ensemble de correctifs Oracle Database 12.1.0.2.160119 (correctif 21948354, publié en janvier 2016)

Bogues corrigés :

```
19189525, 19075256, 19141838, 19865345, 19791273, 19280225, 18845653
20951038, 19243521, 19248799, 21756699, 18988834, 19238590, 21281532
20245930, 18921743, 18799063, 19134173, 19571367, 20476175, 20925795
19018206, 20509482, 20387265, 20588502, 19149990, 18849537, 18886413
17551063, 19183343, 19703301, 19001390, 18202441, 19189317, 19644859
19358317, 19390567, 19279273, 19706965, 19068970, 19619732, 20348653
18607546, 18940497, 19670108, 19649152, 18948177, 19315691, 19676905
18964978, 19035573, 20165574, 19176326, 20413820, 20558005, 19176223
19532017, 20134339, 19074147, 18411216, 20361671, 20425790, 18966843
20294666, 19307662, 19371175, 19195895, 19154375, 19468991, 19174521
19520602, 19382851, 21875360, 19326908, 19658708, 20093776, 20618595
21787056, 17835294, 19791377, 19068610, 20048359, 20746251, 19143550
19185876, 19627012, 20281121, 19577410, 22092979, 19001359, 19518079
18610915, 19490948, 18674024, 18306996, 19309466, 19081128, 19915271
20122715, 21188532, 20284155, 18791688, 20890311, 21442094, 18973548
19303936, 19597439, 20235511, 18964939, 19430401, 19044962, 19409212
19879746, 20657441, 19684504, 19024808, 18799993, 20877664, 19028800
19065556, 19723336, 19077215, 19604659, 21421886, 19524384, 19048007
18288842, 19689979, 20446883, 18952989, 16870214, 19928926, 21526048
19180770, 19197175, 19902195, 20318889, 19730508, 19012119, 19067244
20074391, 19512341, 19841800, 14643995, 20331945, 19587324, 19547370
19065677, 19637186, 21225209, 20397490, 18967382, 19174430, 18674047
19054077, 19536415, 19708632, 19289642, 20869721, 19335438, 17365043
18856999, 19869255, 20471920, 19468347, 21620471, 16359751, 18990693
17890099, 19439759, 19769480, 19272708, 19978542, 20101006, 21300341
20402832, 19329654, 19873610, 21668627, 21517440, 19304354, 19052488
20794034, 19291380, 18681056, 19896336, 19076343, 19561643, 18618122
20440930, 18456643, 19699191, 18909599, 19487147, 18250893, 19016730
18743542, 20347562, 16619249, 18354830, 19687159, 19174942, 20424899
```

```
19989009, 20688221, 20441797, 19157754, 19032777, 19058490, 19399918
18885870, 19434529, 19018447, 18417036, 20919320, 19022470, 19284031
20474192, 20173897, 22062026, 19385656, 19501299, 17274537, 20899461
19440586, 16887946, 19606174, 18436647, 17655240, 19023822, 19178851
19124589, 19805359, 19597583, 19155797, 19393542, 19050649
```

Version 12.1.0.2.v2

La version 12.1.0.2.v2 comprend les éléments suivants :

- PSU Oracle 12.1.0.2.5 (21359755)
- Inclut le correctif de l'heure d'été, correctif 20875898 : DST-24, sorti après la PSU Avril 2015.

Référence : mise à jour d'ensemble de correctifs Oracle Database 12.1.0.2.5 (correctif 21359755, publié en octobre 2015)

Bogues corrigés :

```
19189525, 19075256, 19865345, 19791273, 19280225, 18845653, 19248799
19243521, 18988834, 19238590, 21281532, 18921743, 20245930, 19134173
19571367, 20476175, 20925795, 19018206, 20387265, 19149990, 18849537
19183343, 19703301, 19001390, 18202441, 19189317, 19644859, 19390567
19358317, 19279273, 19706965, 19068970, 19619732, 18607546, 20348653
18940497, 19670108, 19649152, 18948177, 19315691, 19676905, 18964978
20165574, 19035573, 19176326, 20413820, 20558005, 19176223, 19532017
20134339, 19074147, 18411216, 20361671, 20425790, 18966843, 20294666
19371175, 19307662, 19195895, 19154375, 19468991, 19174521, 19520602
19382851, 19658708, 20093776, 17835294, 19068610, 19791377, 20746251
20048359, 19143550, 19185876, 19627012, 20281121, 19577410, 19001359
19518079, 18610915, 18674024, 18306996, 19309466, 19081128, 19915271
20122715, 20284155, 18791688, 21442094, 19303936, 19597439, 20235511
18964939, 19430401, 19044962, 19409212, 20657441, 19684504, 19024808
19028800, 19065556, 19723336, 19077215, 21421886, 19524384, 19048007
18288842, 18952989, 16870214, 19928926, 19180770, 19197175, 19730508
19012119, 19067244, 20074391, 19841800, 19512341, 14643995, 20331945
19587324, 19065677, 19547370, 19637186, 21225209, 20397490, 18967382
19174430, 18674047, 19054077, 19708632, 19536415, 19289642, 19335438
17365043, 18856999, 20471920, 19468347, 21620471, 16359751, 18990693
19439759, 19769480, 19272708, 19978542, 19329654, 20402832, 19873610
19304354, 19052488, 19291380, 18681056, 19896336, 19076343, 19561643
18618122, 20440930, 18456643, 19699191, 18909599, 19487147, 18250893
19016730, 18743542, 20347562, 16619249, 18354830, 19687159, 19174942
20424899, 19989009, 20688221, 20441797, 19157754, 19058490, 19032777
19399918, 18885870, 19434529, 19018447, 18417036, 20919320, 19284031
19022470, 20474192, 22062026, 19385656, 19501299, 17274537, 20899461
19440586, 19606174, 18436647, 19023822, 19178851, 19124589, 19805359
19597583, 19155797, 19393542, 19050649
```

Version 12.1.0.2.v1

La version 12.1.0.2.v1 comprend les éléments suivants :

- PSU Oracle 12.1.0.2.3 (20299023)
- L'option In-Memory permet le stockage d'un sous-ensemble de données dans un format de colonne en mémoire optimisé pour la performance.

- Installe des bases de connaissances Oracle Text supplémentaires depuis Oracle Database. Exemples de média (anglais et français)
- Accès fourni à DBMS_REPAIR via RDSADMIN.RDSADMIN_DBMS_REPAIR
- Accorde ALTER DATABASE LINK, ALTER PUBLIC DATABASE LINK, EXEMPT ACCESS POLICY, EXEMPT IDENTITY POLICY et EXEMPT REDACTION POLICY à l'utilisateur maître

> **Note**
>
> La version 12.1.0.2.v1 prend en charge Enterprise Edition uniquement.

Référence : mise à jour d'ensemble de correctifs Oracle Database 12.1.0.2.3 (correctif 20299023, publié en avril 2015)

Bogues corrigés :

```
19189525, 19065556, 19075256, 19723336, 19077215, 19865345, 18845653
19280225, 19524384, 19248799, 18988834, 19048007, 18288842, 19238590
18921743, 18952989, 16870214, 19928926, 19134173, 19180770, 19018206
19197175, 19149990, 18849537, 19730508, 19183343, 19012119, 19001390
18202441, 19067244, 19189317, 19644859, 19358317, 19390567, 20074391
19279273, 19706965, 19068970, 19841800, 19512341, 14643995, 19619732
20348653, 18607546, 18940497, 19670108, 19649152, 19065677, 19547370
18948177, 19315691, 19637186, 19676905, 18964978, 19035573, 19176326
18967382, 19174430, 19176223, 19532017, 18674047, 19074147, 19054077
19536415, 19708632, 19289642, 20425790, 19335438, 18856999, 19371175
19468347, 19195895, 19154375, 16359751, 18990693, 19439759, 19769480
19272708, 19978542, 19329654, 19873610, 19174521, 19520602, 19382851
19658708, 19304354, 19052488, 19291380, 18681056, 19896336, 17835294
19076343, 19791377, 19068610, 19561643, 18618122, 20440930, 18456643
18909599, 19487147, 19143550, 19185876, 19016730, 18250893, 20347562
19627012, 16619249, 18354830, 19577410, 19687159, 19001359, 19174942
19518079, 18610915, 18674024, 18306996, 19309466, 19081128, 19915271
19157754, 19058490, 20284155, 18791688, 18885870, 19303936, 19434529
19018447, 18417036, 19597439, 20235511, 19022470, 18964939, 19430401
19044962, 19385656, 19501299, 17274537, 19409212, 19440586, 19606174
18436647, 19023822, 19684504, 19178851, 19124589, 19805359, 19024808
19597583, 19155797, 19393542, 19050649, 19028800
```

Voir aussi

- Mise à niveau du moteur de base de données Oracle (p. 975)
- Oracle sur Amazon RDS (p. 928)

Moteur de base de données : 11.2.0.4

Les versions suivantes sont disponibles pour le moteur de base de données 11.2.0.4 :

- Version 11.2.0.4.v25 (p. 1322)
- Version 11.2.0.4.v24 (p. 1325)
- Version 11.2.0.4.v23 (p. 1327)
- Version 11.2.0.4.v22 (p. 1330)
- Version 11.2.0.4.v21 (p. 1332)

- Version 11.2.0.4.v20 (p. 1334)
- Version 11.2.0.4.v19 (p. 1336)
- Version 11.2.0.4.v18 (p. 1338)
- Version 11.2.0.4.v17 (p. 1340)
- Version 11.2.0.4.v16 (p. 1341)
- Version 11.2.0.4.v15 (p. 1343)
- Version 11.2.0.4.v14 (p. 1345)
- Version 11.2.0.4.v13 (p. 1346)
- Version 11.2.0.4.v12 (p. 1348)
- Version 11.2.0.4.v11 (p. 1349)
- Version 11.2.0.4.v10 (p. 1350)
- Version 11.2.0.4.v9 (p. 1352)
- Version 11.2.0.4.v8 (p. 1353)
- Version 11.2.0.4.v7 (p. 1355)
- Version 11.2.0.4.v6 (p. 1356)
- Version 11.2.0.4.v5 (p. 1356)
- Version 11.2.0.4.v4 (p. 1357)
- Version 11.2.0.4.v3 (p. 1359)
- Version 11.2.0.4.v2 (obsolète) (p. 1359)
- Version 11.2.0.4.v1 (p. 1360)

Version 11.2.0.4.v25

La version 11.2.0.4.v25 comprend les éléments suivants :

- Correctif 31103343 : mise à jour d'ensemble de correctifs de base de données : 11.2.0.4.200714
- Correctif 31219953 : PSU de base de données de composant Oracle JVM 11.2.0.4.200714
- Correctif 31335037 : DSTV35 pour RDBMS (TZDATA2020A)
- Correctif 31335142 : DSTV35 pour OJVM (TZDATA2020A)
- Correctif 31596256 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 22188219 : ÉVÉNEMENT D'ATTENTE « L1 VALIDATION » UTILISÉ POUR UN RETOUR EN ARRIÈRE LORSQUE LA MISE EN FILE D’ATTENTE HW NE PEUT PAS ÊTRE ACQUISE
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS

Correctifs combinés pour la version 11.2.0.4.v25, publiés en juillet 2020

Bogues corrigés :

```
2990912, 6599380, 8322815, 9756271, 10136473, 11733603, 11786053
11883252, 12364061, 12611721, 12668795, 12747740, 12816846, 12897813
12905058, 12982566, 13254780, 13364795, 13498382, 13558557, 13609098
13645875, 13680635, 13829543, 13837378, 13853126, 13866822, 13871092
13936038, 13944971, 13951456, 13955826, 13960236, 14010183, 14015842
14034426, 14054676, 14084247, 14106803, 14133975, 14176370, 14245531
```

```
14285317, 14312810, 14338435, 14354737, 14368995, 14458214, 14521218
14521849, 14565184, 14602788, 14657740, 14692762, 14705949, 14735792
14764829, 14774730, 14829250, 14852021, 15861775, 15913355, 15955387
15979965, 15990359, 16042673, 16043574, 16065166, 16069901, 16091637
16180763, 16194160, 16198143, 16220077, 16228604, 16233738, 16268425
16285691, 16306373, 16314254, 16315398, 16344544, 16354467, 16360112
16384983, 16392068, 16399083, 16410570, 16422541, 16450169, 16472716
16494615, 16524926, 16538760, 16542886, 16571443, 16579084, 16595641
16596890, 16613964, 16618694, 16668584, 16674686, 16685417, 16692232
16721594, 16731148, 16756406, 16777840, 16785708, 16799735, 16819962
16832076, 16833527, 16833845, 16837842, 16850630, 16854386, 16855292
16863422, 16870214, 16875230, 16875449, 16898135, 16901385, 16903536
16912439, 16929165, 16934803, 16941434, 16943711, 16956380, 16989630
16992075, 17006183, 17006570, 17008068, 17011832, 17016369, 17019086
17019345, 17019356, 17025461, 17027426, 17030189, 17031322, 17036973
17037130, 17040527, 17040764, 17042658, 17047404, 17050888, 17056813
17071721, 17080436, 17082359, 17082983, 17088068, 17156148, 17165204
17174582, 17184721, 17186905, 17201047, 17201159, 17205719, 17208934
17215560, 17227073, 17227277, 17231779, 17232014, 17235750, 17237521
17238511, 17239687, 17242746, 17246576, 17254374, 17258090, 17258582
17265217, 17267114, 17274537, 17279227, 17282229, 17284817, 17285560
17288409, 17291347, 17296856, 17297939, 17299889, 17302277, 17308789
17311728, 17313525, 17323222, 17325413, 17332800, 17341326, 17343514
17344412, 17346091, 17346671, 17348614, 17359610, 17360606, 17365043
17375354, 17381384, 17385178, 17389192, 17390160, 17390431, 17392698
17393683, 17393915, 17394950, 17397545, 17432124, 17437634, 17441661
17443671, 17446237, 17449815, 17465741, 17468141, 17477958, 17478145
17478514, 17484731, 17484762, 17495022, 17501491, 17518652, 17528315
17532245, 17532729, 17545847, 17546761, 17546973, 17551063, 17551674
17551699, 17551709, 17570240, 17570606, 17571039, 17571306, 17586955
17587063, 17588480, 17596908, 17600719, 17602269, 17610798, 17612828
17614134, 17614227, 17621643, 17622427, 17630484, 17634921, 17643573
17644091, 17648596, 17649265, 17655240, 17655634, 17672719, 17694209
17695685, 17705023, 17716305, 17717883, 17721717, 17722535, 17726838
17752121, 17752995, 17754782, 17761775, 17762296, 17767676, 17783445
17783588, 17785870, 17786278, 17786518, 17787259, 17798953, 17801017
17804361, 17806696, 17811429, 17811438, 17811447, 17811456, 17811789
17816865, 17820741, 17824637, 17835048, 17835627, 17842825, 17847764
17848897, 17851160, 17852463, 17853456, 17853498, 17865671, 17877323
17883081, 17889549, 17889583, 17890099, 17891943, 17891946, 17892268
17903598, 17912217, 17922254, 17936109, 17945983, 17951233, 17957017
17982555, 17982832, 18000422, 18009564, 18018515, 18029658, 18031668
18043064, 18051556, 18061914, 18084625, 18086801, 18090142, 18091059
18092127, 18093615, 18094246, 18096714, 18098207, 18125929, 18135678
18139690, 18155762, 18159793, 18166013, 18166577, 18180390, 18189036
18191164, 18193833, 18199537, 18202441, 18203835, 18203837, 18203838
18228645, 18230522, 18232865, 18235390, 18244962, 18247991, 18259031
18260550, 18262334, 18264060, 18272672, 18273830, 18277454, 18280813
18282562, 18293054, 18306996, 18308268, 18315328, 18316692, 18317531
18325460, 18328509, 18331812, 18331850, 18334586, 18339044, 18356166
18362222, 18373438, 18382302, 18384391, 18384537, 18388363, 18411336
18413820, 18430495, 18436307, 18436647, 18440047, 18440095, 18441944
18456514, 18458318, 18460587, 18471685, 18482502, 18492302, 18508861
18510194, 18515268, 18522509, 18554763, 18554871, 18604493, 18604692
18607546, 18610915, 18614015, 18619917, 18628388, 18641419, 18641451
18641461, 18662619, 18673090, 18673304, 18673325, 18673342, 18674024
18674047, 18674465, 18676416, 18681862, 18682983, 18685892, 18704244
18705484, 18723434, 18740837, 18744139, 18747196, 18759211, 18762750
18765602, 18774543, 18783224, 18798250, 18819257, 18828868, 18832544
18841764, 18849970, 18856106, 18856999, 18868646, 18886413, 18899974
18933818, 18948177, 18964939, 18973548, 18973907, 18996843, 19006757
19006849, 19007266, 19013183, 19032777, 19032867, 19049453, 19058059
19060015, 19121551, 19153980, 19174430, 19175543, 19176885, 19187988
19197175, 19207117, 19207156, 19211433, 19211724, 19223010, 19231857
19258504, 19271443, 19272701, 19277336, 19285025, 19289642, 19297917
19306797, 19309466, 19315668, 19330795, 19358317, 19359219, 19373893
```

```
19374518, 19393542, 19396455, 19403858, 19429927, 19433930, 19440386
19442102, 19445860, 19455741, 19458377, 19461270, 19463893, 19463897
19466309, 19469538, 19475971, 19487147, 19490948, 19516448, 19540573
19544839, 19554106, 19554117, 19563300, 19563715, 19578350, 19584068
19587324, 19601228, 19601762, 19615136, 19644859, 19680952, 19689979
19692824, 19693090, 19697993, 19699191, 19699946, 19718981, 19721304
19727057, 19730508, 19768226, 19769489, 19777862, 19781326, 19788303
19788842, 19791273, 19794897, 19827973, 19831647, 19835133, 19852360
19854503, 19871910, 19888853, 19891090, 19895326, 19896336, 19909862
19915271, 19930276, 19943771, 19972564, 19972566, 19972568, 19972569
19972570, 20004021, 20004087, 20017509, 20023340, 20031873, 20067212
20074391, 20134113, 20142975, 20144308, 20169408, 20175161, 20250147
20273319, 20294666, 20296213, 20299015, 20324049, 20331945, 20334344
20382309, 20387265, 20390564, 20394750, 20408829, 20425790, 20441797
20448824, 20475845, 20476175, 20506699, 20506706, 20506715, 20509482
20513399, 20524085, 20558005, 20563314, 20569094, 20596234, 20598042
20627866, 20631274, 20631846, 20647412, 20657411, 20657441, 20671094
20672075, 20686773, 20717359, 20725343, 20777150, 20803583, 20828947
20856766, 20860659, 20861693, 20869721, 20875898, 20879889, 20882568
20907061, 20914870, 20925795, 20926021, 20936905, 21047407, 21047766
21051833, 21051840, 21051852, 21051858, 21051862, 21059919, 21063322
21067387, 21097043, 21132297, 21142837, 21168487, 21172913, 21174504
21179898, 21197626, 21227138, 21263635, 21275255, 21281607, 21281961
21286665, 21330264, 21343775, 21343838, 21343897, 21351877, 21352646
21354456, 21380789, 21387964, 21394225, 21419850, 21422580, 21424824
21425496, 21429602, 21453153, 21502702, 21515534, 21516611, 21517440
21526048, 21532755, 21534893, 21538485, 21538558, 21538567, 21566639
21566944, 21612959, 21629064, 21641760, 21656630, 21668627, 21698350
21756661, 21756677, 21756699, 21764119, 21787056, 21794615, 21795111
21811517, 21820934, 21834568, 21842740, 21847223, 21868720, 21893235
21897746, 21911701, 21911849, 21972320, 21983325, 22037014, 22083366
22092979, 22118835, 22148226, 22168163, 22175564, 22185234, 22188219
22195441, 22195448, 22195457, 22195465, 22195477, 22195485, 22195492
22228324, 22243719, 22250006, 22253904, 22296366, 22321741, 22321756
22351572, 22353199, 22380919, 22465352, 22499356, 22502493, 22507210
22507234, 22551446, 22568797, 22594718, 22606521, 22657942, 22666802
22670385, 22675136, 22683212, 22683225, 22686674, 22730454, 22760679
22782647, 22809871, 22820579, 22836801, 22873635, 22893153, 22901797
22905130, 22977256, 23003979, 23007241, 23008056, 23026585, 23065323
23105538, 23115139, 23140259, 23177648, 23194294, 23209741, 23262847
23265914, 23294548, 23302839, 23315889, 23328639, 23330119, 23330124
23536835, 23571055, 23614158, 23628685, 23713236, 23725036, 23727132
24307571, 24316947, 24348685, 24385983, 24411921, 24433711, 24448240
24476265, 24476274, 24528741, 24534298, 24555417, 24560906, 24563422
24570598, 24589081, 24624166, 24652769, 24662775, 24701840, 24717859
24719736, 24766121, 24790914, 24835538, 24842886, 24908321, 24975421
25042823, 25067795, 25076732, 25077278, 25093656, 25165496, 25248384
25328093, 25364628, 25369547, 25423453, 25427662, 25489607, 25494379
25505371, 25505382, 25505394, 25505407, 25555252, 25600421, 25634317
25635149, 25649873, 25654936, 25655390, 25764020, 25775213, 25809524
25823754, 25879656, 25879984, 25881255, 25885148, 25897615, 25914276
25947799, 25957038, 26007010, 26023002, 26030218, 26039623, 26078387
26198926, 26203182, 26243698, 26245237, 26336977, 26354017, 26439748
26474853, 26482376, 26513067, 26544823, 26569225, 26575788, 26631046
26637592, 26654363, 26667015, 26667023, 26667032, 26679352, 26744595
26746894, 26910644, 26999139, 27000663, 27015449, 27053456, 27072923
27086138, 27097854, 27255377, 27351628, 27374796, 27441326, 27461842
27534509, 27567477, 27642235, 27710072, 27825893, 27870645, 27952577
28000269, 28022101, 28076295, 28079127, 28100487, 28125601, 28199085
28254374, 28305362, 28357401, 28364007, 28384353, 28501075, 28502128
28612674, 28730253, 28734355, 28790634, 28806384, 28819280, 28849751
28852325, 28855981, 28876684, 28915933, 29027694, 29033139, 29200700
29254615, 29343156, 29434301, 29448234, 29483672, 29483723, 29483771
29511611, 29621961, 29633753, 29774367, 29944660, 29962927, 29962939
29992392, 29997937, 30160639, 30179644, 30215130, 30237239, 30252098
30275351, 30275359, 30305880, 30365745, 30393318, 30534664, 30559616
```

```
30562891, 30562907, 30562909, 30562923, 30562936, 30624864, 30758943
30772207, 30803210, 30855121, 31001455, 31010960, 31022191, 31022281
31031715, 31103343, 31125948, 31172207, 31306274, 31335037, 31335142
31338362, 31492144, 31492164, 31492176
```

Version 11.2.0.4.v24

La version 11.2.0.4.v24 inclut les éléments suivants :

- Correctif 30670774 : PSU de base de données 11.2.0.4.200414
- Correctif 30805543 : PSU de base de données de composant Oracle JVM 11.2.0.4.200414
- Correctif 29997937 : DSTv34 pour RDBMS (TZDATA2019G)
- Correctif 29997959 : DSTV34 OJVM (TZDATA2019B)
- Correctif 31192454 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 22188219 : ÉVÉNEMENT D'ATTENTE « L1 VALIDATION » UTILISÉ POUR UN RETOUR EN ARRIÈRE LORSQUE LA MISE EN FILE D'ATTENTE HW NE PEUT PAS ÊTRE ACQUISE
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS pour Purge de la corbeille (p. 1129)
- Prise en charge de Génération de rapports de performance avec AWR (Automatic Workload Repository) (p. 1119) utilisant le package `rdsadmin.rdsadmin_diagnostic_util`.

Correctifs combinés pour la version 11.2.0.4, publiés en avril 2020

Bogues corrigés :

```
18619917, 19309466, 28876684, 28855981, 18189036, 19781326, 13609098
16285691, 16756406, 18430495, 17323222, 29483723, 19915271, 19516448
14458214, 23713236, 23140259, 29434301, 22502493, 18272672, 16410570
16494615, 19174430, 21352646, 16901385, 16596890, 22243719, 18996843
21387964, 20334344, 17174582, 22250006, 17798953, 14015842, 18031668
15955387, 21534893, 16832076, 16065166, 16579084, 25427662, 21179898
11786053, 15990359, 24589081, 17982832, 18685892, 20142975, 24835538
16315398, 20861693, 17037130, 17284817, 17891946, 17279227, 17588480
17291347, 16731148, 21097043, 24528741, 22321741, 17165204, 26245237
17891943, 17359610, 17265217, 17465741, 29621961, 22551446, 18191164
16721594, 18614015, 27825893, 18440095, 19769489, 20596234, 18482502
16043574, 17360606, 20936905, 22321756, 19211724, 17392698, 19463893
29033139, 17477958, 17040764, 18362222, 19463897, 24624166, 17853456
14521849, 17816865, 19692824, 21868720, 17951233, 25505407, 17040527
31022191, 24975421, 19888853, 18009564, 20882568, 20803583, 23026585
18604692, 17622427, 16903536, 29483771, 17865671, 17883081, 16228604
17325413, 17082359, 12747740, 22168163, 16091637, 20569094, 17468141
30365745, 29962939, 19469538, 29633753, 20598042, 16042673, 23302839
17437634, 28734355, 19049453, 20387265, 16941434, 16833527, 21343775
17297939, 16069901, 14285317, 22380919, 18436647, 23065323, 21983325
17853498, 24790914, 23571055, 16542886, 21286665, 17365043, 17752995
25914276, 17296856, 18783224, 22353199, 22083366, 28305362, 21419850
16180763, 23294548, 26679352, 13960236, 25328093, 25423453, 18339044
17282229, 25600421, 18856999, 18259031, 28806384, 21354456, 23725036
18471685, 30237239, 17258090, 16344544, 17903598, 17011832, 18135678
18704244, 17786518, 19718981, 25655390, 17242746, 20250147, 19197175
17390431, 17835627, 17672719, 17393915, 21566639, 18765602, 21425496
26544823, 22228324, 29962927, 18682983, 30179644, 25165496, 12816846
18774543, 18747196, 17824637, 19429927, 21429602, 16524926, 17343514
19271443, 17019345, 18681862, 17186905, 23330119, 17811438, 26474853
17215560, 16875449, 21380789, 17184721, 18508861, 19466309, 23330124
```

```
17811429, 17019356, 25654936, 17754782, 17752121, 22809871, 17201159
18308268, 19777862, 16198143, 29027694, 18828868, 17586955, 28076295
26654363, 22977256, 16692232, 27374796, 21142837, 20869721, 17649265
25879656, 17847764, 21756699, 19697993, 28364007, 17787259, 23628685
30252098, 23007241, 27351628, 18094246, 20031873, 17375354, 21698350
26513067, 21538567, 22683212, 16450169, 17478145, 17311728, 17648596
17308789, 22836801, 21756677, 18674047, 14084247, 19788303, 22683225
27534509, 16833845, 18948177, 17205719, 21756661, 20004021, 17922254
13837378, 18084625, 17912217, 11883252, 24842886, 12982566, 26203182
14176370, 14764829, 21847223, 16875230, 28079127, 22568797, 17237521
29511611, 25635149, 16934803, 17848897, 20441797, 20175161, 16613964
18334586, 17288409, 17341326, 17449815, 15913355, 16399083, 18740837
20294666, 14565184, 21517440, 17614134, 19854503, 14245531, 16194160
18325460, 15979965, 30562923, 20671094, 27870645, 25093656, 18247991
16912439, 30562936, 24433711, 19930276, 22092979, 20506715, 23003979
20506706, 13871092, 19272701, 17397545, 16785708, 19461270, 21051862
13829543, 16220077, 17008068, 18061914, 20448824, 30275359, 18674024
19689979, 24411921, 30275351, 17596908, 17036973, 22175564, 17612828
20725343, 28199085, 23194294, 17630484, 21051858, 20017509, 21051852
17767676, 17232014, 22893153, 12611721, 25555252, 18356166, 17071721
19315668, 25764020, 16863422, 21051840, 17267114, 17820741, 18043064
21538558, 26243698, 20324049, 30305880, 16392068, 18744139, 24348685
26746894, 18628388, 27072923, 14010183, 16595641, 17080436, 17332800
20777150, 21453153, 20299015, 18413820, 18264060, 16819962, 22465352
21351877, 21051833, 18673342, 30562907, 30562909, 29200700, 27441326
16571443, 18328509, 27567477, 18674465, 16422541, 18306996, 19359219
21424824, 17443671, 17478514, 21067387, 16268425, 17381384, 18723434
17235750, 23328639, 22195448, 24570598, 21172913, 17655240, 18384391
16992075, 22195441, 17025461, 30562891, 16472716, 19289642, 21502702
22195457, 20475845, 22148226, 26030218, 18331850, 17945983, 13498382
24652769, 18673304, 17610798, 19891090, 25369547, 18456514, 8322815
22657942, 17313525, 17050888, 18317531, 19835133, 17495022, 11733603
18798250, 19285025, 18260550, 17390160, 18316692, 19458377, 14368995
17551063, 21343838, 12905058, 14735792, 28612674, 16855292, 23315889
13364795, 18235390, 18293054, 18673325, 19393542, 30215130, 14657740
17532729, 17393683, 17389192, 17783588, 17852463, 19358317, 17441661
14034426, 28254374, 20631274, 19207117, 26569225, 17518652, 24662775
19475971, 18282562, 19896336, 17348614, 19827973, 17346671, 31022281
19791273, 24476274, 22296366, 13853126, 18273830, 17570606, 13558557
26007010, 16685417, 18180390, 14692762, 18159793, 17027426, 24476265
23177648, 17851160, 16870214, 18202441, 17227073, 20657411, 19006849
22606521, 20506699, 28000269, 23536835, 17761775, 20382309, 16306373
17801017, 19680952, 16850630, 17694209, 26667015, 17877323, 18230522
24563422, 17446237, 17889549, 17551674, 16233738, 22730454, 17571039
26667023, 19972570, 18849970, 21532755, 20860659, 22905130, 21168487
17016369, 21263635, 17231779, 21343897, 17717883, 27710072, 18522509
23209741, 17484731, 21972320, 19972569, 19972568, 17716305, 21059919
19972566, 19972564, 26667032, 17394950, 20657441, 17551699, 17006570
18051556, 12364061, 18029658, 17546973, 18262334, 19699191, 17227277
18018515, 16943711, 17982555, 20828947, 18098207, 18436307, 19584068
16898135, 13936038, 19601762, 31010960, 14054676, 25505394, 18228645
19013183, 25042823, 17721717, 17239687, 25248384, 25634317, 20134113
20273319, 28501075, 21063322, 17344412, 22507210, 16354467, 21795111
25505371, 16777840, 25879984, 17811456, 19730508, 17385178, 18166013
17484762, 10136473, 6599380, 20717359, 20296213, 27097854, 13955826
18193833, 17545847, 16837842, 18964939, 19871910, 25505382, 17811447
18554763, 21132297, 25957038, 20004087, 17889583, 19544839, 26631046
22507234, 24719736, 18868646, 17042658, 20627866, 14106803, 13951456
18139690, 18277454, 13680635, 25823754, 18554871, 18515268, 20169408
24908321, 17274537, 17602269, 26575788, 19032867, 17762296, 14829250
16929165, 14602788, 28849751, 21794615, 18899974, 29944660, 18441944
17811789, 20074391, 14852021, 17705023, 13645875, 24316947, 16668584
17786278, 25947799, 20879889, 19578350, 28022101, 22594718, 16384983
26439748, 17957017, 19121551, 17570240, 19788842, 18382302, 27086138
21330264, 21197626, 14338435, 13944971, 21656630, 18886413, 17156148
17936109, 20509482, 27255377, 24717859, 18762750, 21526048, 24560906
```

```
18096714, 17238511, 26078387, 27053456, 20144308, 25364628, 18244962
19433930, 20476175, 19297917, 21174504, 18280813, 28819280, 17614227
28357401, 21911701, 17006183, 25809524, 18092127, 19727057, 17695685
26039623, 22820579, 20856766, 15861775, 17258582, 21668627, 19487147
20925795, 28100487, 26482376, 19554106, 22760679, 21629064, 18199537
18091059, 17299889, 21538485, 17546761, 26336977, 25775213, 18155762
30803210, 16956380, 19207156, 14705949, 23105538, 26198926, 19258504
16314254, 17246576, 17655634, 17890099, 16989630, 20067212, 19721304
25077278, 19490948, 18203835, 18203838, 18973907, 18203837, 29483672
19615136, 17587063, 18000422, 18641451, 18090142, 21641760, 17019086
30559616, 19373893, 18373438, 21820934, 18641461, 17346091, 21422580
22351572, 18604493, 23008056, 22901797, 18610915, 17892268, 17501491
20907061, 14354737, 17835048, 21787056, 22195485, 22782647, 17082983
18641419, 16618694, 14133975, 22195492, 18331812, 18093615, 24385983
25897615, 20513399, 21281607, 13866822, 18841764, 17600719, 17842825
20558005, 17088068, 9756271, 22195465, 18440047, 19211433, 21515534
20331945, 22686674, 18384537, 18607546, 17254374, 18315328, 23115139
28790634, 21394225, 16360112, 22195477, 17726838, 18510194, 17571306
24766121, 17302277, 21842740, 17551709, 26910644, 17634921, 25489607
16538760, 18933818, 19176885, 17201047, 25649873, 25067795, 28502128
27952577, 14774730, 27461842, 19153980, 21911849, 23727132, 18166577
27000663, 24448240, 17056813, 21811517, 19909862, 25494379, 22675136
24534298, 19895326, 22253904, 17804361, 19231857, 27642235, 26023002
17528315, 19058059, 30534664, 29992392, 19554117, 19007266, 28915933
30855121, 30160639, 17285560, 29254615, 22670385, 18458318, 19187988
23265914, 19699946, 19006757, 19374518, 29774367, 19223010, 29448234
25076732, 22118835, 26637592, 19852360, 20408829, 21047766, 21566944
28730253, 16799735, 17432124, 18759211, 19396455, 20875898, 22037014
22873635, 23614158, 24701840, 25881255, 27015449, 28125601, 28852325
29997937, 29997959, 26354017, 21893235, 18125929, 19601228, 12668795
20524085, 19403858, 18086801, 16854386, 21612959, 20563314, 18705484
16674686, 20425790, 20390564, 19032777, 21275255, 17783445, 19943771
18973548, 18411336, 18673090, 19768226, 21047407, 17030189, 18856106
19693090, 21227138, 18492302, 19831647, 12897813, 19563300, 20914870
19587324, 13254780, 18676416, 21834568, 19794897, 26744595, 17208934
17031322, 19060015, 19277336, 19455741, 21764119, 17785870, 20631846
22185234, 20023340, 20647412, 19440386, 21281961, 25885148, 17722535
20926021, 20686773, 17621643, 18662619, 19563715, 19442102, 21516611
14312810, 20672075, 21897746, 2990912, 23262847, 19644859, 19175543
17644091, 20394750, 19306797, 18819257, 22188219
```

Version 11.2.0.4.v23

La version 11.2.0.4.v23 inclut les éléments suivants :

- Correctif 30298532 : Mise à jour d'ensemble de correctifs de base de données : 11.2.0.4.200114
- Correctif 30503372 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS OJVM 11.2.0.4.200114
- Correctif 29997937 : DSTv34 pour RDBMS (TZDATA2019G)
- Correctif 29997959 : DSTV34 OJVM (TZDATA2019B)
- Oracle GoldenGate : correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 19440386 : ÉCHEC DE DÉCLENCHEMENT D'ORA-1 POUR MISE À JOUR PACKAGE QUAND CONTRAINTE=IMMÉDIATE
- Correctif 19277336 : LE RÉPLICA INTÉGRÉ INVALIDE LES PACKAGES DÉPENDANTS ET GÉNÈRE UNE ERREUR ORA-4068
- Correctif 24286409 : DEMANDE DE FUSION EN PLUS DU PSU DE BASE DE DONNÉES 11.2.0.4.6 POUR BOGUES 20647412 21534893
- Correctif 24010393 : DEMANDE DE FUSION EN PLUS DU PSU DE BASE DE DONNÉES 11.2.0.4.6 POUR BOGUES 12897813 21281961

- Correctif 19306797 : LE RÉTABLISSEMENT DE PULSATION N'EST PAS GÉNÉRÉ POUR LES HÔTES NON-RAC SI LA JOURNALISATION SUPPLÉMENTAIRE EST ACTIVÉE
- Correctif 19563715 : LOGMINER NE PROGRESSE PAS QUAND 4 GO DE MÉMOIRE OU PLUS SONT UTILISÉS DANS GOLDENGATE
- Correctif 20425790 : LES CORRECTIFS LOGMINER DEVRAIENT FONCTIONNER DE MANIÈRE TRANSPARENTE DANS UNE BDD ACTIVÉE SANS PARTITIONNEMENT
- Correctif 17031322 : 46719 : LES VARIABLES BIND RETOURNÉES PAR OCIXMLDBREWRITEXML NE CONSERVENT PAS LES ESPACES
- Correctif 30303921 : DEMANDE DE FUSION EN PLUS DU PSU DE BASE DE DONNÉES 11.2.0.4.190416 POUR BOGUES 29879564 14312810
- Correctif 30293609 : DEMANDE DE FUSION EN PLUS DU PSU DE BASE DE DONNÉES 11.2.0.4.190416 POUR BOGUES 29600521 23262847
- Correctif 26744595 : LGSB : APPLIQUER ABANDONS AVEC ORA-26786 (ROW-EXISTS) COLLISION AVEC HCC(PR)-NO HCC(SB)
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS

Correctif Oracle 30298532, publié en janvier 2020

Bogues corrigés :

```
18619917, 19309466, 28876684, 28855981, 18189036, 19781326, 13609098
16285691, 16756406, 18430495, 17323222, 29483723, 19915271, 19516448
14458214, 23713236, 23140259, 29434301, 22502493, 18272672, 16410570
16494615, 19174430, 21352646, 16901385, 16596890, 22243719, 18996843
21387964, 20334344, 17174582, 22250006, 17798953, 14015842, 18031668
15955387, 16832076, 16065166, 16579084, 25427662, 21179898, 11786053
15990359, 17982832, 18685892, 20142975, 24835538, 16315398, 20861693
17037130, 17284817, 17891946, 17279227, 17588480, 17291347, 16731148
21097043, 24528741, 22321741, 17165204, 26245237, 17891943, 17359610
17265217, 17465741, 22551446, 18191164, 16721594, 18614015, 27825893
18440095, 19769489, 20596234, 18482502, 16043574, 17360606, 22321756
19211724, 17392698, 19463893, 29033139, 17477958, 17040764, 18362222
19463897, 24624166, 17853456, 14521849, 17816865, 19692824, 21868720
17951233, 25505407, 17040527, 24975421, 19888853, 18009564, 20882568
20803583, 23026585, 18604692, 17622427, 16903536, 17865671, 29483771
17883081, 16228604, 17325413, 17082359, 12747740, 22168163, 16091637
20569094, 17468141, 30365745, 29962939, 19469538, 29633753, 20598042
16042673, 17437634, 23302839, 28734355, 19049453, 20387265, 16833527
21343775, 17297939, 16069901, 14285317, 22380919, 18436647, 23065323
21983325, 17853498, 24790914, 23571055, 16542886, 21286665, 17365043
17752995, 25914276, 17296856, 18783224, 22353199, 22083366, 28305362
16180763, 21419850, 23294548, 26679352, 13960236, 25423453, 18339044
17282229, 25600421, 18856999, 18259031, 28806384, 21354456, 23725036
18471685, 30237239, 17258090, 16344544, 17903598, 17011832, 18135678
18704244, 17786518, 19718981, 25655390, 17242746, 20250147, 19197175
17390431, 17835627, 17672719, 17393915, 21566639, 18765602, 21425496
26544823, 22228324, 29962927, 18682983, 25165496, 12816846, 18774543
18747196, 17824637, 19429927, 21429602, 16524926, 17343514, 19271443
17019345, 18681862, 17186905, 23330119, 17811438, 26474853, 17215560
16875449, 21380789, 17184721, 18508861, 19466309, 23330124, 17811429
17019356, 25654936, 17754782, 17752121, 22809871, 17201159, 18308268
19777862, 16198143, 29027694, 18828868, 17586955, 28076295, 22977256
16692232, 27374796, 21142837, 20869721, 17649265, 25879656, 21756699
19697993, 28364007, 17787259, 23628685, 23007241, 30252098, 27351628
18094246, 20031873, 17375354, 21698350, 21538567, 22683212, 16450169
17478145, 17311728, 17648596, 17308789, 22836801, 21756677, 18674047
14084247, 19788303, 22683225, 27534509, 16833845, 18948177, 17205719
```

```
21756661, 20004021, 17922254, 13837378, 18084625, 17912217, 11883252
24842886, 12982566, 26203182, 14176370, 14764829, 21847223, 16875230
28079127, 22568797, 17237521, 29511611, 25635149, 16934803, 17848897
20441797, 16613964, 18334586, 17288409, 17341326, 17449815, 15913355
16399083, 18740837, 20294666, 14565184, 21517440, 17614134, 19854503
14245531, 16194160, 18325460, 15979965, 30562923, 20671094, 27870645
25093656, 18247991, 16912439, 24433711, 19930276, 22092979, 20506715
23003979, 20506706, 13871092, 19272701, 17397545, 16785708, 19461270
21051862, 13829543, 16220077, 17008068, 18061914, 20448824, 30275359
18674024, 19689979, 24411921, 30275351, 17596908, 17036973, 17612828
20725343, 28199085, 23194294, 17630484, 21051858, 20017509, 21051852
17767676, 17232014, 22893153, 12611721, 25555252, 18356166, 17071721
25764020, 16863422, 21051840, 17267114, 18043064, 21538558, 26243698
20324049, 16392068, 18744139, 24348685, 26746894, 27072923, 14010183
16595641, 17080436, 17332800, 20777150, 21453153, 20299015, 18413820
18264060, 16819962, 22465352, 21351877, 21051833, 18673342, 30562907
30562909, 29200700, 27441326, 16571443, 18328509, 27567477, 18674465
16422541, 18306996, 17443671, 19359219, 21424824, 17478514, 21067387
16268425, 17381384, 18723434, 17235750, 23328639, 22195448, 24570598
21172913, 17655240, 18384391, 16992075, 22195441, 17025461, 30562891
16472716, 19289642, 21502702, 22195457, 20475845, 22148226, 26030218
18331850, 17945983, 13498382, 24652769, 18673304, 17610798, 19891090
25369547, 18456514, 8322815, 22657942, 17313525, 17050888, 18317531
17495022, 11733603, 18798250, 19285025, 18260550, 17390160, 18316692
19458377, 14368995, 17551063, 21343838, 12905058, 14735792, 28612674
16855292, 23315889, 13364795, 18235390, 18293054, 18673325, 19393542
14657740, 17393683, 17389192, 17783588, 17852463, 19358317, 17441661
14034426, 28254374, 20631274, 19207117, 26569225, 17518652, 24662775
19475971, 18282562, 17348614, 19827973, 17346671, 24476274, 22296366
13853126, 18273830, 17570606, 13558557, 26007010, 16685417, 18180390
14692762, 17027426, 18159793, 24476265, 23177648, 17851160, 16870214
18202441, 17227073, 20657411, 19006849, 20506699, 22606521, 28000269
23536835, 17761775, 20382309, 16306373, 19680952, 16850630, 17694209
26667015, 17877323, 18230522, 24563422, 17446237, 17889549, 17551674
16233738, 22730454, 17571039, 26667023, 19972570, 18849970, 21532755
20860659, 22905130, 21168487, 17016369, 17231779, 21263635, 21343897
27710072, 18522509, 23209741, 17484731, 21972320, 19972569, 19972568
17716305, 21059919, 19972566, 19972564, 26667032, 17394950, 20657441
17551699, 17006570, 18051556, 12364061, 18029658, 17546973, 18262334
19699191, 17227277, 18018515, 16943711, 17982555, 20828947, 18098207
18436307, 19584068, 16898135, 13936038, 19601762, 14054676, 25505394
18228645, 19013183, 25042823, 17721717, 17239687, 25248384, 25634317
20134113, 20273319, 28501075, 21063322, 17344412, 22507210, 16354467
21795111, 25505371, 16777840, 25879984, 17811456, 19730508, 17385178
18166013, 17484762, 10136473, 6599380, 20717359, 20296213, 27097854
13955826, 18193833, 17545847, 16837842, 18964939, 19871910, 25505382
17811447, 18554763, 21132297, 25957038, 20004087, 17889583, 19544839
26631046, 22507234, 24719736, 18868646, 17042658, 20627866, 14106803
13951456, 18139690, 18277454, 13680635, 25823754, 18554871, 20169408
18515268, 24908321, 17274537, 17602269, 26575788, 19032867, 17762296
14829250, 16929165, 14602788, 28849751, 21794615, 18899974, 18441944
29944660, 17811789, 20074391, 14852021, 17705023, 13645875, 24316947
16668584, 17786278, 25947799, 20879889, 19578350, 28022101, 22594718
16384983, 26439748, 17957017, 19121551, 17570240, 19788842, 18382302
27086138, 21330264, 21197626, 14338435, 13944971, 21656630, 18886413
17156148, 17936109, 20509482, 27255377, 24717859, 18762750, 21526048
24560906, 18096714, 17238511, 26078387, 27053456, 20144308, 18244962
19433930, 20476175, 19297917, 21174504, 18280813, 28819280, 17614227
28357401, 17006183, 18092127, 19727057, 17695685, 26039623, 22820579
20856766, 15861775, 17258582, 21668627, 19487147, 20925795, 28100487
26482376, 19554106, 21629064, 18199537, 18091059, 17299889, 21538485
17546761, 25775213, 26336977, 18155762, 16956380, 19207156, 14705949
23105538, 26198926, 19258504, 16314254, 17246576, 17655634, 16989630
20067212, 19721304, 19490948, 25077278, 18203835, 18203838, 18973907
18203837, 29483672, 19615136, 17587063, 18000422, 18641451, 18090142
21641760, 17019086, 30559616, 19373893, 18373438, 18641461, 17346091
```

```
21422580, 22351572, 18604493, 23008056, 22901797, 18610915, 17892268
17501491, 20907061, 14354737, 17835048, 21787056, 22195485, 22782647
17082983, 18641419, 16618694, 14133975, 22195492, 18331812, 18093615
24385983, 25897615, 20513399, 21281607, 13866822, 18841764, 17600719
17842825, 20558005, 17088068, 9756271, 22195465, 18440047, 19211433
21515534, 20331945, 22686674, 18384537, 18607546, 17254374, 18315328
23115139, 28790634, 21394225, 16360112, 22195477, 17726838, 18510194
17571306, 17302277, 24766121, 21842740, 17551709, 26910644, 17634921
25489607, 16538760
```

Version 11.2.0.4.v22

La version 11.2.0.4.v22 comprend les éléments suivants :

- Correctif 29913194 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS DE BASE DE DONNÉES 11.2.0.4.191015
- Correctif 30132974 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS OJVM 11.2.0.4.191015
- Correctif 29997937 : DSTv34 pour RDBMS (TZDATA2019G)
- Correctif 29997959 : DSTV34 OJVM (TZDATA2019B)
- Oracle GoldenGate : correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 19440386 : ÉCHEC DE DÉCLENCHEMENT D'ORA-1 POUR MISE À JOUR PACKAGE QUAND CONTRAINTE=IMMÉDIATE
- Correctif 19277336 : LE RÉPLICA INTÉGRÉ INVALIDE LES PACKAGES DÉPENDANTS ET GÉNÈRE UNE ERREUR ORA-4068
- Correctif 24286409 : DEMANDE DE FUSION EN PLUS DU PSU DE BASE DE DONNÉES 11.2.0.4.6 POUR BOGUES 20647412 21534893
- Correctif 24010393 : DEMANDE DE FUSION EN PLUS DU PSU DE BASE DE DONNÉES 11.2.0.4.6 POUR BOGUES 12897813 21281961
- Correctif 19306797 : LE RÉTABLISSEMENT DE PULSATION N'EST PAS GÉNÉRÉ POUR LES HÔTES NON-RAC SI LA JOURNALISATION SUPPLÉMENTAIRE EST ACTIVÉE
- Correctif 19563715 : LOGMINER NE PROGRESSE PAS QUAND 4 GO DE MÉMOIRE OU PLUS SONT UTILISÉS DANS GOLDENGATE
- Correctif 20425790 : LES CORRECTIFS LOGMINER DEVRAIENT FONCTIONNER DE MANIÈRE TRANSPARENTE DANS UNE BDD ACTIVÉE SANS PARTITIONNEMENT
- Correctif 17031322 : 46719 : LES VARIABLES BIND RETOURNÉES PAR OCIXMLDBREWRITEXML NE CONSERVENT PAS LES ESPACES
- Correctif 30303921 : DEMANDE DE FUSION EN PLUS DU PSU DE BASE DE DONNÉES 11.2.0.4.190416 POUR BOGUES 29879564 14312810
- Correctif 30293609 : DEMANDE DE FUSION EN PLUS DU PSU DE BASE DE DONNÉES 11.2.0.4.190416 POUR BOGUES 29600521 23262847
- Correctif 26744595 : LGSB : APPLIQUER ABANDONS AVEC ORA-26786 (ROW-EXISTS) COLLISION AVEC HCC(PR)-NO HCC(SB)
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS

Correctif Oracle 29913194, publié en octobre 2019

Bogues corrigés :

```
17184721, 21174504, 20169408, 21538558, 16091637, 18092127, 17381384
15979965, 20671094, 16731148, 16314254, 18441944, 13837378, 17835048
17291347, 23105538, 28254374, 13558557, 21656630, 21842740, 17008068
18382302, 17201159, 17853498, 25427662, 21197626, 17246576, 20717359
18356166, 18681862, 18440047, 20569094, 20031873, 16875449, 20387265
19788842, 17296856, 21330264, 14010183, 17648596, 17025461, 18886413
17551063, 24719736, 17258582, 17267114, 21063322, 22507210, 17912217
17889583, 18202441, 17040764, 17478145, 16524926, 25655390, 19358317
22730454, 22148226, 18747196, 26544823, 18641419, 17036973, 18948177
17811789, 16542886, 14285317, 18009564, 17359610, 16618694, 8322815
16832076, 18247991, 16692232, 22507234, 28022101, 17570240, 13871092
24624166, 26631046, 24348685, 19429927, 17848897, 17441661, 14034426
17465741, 20273319, 19207156, 16596890, 17437634, 20506706, 18510194
21343897, 28849751, 18339044, 21453153, 17951233, 21795111, 22321741
18430495, 21787056, 22380919, 20506715, 19692824, 19469538, 17811429
17903598, 19721304, 11786053, 29511611, 18230522, 19554106, 19458377
21281607, 17612828, 6599380, 18029658, 22092979, 19516448, 17040527
22321756, 17811438, 18641461, 18682983, 14657740, 25635149, 21502702
13364795, 19490948, 21387964, 17346671, 17588480, 22351572, 18235390
26474853, 18849970, 17982832, 17889549, 19309466, 16472716, 23008056
20627866, 24908321, 20134113, 25775213, 20596234, 18331850, 18641451
17019356, 20882568, 17344412, 19461270, 21179898, 17546761, 24842886
17231779, 14521849, 18203835, 18203838, 18964939, 18203837, 17313525
22195457, 18139690, 16837842, 14106803, 22296366, 17842825, 22657942
21352646, 16360112, 22594718, 20657441, 22195441, 17389192, 26198926
14565184, 19781326, 17019345, 17205719, 18740837, 18440095, 14764829
14354737, 22195448, 17019086, 13944971, 16571443, 21868720, 17186905
17080436, 18673342, 28501075, 22905130, 17027426, 19972569, 27374796
19972568, 16833845, 19972566, 20144308, 17282229, 19972564, 16870214
16410570, 21629064, 19615136, 21354456, 26039623, 19871910, 17390431
18762750, 23007241, 25248384, 16613964, 18098207, 17957017, 17484762
18471685, 19730508, 18264060, 21538485, 17323222, 17754782, 17600719
18317531, 17852463, 17596908, 17655634, 18166013, 16228604, 20074391
27053456, 24790914, 19972570, 26482376, 20856766, 18090142, 19891090
18996843, 16042673, 19854503, 17835627, 22901797, 20334344, 17393683
20861693, 18000422, 17551709, 26575788, 23315889, 20506699, 19006849
18277454, 18456514, 17258090, 19174430, 20657411, 17174582, 25654936
17242746, 27097854, 16399083, 17824637, 21132297, 17762296, 22465352
22168163, 28612674, 18604692, 17397545, 16450169, 12364061, 20067212
19373893, 18856999, 19211724, 19463893, 19463897, 27351628, 21343775
17853456, 18373438, 18673304, 20004021, 28000269, 26030218, 21668627
16194160, 17477958, 23140259, 16538760, 12982566, 24570598, 20828947
27255377, 18259031, 20296213, 21425496, 28855981, 18293054, 17610798
19699191, 23065323, 17311728, 18135678, 18774543, 23294548, 16785708
10136473, 22551446, 19777862, 24560906, 17786518, 18315328, 25879984
18334586, 12747740, 22250006, 18096714, 19032867, 21641760, 17390160
18899974, 17232014, 20598042, 16354467, 26245237, 26679352, 17484731
18673325, 16422541, 18155762, 19827973, 14015842, 22683225, 17726838
18554871, 23177648, 18051556, 20803583, 18282562, 17922254, 15990359
21972320, 16855292, 16668584, 21343838, 20299015, 29483672, 17446237
18043064, 18093615, 17694209, 23713236, 17288409, 18308268, 20475845
17274537, 13955826, 16934803, 18841764, 17634921, 17501491, 16315398
23725036, 22683212, 17006183, 13829543, 18191164, 26746894, 22809871
17655240, 28819280, 19393542, 18384391, 29633753, 21538567, 17695685
16198143, 21847223, 28199085, 25823754, 17892268, 20142975, 19584068
17165204, 25165496, 27072923, 18604493, 18508861, 21756699, 18554763
16901385, 21532755, 18189036, 17443671, 17385178, 14829250, 17936109
20476175, 20925795, 20509482, 17478514, 27441326, 16850630, 13951456
16595641, 14054676, 15861775, 21142837, 16912439, 17299889, 17297939
23003979, 16833527, 18619917, 17798953, 17630484, 19697993, 17816865
25914276, 18607546, 17571306, 21286665, 16898135, 17341326, 16819962
26910644, 17851160, 17586955, 20558005, 19049453, 21051840, 17587063
16956380, 18328509, 25042823, 14735792, 25423453, 14133975, 29033139
19718981, 18061914, 18522509, 16233738, 17518652, 21051833, 18765602
20294666, 23194294, 20860659, 18272672, 20324049, 18199537, 17332800
13609098, 22502493, 18384537, 14338435, 17945983, 27710072, 16392068
```

```
21067387, 17752995, 21097043, 21051862, 16863422, 17237521, 25505382
29483723, 18244962, 19544839, 28357401, 19433930, 24433711, 24717859
17156148, 18973907, 23026585, 17449815, 17877323, 18180390, 17088068
17037130, 20004087, 21422580, 19466309, 11733603, 25505371, 18610915
21051858, 18084625, 29027694, 18674024, 26243698, 21051852, 18091059
18306996, 16306373, 25369547, 19930276, 17787259, 19915271, 18193833
20631274, 20513399, 16344544, 26439748, 25879656, 14692762, 18614015
22782647, 17346091, 18413820, 19297917, 18228645, 17721717, 13960236
18685892, 18436307, 11883252, 19888853, 21756677, 17891943, 19475971
22353199, 16384983, 19121551, 27825893, 25634317, 12816846, 17982555
17761775, 17227073, 13936038, 22243719, 17265217, 25505394, 17071721
16721594, 18262334, 21756661, 17891946, 15913355, 17672719, 17602269
17239687, 17042658, 25555252, 17238511, 21059919, 17811456, 17284817
17752121, 20879889, 28806384, 21380789, 19601762, 17394950, 17011832
28305362, 16579084, 22195465, 16875230, 14602788, 28790634, 18325460
27567477, 30275351, 26569225, 24476265, 24476274, 12611721, 18674465
16903536, 17006570, 19689979, 28076295, 16043574, 18783224, 22836801
14705949, 24662775, 16494615, 21526048, 17392698, 19197175, 16069901
17811447, 29200700, 27870645, 28876684, 17308789, 24835538, 22195477
17865671, 17343514, 19013183, 17325413, 18316692, 16180763, 30275359
17348614, 14368995, 21983325, 17393915, 16285691, 19788303, 19211433
20331945, 17883081, 17705023, 24316947, 17614227, 23571055, 19578350
22195485, 14084247, 24975421, 26078387, 23115139, 13645875, 23328639
16777840, 19727057, 21698350, 14852021, 18744139, 18674047, 17716305
19285025, 18482502, 17622427, 19289642, 27534509, 25947799, 22195492
14458214, 20869721, 21172913, 17767676, 18723434, 25505407, 17786278
19258504, 17082983, 17365043, 21351877, 13498382, 18331812, 16065166
25489607, 16685417, 21566639, 18031668, 22893153, 17551674, 16943711
19272701, 21517440, 25897615, 17649265, 13866822, 18094246, 24528741
17783588, 14245531, 17082359, 18280813, 26007010, 20448824, 23330119
16268425, 19487147, 25600421, 18018515, 17302277, 17215560, 24411921
19271443, 25764020, 14176370, 17016369, 20777150, 16756406, 23330124
22977256, 20441797, 19769489, 28100487, 17545847, 25093656, 18260550
13853126, 17227277, 17551699, 23536835, 30237239, 25957038, 24652769
20725343, 19207117, 9756271, 17495022, 18868646, 17614134, 26667023
17546973, 19680952, 18704244, 26667015, 17050888, 18273830, 18828868
17360606, 16992075, 24563422, 17375354, 12905058, 18362222, 21429602
17254374, 27086138, 28364007, 26667032, 17571039, 17468141, 18436647
17570606, 17235750, 21168487, 17279227, 16220077, 16929165
```

Version 11.2.0.4.v21

La version 11.2.0.4.v21 comprend les éléments suivants :

- Correctif 29497421 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS DATABASE 11.2.0.4.190716
- Correctif 29610422 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS OJVM 11.2.0.4.190716
- Correctif 28852325 : DSTv33 pour RDBMS (TZDATA2018G)
- Correctif 28852334 : DSTv33 pour OJVM (TZDATA2018G)
- Correctif 30018733 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS

Correctif Oracle 29497421, publié en juillet 2019

Bogues corrigés :

```
17184721, 21174504, 20169408, 21538558, 16091637, 18092127, 17381384
15979965, 20671094, 16731148, 16314254, 18441944, 13837378, 17835048
23105538, 17291347, 28254374, 13558557, 21842740, 21656630, 17008068
18382302, 17201159, 25427662, 17853498, 21197626, 20717359, 17246576
18356166, 18681862, 18440047, 20569094, 20031873, 16875449, 20387265
19788842, 17296856, 21330264, 14010183, 17648596, 17025461, 18886413
17551063, 17258582, 24719736, 17267114, 21063322, 22507210, 17912217
17889583, 18202441, 17040764, 17478145, 16524926, 25655390, 19358317
22730454, 22148226, 18747196, 26544823, 18641419, 17036973, 18948177
17811789, 16542886, 14285317, 18009564, 17359610, 16618694, 8322815
16832076, 18247991, 16692232, 22507234, 28022101, 17570240, 13871092
24624166, 26631046, 24348685, 19429927, 17848897, 17441661, 14034426
17465741, 20273319, 19207156, 16596890, 17437634, 18510194, 21343897
20506706, 28849751, 18339044, 21453153, 17951233, 21795111, 22321741
18430495, 21787056, 22380919, 19692824, 19469538, 20506715, 17811429
17903598, 19721304, 11786053, 29511611, 18230522, 19554106, 19458377
21281607, 17612828, 6599380, 18029658, 22092979, 17040527, 22321756
17811438, 18641461, 18682983, 21502702, 14657740, 25635149, 13364795
19490948, 21387964, 17346671, 17588480, 22351572, 18235390, 18849970
26474853, 17889549, 19309466, 16472716, 23008056, 20627866, 24908321
20134113, 25775213, 20596234, 18331850, 18641451, 20882568, 17019356
17344412, 19461270, 21179898, 17546761, 24842886, 17231779, 14521849
18203835, 18203838, 18964939, 18203837, 17313525, 22195457, 18139690
16837842, 14106803, 22296366, 17842825, 22657942, 21352646, 16360112
22594718, 20657441, 22195441, 17389192, 26198926, 14565184, 17019345
19781326, 17205719, 18740837, 18440095, 14764829, 14354737, 22195448
17019086, 13944971, 16571443, 21868720, 17186905, 17080436, 18673342
28501075, 22905130, 17027426, 19972569, 27374796, 19972568, 16833845
19972566, 20144308, 17282229, 19972564, 16870214, 16410570, 21629064
19615136, 19871910, 21354456, 26039623, 17390431, 18762750, 23007241
25248384, 16613964, 18098207, 17957017, 17484762, 18471685, 19730508
18264060, 21538485, 17323222, 17754782, 17600719, 18317531, 17852463
17596908, 17655634, 18166013, 16228604, 20074391, 27053456, 24790914
19972570, 26482376, 20856766, 18090142, 19891090, 18996843, 16042673
19854503, 17835627, 22901797, 20334344, 17393683, 20861693, 18000422
17551709, 26575788, 23315889, 20506699, 19006849, 18277454, 18456514
17258090, 19174430, 20657411, 17174582, 25654936, 17242746, 27097854
16399083, 17824637, 21132297, 22465352, 17762296, 22168163, 28612674
18604692, 17397545, 16450169, 12364061, 20067212, 18856999, 19211724
19463893, 19463897, 27351628, 21343775, 17853456, 18373438, 18673304
20004021, 26030218, 28000269, 21668627, 16194160, 17477958, 23140259
16538760, 12982566, 24570598, 20828947, 27255377, 18259031, 20296213
28855981, 21425496, 18293054, 17610798, 19699191, 23065323, 17311728
18135678, 18774543, 23294548, 16785708, 10136473, 19777862, 22551446
24560906, 17786518, 18315328, 25879984, 18334586, 22250006, 12747740
18096714, 19032867, 21641760, 17390160, 18899974, 17232014, 20598042
26679352, 26245237, 16354467, 17484731, 18673325, 16422541, 18155762
19827973, 14015842, 22683225, 17726838, 18554871, 23177648, 18051556
20803583, 18282562, 17922254, 15990359, 21972320, 16855292, 16668584
21343838, 20299015, 17446237, 18043064, 18093615, 23713236, 17694209
17288409, 20475845, 18308268, 17274537, 13955826, 16934803, 17634921
17501491, 16315398, 23725036, 22683212, 17006183, 13829543, 18191164
26746894, 22809871, 17655240, 28819280, 18384391, 19393542, 21538567
17695685, 16198143, 21847223, 25823754, 17892268, 20142975, 19584068
17165204, 25165496, 18604493, 18508861, 21756699, 18554763, 16901385
21532755, 18189036, 17443671, 17385178, 14829250, 17936109, 20925795
20509482, 17478514, 27441326, 16850630, 13951456, 16595641, 14054676
15861775, 21142837, 16912439, 17299889, 17297939, 23003979, 16833527
18619917, 17798953, 19697993, 17816865, 25914276, 18607546, 17571306
21286665, 16898135, 17341326, 16819962, 26910644, 17851160, 17586955
20558005, 19049453, 21051840, 17587063, 16956380, 25042823, 14735792
18328509, 25423453, 14133975, 29033139, 19718981, 18061914, 16233738
18522509, 17518652, 21051833, 20294666, 18765602, 23194294, 20860659
18272672, 20324049, 18199537, 17332800, 13609098, 22502493, 18384537
14338435, 27710072, 17945983, 16392068, 21067387, 17752995, 21097043
21051862, 16863422, 17237521, 25505382, 18244962, 28357401, 19544839
```

```
19433930, 24433711, 24717859, 17156148, 18973907, 23026585, 17449815
17877323, 18180390, 17088068, 17037130, 20004087, 21422580, 19466309
11733603, 25505371, 18610915, 21051858, 18084625, 29027694, 18674024
26243698, 21051852, 18091059, 18306996, 25369547, 16306373, 19930276
17787259, 18193833, 19915271, 20513399, 20631274, 16344544, 26439748
25879656, 14692762, 18614015, 22782647, 17346091, 18413820, 19297917
18228645, 17721717, 13960236, 18685892, 18436307, 11883252, 19888853
21756677, 17891943, 19475971, 22353199, 16384983, 19121551, 27825893
25634317, 12816846, 17982555, 17761775, 13936038, 17227073, 22243719
17265217, 25505394, 17071721, 16721594, 18262334, 21756661, 17891946
15913355, 17672719, 17602269, 17239687, 17042658, 25555252, 17238511
21059919, 17811456, 17284817, 17752121, 20879889, 28806384, 19601762
21380789, 17394950, 28305362, 17011832, 16579084, 22195465, 16875230
14602788, 28790634, 18325460, 27567477, 26569225, 24476265, 24476274
12611721, 18674465, 16903536, 17006570, 19689979, 28076295, 16043574
18783224, 22836801, 24662775, 16494615, 21526048, 17392698, 19197175
16069901, 29200700, 17811447, 27870645, 28876684, 17308789, 24835538
22195477, 17865671, 17343514, 19013183, 17325413, 18316692, 16180763
17348614, 14368995, 21983325, 17393915, 16285691, 19211433, 20331945
17883081, 17705023, 24316947, 23571055, 17614227, 19578350, 22195485
14084247, 24975421, 26078387, 23115139, 13645875, 23328639, 16777840
21698350, 19727057, 14852021, 18744139, 18674047, 17716305, 19285025
18482502, 17622427, 19289642, 27534509, 25947799, 22195492, 14458214
20869721, 21172913, 17767676, 18723434, 25505407, 17786278, 19258504
17082983, 17365043, 21351877, 13498382, 18331812, 16065166, 25489607
16685417, 21566639, 18031668, 22893153, 17551674, 16943711, 19272701
21517440, 25897615, 17649265, 13866822, 18094246, 24528741, 17783588
14245531, 17082359, 18280813, 26007010, 20448824, 23330119, 16268425
19487147, 25600421, 18018515, 17302277, 17215560, 24411921, 19271443
25764020, 14176370, 17016369, 20777150, 16756406, 23330124, 22977256
20441797, 19769489, 28100487, 17545847, 25093656, 18260550, 13853126
17227277, 17551699, 23536835, 25957038, 24652769, 20725343, 19207117
9756271, 17495022, 18868646, 17614134, 26667023, 17546973, 19680952
18704244, 26667015, 17050888, 18273830, 18828868, 17360606, 16992075
24563422, 17375354, 12905058, 18362222, 21429602, 17254374, 27086138
26667032, 28364007, 17571039, 17468141, 18436647, 17570606, 17235750
21168487, 17279227, 16220077, 16929165
```

Version 11.2.0.4.v20

La version 11.2.0.4.v20 inclut les éléments suivants :

- Correctif 29141056 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS DATABASE 11.2.0.4.190416
- Correctif 29251270 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS OJVM 11.2.0.4.190416
- Correctif 28852325 : DSTv33 pour RDBMS (TZDATA2018G)
- Correctif 28852334 : DSTv33 pour OJVM (TZDATA2018G)
- Correctif 29638593 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 28730253 : PRISE EN CHARGE DE LA NOUVELLE ÈRE REIWA POUR LE CALENDRIER IMPÉRIAL JAPONAIS

Correctif Oracle 22768427, publié en avril 2019

Bogues corrigés :

```
17184721, 21174504, 21538558, 16091637, 18092127, 17381384, 15979965
20671094, 16731148, 16314254, 13837378, 18441944, 17291347, 23105538
17835048, 28254374, 13558557, 21656630, 21842740, 17008068, 18382302
```

```
17201159, 25427662, 17853498, 21197626, 20717359, 17246576, 18356166
18681862, 18440047, 20569094, 20031873, 16875449, 20387265, 19788842
17296856, 21330264, 14010183, 17648596, 18886413, 17025461, 17551063
24719736, 17267114, 21063322, 22507210, 17912217, 17889583, 18202441
17040764, 17478145, 16524926, 25655390, 19358317, 22730454, 22148226
18747196, 26544823, 18641419, 17036973, 18948177, 17811789, 16542886
14285317, 18009564, 17359610, 16618694, 8322815, 16832076, 18247991
16692232, 22507234, 17570240, 13871092, 24624166, 26631046, 19429927
24348685, 17848897, 17441661, 14034426, 17465741, 20273319, 19207156
16596890, 18510194, 17437634, 21343897, 20506706, 28849751, 18339044
21453153, 17951233, 21795111, 22321741, 18430495, 21787056, 22380919
19469538, 19692824, 20506715, 17811429, 17903598, 19721304, 11786053
18230522, 19554106, 19458377, 21281607, 17612828, 6599380, 22092979
17040527, 22321756, 17811438, 18641461, 18682983, 14657740, 25635149
13364795, 19490948, 21387964, 17346671, 17588480, 22351572, 18235390
18849970, 26474853, 17889549, 19309466, 20627866, 23008056, 16472716
24908321, 20134113, 25775213, 20596234, 18331850, 18641451, 20882568
17019356, 17344412, 19461270, 21179898, 17546761, 24842886, 17231779
14521849, 18203835, 18203838, 18964939, 18203837, 17313525, 22195457
18139690, 16837842, 14106803, 22296366, 17842825, 22657942, 21352646
16360112, 22594718, 20657441, 22195441, 17389192, 26198926, 14565184
19781326, 17019345, 17205719, 18740837, 18440095, 14764829, 14354737
22195448, 17019086, 13944971, 16571443, 21868720, 17186905, 17080436
18673342, 22905130, 17027426, 27374796, 19972569, 19972568, 20144308
19972566, 17282229, 19972564, 16870214, 16410570, 21629064, 19615136
21354456, 26039623, 17390431, 18762750, 23007241, 16613964, 17957017
18098207, 17484762, 18471685, 19730508, 18264060, 21538485, 17323222
17754782, 17600719, 18317531, 17852463, 17596908, 17655634, 18166013
16228604, 20074391, 27053456, 24790914, 19972570, 20856766, 18090142
19891090, 18996843, 16042673, 19854503, 17835627, 22901797, 20334344
17393683, 20861693, 18000422, 17551709, 26575788, 23315889, 20506699
19006849, 18277454, 18456514, 19174430, 17258090, 17174582, 25654936
17242746, 27097854, 16399083, 17824637, 21132297, 22465352, 17762296
22168163, 18604692, 17397545, 16450169, 12364061, 20067212, 18856999
19211724, 19463893, 27351628, 19463897, 21343775, 17853456, 18373438
18673304, 20004021, 28000269, 26030218, 21668627, 16194160, 17477958
23140259, 16538760, 12982566, 24570598, 20828947, 27255377, 18259031
20296213, 21425496, 28855981, 18293054, 17610798, 19699191, 23065323
17311728, 18135678, 18774543, 23294548, 16785708, 10136473, 24560906
19777862, 22551446, 17786518, 25879984, 18315328, 18334586, 12747740
18096714, 19032867, 21641760, 17390160, 18899974, 17232014, 20598042
26679352, 26245237, 16354467, 17484731, 18673325, 16422541, 18155762
19827973, 14015842, 22683225, 17726838, 18554871, 23177648, 18051556
20803583, 18282562, 21972320, 15990359, 17922254, 16855292, 16668584
21343838, 20299015, 17446237, 18043064, 18093615, 23713236, 17694209
17288409, 20475845, 18308268, 17274537, 13955826, 16934803, 17634921
17501491, 16315398, 23725036, 22683212, 17006183, 13829543, 18191164
26746894, 22809871, 17655240, 28819280, 18384391, 19393542, 21538567
16198143, 21847223, 25823754, 17892268, 20142975, 19584068, 17165204
25165496, 18604493, 21756699, 18508861, 18554763, 16901385, 21532755
18189036, 17443671, 17385178, 14829250, 17936109, 20925795, 20509482
17478514, 27441326, 16850630, 13951456, 16595641, 14054676, 15861775
21142837, 16912439, 17299889, 17297939, 23003979, 16833527, 18619917
17798953, 19697993, 17816865, 25914276, 18607546, 17571306, 21286665
16898135, 16819962, 17341326, 26910644, 17851160, 17586955, 20558005
19049453, 21051840, 17587063, 16956380, 18328509, 25423453, 14133975
29033139, 19718981, 18061914, 18522509, 17518652, 21051833, 20294666
18765602, 20860659, 18272672, 20324049, 18199537, 17332800, 13609098
22502493, 18384537, 14338435, 17945983, 16392068, 21067387, 17752995
21051862, 16863422, 17237521, 25505382, 18244962, 19544839, 24433711
24717859, 17156148, 18973907, 23026585, 17449815, 17877323, 18180390
17088068, 17037130, 20004087, 21422580, 19466309, 11733603, 25505371
18610915, 21051858, 18084625, 29027694, 18674024, 26243698, 21051852
18091059, 18306996, 25369547, 16306373, 17787259, 18193833, 19915271
20513399, 20631274, 26439748, 16344544, 25879656, 14692762, 18614015
22782647, 17346091, 18228645, 17721717, 13960236, 18685892, 18436307
```

```
11883252, 19888853, 21756677, 17891943, 19475971, 22353199, 16384983
19121551, 25634317, 27825893, 12816846, 17982555, 17761775, 17227073
22243719, 17265217, 25505394, 17071721, 16721594, 18262334, 21756661
17891946, 15913355, 17672719, 17602269, 17239687, 17042658, 25555252
17238511, 21059919, 17811456, 17284817, 17752121, 20879889, 28806384
21380789, 17394950, 17011832, 16579084, 22195465, 14602788, 28790634
18325460, 27567477, 26569225, 24476265, 24476274, 12611721, 18674465
16903536, 17006570, 19689979, 28076295, 16043574, 18783224, 24662775
16494615, 21526048, 17392698, 19197175, 16069901, 17811447, 27870645
28876684, 17308789, 24835538, 22195477, 17865671, 17343514, 19013183
17325413, 18316692, 16180763, 17348614, 14368995, 21983325, 17393915
16285691, 19211433, 20331945, 17883081, 17705023, 24316947, 17614227
19578350, 22195485, 14084247, 24975421, 26078387, 23115139, 13645875
16777840, 19727057, 14852021, 18744139, 18674047, 17716305, 19285025
18482502, 17622427, 19289642, 27534509, 25947799, 22195492, 14458214
20869721, 21172913, 17767676, 18723434, 25505407, 17786278, 19258504
17082983, 17365043, 21351877, 13498382, 18331812, 16065166, 25489607
16685417, 18031668, 22893153, 17551674, 16943711, 19272701, 21517440
25897615, 17649265, 13866822, 18094246, 24528741, 17783588, 14245531
17082359, 26007010, 18280813, 20448824, 23330119, 16268425, 19487147
25600421, 18018515, 17302277, 17215560, 24411921, 19271443, 25764020
14176370, 17016369, 20777150, 16756406, 23330124, 22977256, 20441797
19769489, 28100487, 17545847, 25093656, 18260550, 13853126, 17227277
17551699, 23536835, 25957038, 24652769, 20725343, 19207117, 9756271
18868646, 17614134, 26667023, 17546973, 19680952, 18704244, 26667015
17050888, 18273830, 18828868, 17360606, 16992075, 24563422, 17375354
12905058, 18362222, 21429602, 17254374, 26667032, 28364007, 27086138
17571039, 17468141, 18436647, 17570606, 17235750, 21168487, 17279227
16220077, 16929165
```

Version 11.2.0.4.v19

La version 11.2.0.4.v19 inclut les éléments suivants :

- Correctif 28729262 : Mise à jour d'ensemble de correctifs Oracle Database 11.2.0.4.190115
- Correctif 28790660 : Mise à jour d'ensemble de correctifs Oracle JVM 11.2.0.4.190115
- Correctif 28125601 : DSTv32 pour RDBMS (TZDATA2018E)
- Correctif 27015468 : DSTv32 pour OJVM (TZDATA2018E)
- Correctif 27216420 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS

Correctif Oracle 28729262, publié en janvier 2019

Bogues corrigés :

```
17288409, 21051852, 24316947, 17811429, 17205719, 18607546, 25654936
17484762, 17816865, 20506699, 24835538, 25957038, 19692824, 23330119
17922254, 17754782, 13364795, 16934803, 17311728, 18604692, 20387265
26679352, 17284817, 17441661, 20671094, 24560906, 16992075, 25635149
17446237, 14015842, 19972569, 21756677, 17375354, 17449815, 20925795
21538558, 17019086, 19463897, 26575788, 13866822, 17235750, 17982555
17478514, 18317531, 14338435, 18235390, 19461270, 20803583, 13944971
19475971, 20142975, 17811789, 16929165, 18704244, 24662775, 20506706
17546973, 21422580, 17359610, 20334344, 14054676, 25489607, 17088068
17570606, 18264060, 17346091, 17343514, 21538567, 19680952, 18471685
19211724, 21132297, 23105538, 13951456, 25775213, 16315398, 21847223
18744139, 16850630, 23177648, 19049453, 18673304, 18090142, 17883081
19915271, 18641419, 18262334, 25600421, 17006183, 16065166, 18277454
18685892, 16833527, 10136473, 18051556, 17865671, 25879984, 18554871
```

```
17852463, 18774543, 17853498, 18334586, 19487147, 20879889, 17551709
17588480, 19827973, 17344412, 17842825, 18828868, 20509482, 17025461
13609098, 19429927, 26039623, 11883252, 17239687, 16410570, 23007241
17602269, 19197175, 22195457, 18316692, 17313525, 12611721, 21174504
19544839, 18964939, 20294666, 17600719, 26667015, 18191164, 17571306
19393542, 18482502, 20777150, 27086138, 19466309, 22243719, 17165204
17040527, 18098207, 16785708, 24790914, 19891090, 17465741, 16180763
17174582, 12982566, 16777840, 27097854, 19463893, 22195465, 16875449
22148226, 12816846, 17237521, 6599380, 19358317, 17811438, 25505394
17811447, 21983325, 17945983, 18762750, 16912439, 17184721, 18061914
20598042, 26631046, 21380789, 17282229, 18948177, 18331850, 21142837
18202441, 17082359, 18723434, 19554106, 21532755, 21972320, 25505371
20273319, 14034426, 18339044, 19458377, 17752995, 20448824, 17891943
17767676, 17258090, 16668584, 18384391, 21063322, 17040764, 17381384
15913355, 18356166, 14084247, 20596234, 21641760, 20506715, 13853126
21756661, 18203837, 18610915, 14245531, 16043574, 21756699, 22195441
17848897, 17877323, 26667032, 28790634, 19272701, 21453153, 20569094
17468141, 17786518, 20861693, 17912217, 17037130, 16956380, 18155762
17478145, 17394950, 18189036, 18641461, 17551674, 18619917, 17027426
17019356, 21352646, 16268425, 24476274, 22195492, 19584068, 26544823
18436307, 22507210, 17265217, 13498382, 17634921, 19469538, 21526048
19258504, 23003979, 16354467, 18043064, 19174430, 20004087, 17443671
22195485, 18000422, 22321756, 20004021, 17571039, 27053456, 25897615
16832076, 21067387, 22905130, 16344544, 21429602, 18009564, 14354737
18135678, 21286665, 18614015, 14521849, 20441797, 28876684, 18362222
25655390, 16472716, 17835048, 17050888, 17936109, 14010183, 17325413
18747196, 19207156, 17231779, 21842740, 17761775, 16721594, 17082983
20067212, 21179898, 17279227, 17302277, 18084625, 20717359, 24624166
15990359, 24842886, 26746894, 18203835, 23026585, 17297939, 17811456
16731148, 22380919, 21168487, 14133975, 17215560, 13829543, 18740837
17694209, 17385178, 18091059, 8322815, 18259031, 17586955, 19689979
25165496, 28254374, 17201159, 17655634, 18331812, 19730508, 17551699
17648596, 18868646, 16220077, 16069901, 17393915, 17348614, 17957017
17274537, 18096714, 17308789, 18436647, 14285317, 19289642, 14764829
17622427, 18328509, 23115139, 16943711, 22195477, 22502493, 14368995
17346671, 18996843, 17783588, 18604493, 21343838, 16618694, 17672719
18856999, 18783224, 17851160, 17546761, 22168163, 17798953, 18273830
22092979, 16596890, 19972566, 13871092, 20828947, 26667023, 17726838
16384983, 22296366, 17360606, 13645875, 22321741, 16542886, 18199537
25879656, 25634317, 21787056, 23140259, 17889549, 21172913, 14565184
26245237, 20475845, 27825893, 17071721, 21281607, 17610798, 18308268
20299015, 21343897, 22893153, 22594718, 28076295, 20657441, 17397545
18230522, 16360112, 19769489, 12905058, 18641451, 12747740, 18430495
25423453, 17016369, 17042658, 14602788, 17551063, 26243698, 19972568
21517440, 23725036, 19788842, 18508861, 14657740, 17332800, 13837378
17186905, 19972564, 17019345, 19699191, 18315328, 27441326, 17437634
24570598, 22353199, 18093615, 19006849, 28806384, 17392698, 19013183
17296856, 18674024, 26569225, 17232014, 16855292, 21051840, 14692762
17762296, 17705023, 23294548, 22351572, 22507234, 19121551, 20324049
21330264, 26198926, 19854503, 23315889, 26030218, 26910644, 21868720
19309466, 27567477, 25764020, 18681862, 17365043, 17390160, 18554763
20031873, 20558005, 24717859, 21795111, 18456514, 13955826, 16306373
18139690, 17501491, 17752121, 17299889, 21668627, 23713236, 24652769
17889583, 18673325, 22551446, 17242746, 18293054, 18674465, 19721304
19211433, 19888853, 25914276, 24563422, 17951233, 18094246, 17649265
19615136, 17011832, 17477958, 16870214, 18522509, 20631274, 16091637
17323222, 16595641, 16524926, 18228645, 17484731, 18282562, 17596908
18272672, 18031668, 17156148, 16494615, 22683225, 20869721, 17545847
25093656, 28819280, 18682983, 17655240, 24528741, 17614134, 13558557
25427662, 17341326, 22465352, 29033139, 17891946, 17716305, 22657942
27374796, 16392068, 18440095, 19271443, 21351877, 20513399, 18092127
17614227, 18440047, 18849970, 14106803, 16903536, 20725343, 18973907
18673342, 17389192, 25505382, 22809871, 19032867, 17612828, 17006570
16194160, 25369547, 25505407, 16685417, 17721717, 21354456, 17390431
17570240, 16863422, 13960236, 28100487, 18325460, 17008068, 19727057
28855981, 16422541, 17267114, 19972570, 18244962, 21538485, 18203838
```

```
18765602, 16198143, 17246576, 14829250, 28364007, 17835627, 20860659
21629064, 18247991, 14458214, 21051862, 17786278, 16692232, 17227277
24348685, 16042673, 24476265, 24975421, 22901797, 16314254, 19285025
16228604, 16756406, 14176370, 16837842, 20144308, 17393683, 23536835
25823754, 18899974, 17787259, 24719736, 20331945, 26078387, 20074391
19490948, 15861775, 16399083, 25947799, 25555252, 18018515, 22683212
18260550, 21051858, 17080436, 16613964, 17036973, 16579084, 24433711
18384537, 27870645, 18280813, 20296213, 16901385, 15979965, 17518652
23330124, 20856766, 18441944, 16450169, 9756271, 27534509, 22730454
19718981, 17291347, 17892268, 11733603, 16285691, 17587063, 21343775
18180390, 16538760, 26474853, 18193833, 21387964, 21051833, 17238511
19777862, 17824637, 23065323, 21656630, 19697993, 17903598, 16571443
18306996, 18166013, 19578350, 14852021, 18674047, 17853456, 12364061
24411921, 19207117, 22195448
```

Version 11.2.0.4.v18

La version 11.2.0.4.v18 inclut les éléments suivants :

- Correctif 28204707 : PSU Oracle Database 11.2.0.4.181016
- Correctif 28440700 : PSU Oracle JVM 11.2.0.4.181016
- Correctif 28125601 : DSTv32 pour RDBMS (TZDATA2018E)
- Correctif 27015468 : DSTv32 pour OJVM (TZDATA2018E)
- Correctif 27216420 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Les correctifs 27659043 et 19692824 sont maintenant inclus dans la mise à jour d'ensemble de correctifs d'Oracle Database

Correctif Oracle 28204707, publié en octobre 2018

Bogues corrigés :

```
17288409, 21051852, 24316947, 17811429, 17205719, 18607546, 25654936
17484762, 17816865, 20506699, 24835538, 25957038, 19692824, 23330119
17922254, 17754782, 13364795, 16934803, 17311728, 18604692, 26679352
20387265, 17284817, 17441661, 20671094, 24560906, 25635149, 16992075
17446237, 14015842, 19972569, 21756677, 17375354, 21538558, 20925795
17449815, 17019086, 19463897, 26575788, 13866822, 17235750, 17982555
17478514, 18317531, 14338435, 18235390, 19461270, 20803583, 13944971
19475971, 20142975, 17811789, 16929165, 18704244, 24662775, 20506706
17359610, 17546973, 21422580, 20334344, 14054676, 25489607, 17570606
17088068, 17346091, 18264060, 17343514, 21538567, 19680952, 18471685
19211724, 21132297, 25775213, 13951456, 16315398, 21847223, 18744139
16850630, 23177648, 19049453, 18090142, 18673304, 17883081, 19915271
18641419, 18262334, 25600421, 17006183, 16065166, 18277454, 18685892
16833527, 10136473, 18051556, 17865671, 25879984, 18554871, 17852463
18774543, 17853498, 18334586, 19487147, 20879889, 17551709, 17588480
19827973, 17344412, 17842825, 18828868, 20509482, 17025461, 26039623
19429927, 13609098, 11883252, 16410570, 17239687, 23007241, 17602269
19197175, 22195457, 18316692, 17313525, 12611721, 21174504, 19544839
20294666, 18964939, 17600719, 26667015, 18191164, 17571306, 19393542
20777150, 18482502, 27086138, 19466309, 22243719, 17165204, 17040527
18098207, 24790914, 16785708, 19891090, 17465741, 16180763, 17174582
12982566, 16777840, 19463893, 22195465, 16875449, 22148226, 12816846
17237521, 6599380, 19358317, 17811438, 25505394, 17811447, 21983325
17945983, 18762750, 16912439, 17184721, 18061914, 20598042, 26631046
21380789, 17282229, 18948177, 18331850, 21142837, 18202441, 17082359
18723434, 21972320, 21532755, 19554106, 25505371, 20273319, 14034426
```

```
18339044, 19458377, 17752995, 20448824, 17891943, 17767676, 17258090
16668584, 18384391, 21063322, 17040764, 17381384, 15913355, 18356166
14084247, 20596234, 21641760, 20506715, 13853126, 21756661, 18610915
18203837, 14245531, 16043574, 21756699, 22195441, 17848897, 17877323
26667032, 21453153, 19272701, 20569094, 17468141, 17786518, 20861693
17912217, 17037130, 16956380, 18155762, 17478145, 17394950, 18641461
18189036, 17551674, 18619917, 17019356, 17027426, 21352646, 16268425
24476274, 22195492, 19584068, 26544823, 18436307, 22507210, 17265217
13498382, 17634921, 19469538, 21526048, 19258504, 23003979, 16354467
18043064, 19174430, 20004087, 17443671, 22195485, 18000422, 22321756
20004021, 17571039, 25897615, 27053456, 16832076, 21067387, 22905130
16344544, 21429602, 18009564, 14354737, 21286665, 18135678, 14521849
18614015, 20441797, 18362222, 25655390, 16472716, 17835048, 17050888
17936109, 14010183, 17325413, 18747196, 19207156, 17231779, 21842740
17761775, 16721594, 17082983, 20067212, 21179898, 17279227, 17302277
18084625, 20717359, 24624166, 15990359, 24842886, 26746894, 18203835
23026585, 17297939, 17811456, 16731148, 22380919, 21168487, 14133975
13829543, 17215560, 18740837, 17694209, 17385178, 18091059, 8322815
18259031, 28254374, 19689979, 25165496, 17586955, 17201159, 17655634
18331812, 17551699, 19730508, 17648596, 18868646, 16220077, 16069901
17393915, 17348614, 17957017, 17274537, 18096714, 17308789, 18436647
14285317, 19289642, 14764829, 17622427, 18328509, 23115139, 16943711
22195477, 22502493, 14368995, 17346671, 18996843, 17783588, 18604493
21343838, 16618694, 17672719, 18856999, 18783224, 17851160, 17546761
22168163, 17798953, 18273830, 22092979, 16596890, 19972566, 13871092
20828947, 26667023, 17726838, 16384983, 22296366, 17360606, 13645875
22321741, 25634317, 16542886, 18199537, 25879656, 21787056, 23140259
17889549, 21172913, 26245237, 14565184, 27825893, 20475845, 17071721
21281607, 17610798, 18308268, 20299015, 21343897, 22893153, 22594718
20657441, 17397545, 18230522, 16360112, 19769489, 12905058, 18641451
12747740, 18430495, 25423453, 17016369, 17042658, 14602788, 17551063
26243698, 19972568, 21517440, 23725036, 19788842, 18508861, 14657740
17332800, 13837378, 17186905, 19972564, 17019345, 19699191, 18315328
27441326, 17437634, 24570598, 22353199, 18093615, 19006849, 17392698
19013183, 17296856, 18674024, 26569225, 17232014, 16855292, 21051840
14692762, 17762296, 17705023, 23294548, 22351572, 22507234, 19121551
20324049, 21330264, 26198926, 19854503, 23315889, 26910644, 26030218
21868720, 19309466, 25764020, 18681862, 17365043, 17390160, 20031873
20558005, 18554763, 24717859, 21795111, 18456514, 13955826, 16306373
18139690, 17501491, 17752121, 17299889, 21668627, 23713236, 24652769
17889583, 18673325, 22551446, 18674465, 17242746, 19721304, 18293054
19211433, 19888853, 25914276, 24563422, 17951233, 18094246, 17649265
19615136, 17011832, 17477958, 16870214, 18522509, 20631274, 16091637
17323222, 16595641, 16524926, 17484731, 18228645, 18282562, 17596908
18272672, 18031668, 17156148, 16494615, 22683225, 20869721, 17545847
25093656, 18682983, 17655240, 24528741, 17614134, 25427662, 13558557
17341326, 22465352, 17891946, 17716305, 22657942, 27374796, 16392068
18440095, 19271443, 21351877, 20513399, 18092127, 17614227, 18440047
18849970, 16903536, 14106803, 20725343, 18973907, 18673342, 17389192
19032867, 25505382, 22809871, 17612828, 17006570, 16194160, 25369547
25505407, 16685417, 17721717, 21354456, 17390431, 17570240, 13960236
16863422, 28100487, 18325460, 17008068, 19727057, 16422541, 17267114
19972570, 18244962, 21538485, 18203838, 18765602, 16198143, 17246576
14829250, 28364007, 17835627, 20860659, 21629064, 18247991, 14458214
21051862, 17786278, 16692232, 17227277, 24348685, 24476265, 16042673
24975421, 22901797, 16314254, 19285025, 16228604, 16756406, 14176370
16837842, 20144308, 17393683, 23536835, 25823754, 18899974, 17787259
24719736, 20331945, 26078387, 19490948, 20074391, 15861775, 16399083
25555252, 25947799, 18018515, 22683212, 18260550, 21051858, 17080436
16613964, 17036973, 16579084, 24433711, 18384537, 27870645, 18280813
20296213, 16901385, 15979965, 17518652, 23330124, 20856766, 18441944
16450169, 9756271, 27534509, 22730454, 19718981, 17291347, 17892268
11733603, 16285691, 17587063, 21343775, 18180390, 26474853, 16538760
18193833, 21387964, 21051833, 17238511, 19777862, 17824637, 23065323
21656630, 17903598, 16571443, 18166013, 18306996, 19578350, 14852021
17853456, 18674047, 12364061, 24411921, 19207117, 22195448
```

Version 11.2.0.4.v17

La version 11.2.0.4.v17 comprend les éléments suivants :

- Correctif 27734982 : PSU Oracle Database 11.2.0.4.180717
- Correctif 27923163 : PSU Oracle JVM 11.2.0.4.180717
- Correctif 28125601 : DSTv32 pour RDBMS (TZDATA2018E)
- Correctif 27015468 : DSTv32 pour OJVM (TZDATA2018E)
- Correctif 27216420 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 27659043 : solution groupée MES 405
- Correctif 19692824 : DBCONTROL ne sort pas sur OEL 7

Correctif Oracle 27734982, publié en juillet 2018

Bogues corrigés :

```
17288409, 21051852, 24316947, 17811429, 17205719, 18607546, 25654936
17816865, 20506699, 24835538, 25957038, 23330119, 17922254, 17754782
13364795, 16934803, 17311728, 20387265, 17284817, 17441661, 20671094
24560906, 16992075, 17446237, 14015842, 19972569, 21756677, 17375354
21538558, 20925795, 17449815, 19463897, 26575788, 13866822, 17235750
17982555, 17478514, 18317531, 14338435, 18235390, 19461270, 20803583
13944971, 19475971, 20142975, 17811789, 16929165, 18704244, 24662775
20506706, 17546973, 21422580, 20334344, 14054676, 25489607, 17088068
17346091, 18264060, 17343514, 21538567, 19680952, 18471685, 19211724
21132297, 13951456, 16315398, 21847223, 18744139, 16850630, 23177648
19049453, 18090142, 18673304, 17883081, 19915271, 18641419, 18262334
25600421, 17006183, 16065166, 18277454, 16833527, 10136473, 18051556
17865671, 18554871, 17852463, 18774543, 17853498, 18334586, 19487147
20879889, 17551709, 17588480, 19827973, 17344412, 17842825, 18828868
20509482, 17025461, 13609098, 11883252, 17239687, 23007241, 17602269
19197175, 22195457, 18316692, 17313525, 12611721, 21174504, 19544839
20294666, 18964939, 17600719, 26667015, 18191164, 17571306, 19393542
20777150, 18482502, 27086138, 19466309, 22243719, 17165204, 17040527
18098207, 16785708, 17465741, 16180763, 17174582, 12982566, 16777840
19463893, 22195465, 16875449, 22148226, 12816846, 17237521, 6599380
19358317, 17811438, 25505394, 17811447, 21983325, 17945983, 18762750
16912439, 17184721, 18061914, 20598042, 21380789, 17282229, 18948177
18331850, 21142837, 18202441, 17082359, 18723434, 21972320, 21532755
19554106, 25505371, 14034426, 18339044, 19458377, 17752995, 20448824
17891943, 17767676, 17258090, 16668584, 18384391, 17040764, 17381384
15913355, 18356166, 14084247, 20596234, 21641760, 20506715, 13853126
21756661, 18203837, 14245531, 16043574, 21756699, 22195441, 17848897
17877323, 21453153, 19272701, 20569094, 17468141, 17786518, 20861693
17912217, 17037130, 16956380, 18155762, 17478145, 17394950, 18641461
18189036, 18619917, 17027426, 21352646, 16268425, 24476274, 22195492
19584068, 26544823, 18436307, 22507210, 17265217, 13498382, 17634921
19469538, 21526048, 19258504, 23003979, 18043064, 19174430, 20004087
17443671, 22195485, 18000422, 20004021, 22321756, 17571039, 27053456
25897615, 21067387, 16832076, 22905130, 16344544, 21429602, 18009564
14354737, 21286665, 18135678, 14521849, 18614015, 20441797, 18362222
25655390, 16472716, 17835048, 17050888, 17936109, 14010183, 17325413
18747196, 17761775, 16721594, 17082983, 20067212, 21179898, 17302277
18084625, 20717359, 24624166, 15990359, 24842886, 26746894, 18203835
23026585, 17297939, 17811456, 16731148, 22380919, 21168487, 14133975
13829543, 17215560, 17694209, 17385178, 18091059, 8322815, 18259031
19689979, 25165496, 17586955, 17201159, 17655634, 18331812, 19730508
```

```
17648596, 18868646, 16220077, 16069901, 17393915, 17348614, 17957017
17274537, 18096714, 17308789, 18436647, 14285317, 19289642, 14764829
17622427, 18328509, 16943711, 22195477, 22502493, 14368995, 17346671
18996843, 17783588, 18604493, 21343838, 16618694, 17672719, 18856999
18783224, 17851160, 17546761, 22168163, 17798953, 18273830, 22092979
16596890, 19972566, 20828947, 13871092, 26667023, 17726838, 16384983
22296366, 17360606, 13645875, 22321741, 16542886, 18199537, 25879656
21787056, 17889549, 21172913, 14565184, 27825893, 20475845, 17071721
21281607, 18308268, 17610798, 20299015, 21343897, 22893153, 20657441
17397545, 18230522, 16360112, 19769489, 12905058, 18641451, 12747740
18430495, 25423453, 17016369, 17042658, 14602788, 17551063, 19972568
21517440, 23725036, 19788842, 18508861, 14657740, 17332800, 13837378
17186905, 19972564, 19699191, 18315328, 27441326, 17437634, 24570598
22353199, 18093615, 19006849, 17392698, 19013183, 17296856, 18674024
26569225, 17232014, 16855292, 21051840, 14692762, 17762296, 17705023
23294548, 22351572, 22507234, 19121551, 20324049, 21330264, 26198926
19854503, 23315889, 26910644, 26030218, 21868720, 19309466, 25764020
18681862, 17365043, 17390160, 20031873, 20558005, 18554763, 24717859
21795111, 18456514, 16306373, 13955826, 18139690, 17501491, 17752121
17299889, 21668627, 23713236, 24652769, 17889583, 18673325, 22551446
17242746, 19721304, 18293054, 19211433, 19888853, 24563422, 17951233
18094246, 17649265, 19615136, 17011832, 17477958, 16870214, 18522509
20631274, 16091637, 17323222, 16595641, 16524926, 18228645, 18282562
17596908, 18031668, 17156148, 16494615, 22683225, 20869721, 17545847
25093656, 17655240, 24528741, 17614134, 25427662, 13558557, 17341326
22465352, 17891946, 17716305, 22657942, 27374796, 16392068, 18440095
19271443, 21351877, 20513399, 18092127, 17614227, 18440047, 18849970
16903536, 14106803, 18973907, 18673342, 17389192, 19032867, 25505382
22809871, 17612828, 17006570, 16194160, 25369547, 25505407, 16685417
17721717, 21354456, 17390431, 17570240, 16863422, 28100487, 18325460
17008068, 19727057, 16422541, 17267114, 19972570, 18244962, 21538485
18203838, 18765602, 16198143, 17246576, 14829250, 17835627, 20860659
21629064, 18247991, 14458214, 21051862, 17786278, 16692232, 24348685
17227277, 24476265, 16042673, 16314254, 19285025, 16228604, 16756406
16837842, 20144308, 17393683, 23536835, 25823754, 18899974, 17787259
24719736, 20331945, 19490948, 20074391, 15861775, 16399083, 25947799
18018515, 22683212, 18260550, 21051858, 17080436, 16613964, 17036973
16579084, 24433711, 18384537, 27870645, 18280813, 20296213, 16901385
15979965, 23330124, 18441944, 16450169, 27534509, 9756271, 17892268
11733603, 16285691, 17587063, 21343775, 18180390, 26474853, 16538760
18193833, 21387964, 21051833, 17238511, 19777862, 17824637, 23065323
17903598, 16571443, 18306996, 19578350, 14852021, 17853456, 18674047
12364061, 24411921, 19207117, 22195448
```

Version 11.2.0.4.v16

La version 11.2.0.4.v16 comprend les éléments suivants :

- Correctif 27338049 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS DATABASE 11.2.0.4.180417
- Correctif 27475598 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS OJVM 11.2.0.4.180417
- Correctif 27015449 : RDBMS - MISE À JOUR DSTV31 PROACTIVE - TZDATA2017C
- Correctif 27015468 : MISE À JOUR DSTV31 PROACTIVE - TZDATA2017C - CORRECTIF OJVM NÉCESSAIRE
- Correctif 27216420 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 27659043 : GROUPE MES 405 SUR RDBMS 11.2.0.4.180116 PSU
- Correctif 19692824 : DBCONTROL ne sort pas sur OEL 7
- Prise en charge du package `DBMS_ADVANCED_REWRITE`
- Correction d'un bogue dans lequel `DBA_LOCKS` et les vues associées disponibles dans les nouvelles instances de base de données de version 11.2.0.4.v15 n'étaient pas créés dans les mises à niveau

vers 11.2.0.4.v15. Les vues sont à présent créées dans les nouvelles instances de base de données et les instances de base de données mises à niveau de version 11.2.0.4.v16 et ultérieure.

Correctif Oracle 27338049, publié en avril 2018

Bogues corrigés :

```
21174504, 17184721, 21538558, 16091637, 18092127, 17381384, 15979965
20671094, 16731148, 16314254, 13837378, 18441944, 17835048, 13558557
17008068, 17201159, 25427662, 17853498, 20717359, 17246576, 18356166
18681862, 18440047, 20569094, 20031873, 16875449, 20387265, 19788842
17296856, 21330264, 14010183, 17648596, 17551063, 17025461, 24719736
17267114, 22507210, 17912217, 17889583, 18202441, 17040764, 17478145
16524926, 25655390, 19358317, 22148226, 18747196, 26544823, 18641419
17036973, 18948177, 17811789, 16542886, 14285317, 18009564, 16618694
8322815, 16832076, 18247991, 16692232, 22507234, 17570240, 13871092
24624166, 17848897, 17441661, 14034426, 17465741, 16596890, 17437634
21343897, 20506706, 21453153, 18339044, 22321741, 21795111, 17951233
18430495, 21787056, 22380919, 19469538, 20506715, 17811429, 19721304
17903598, 18230522, 19554106, 19458377, 21281607, 17612828, 6599380
22092979, 22321756, 17040527, 17811438, 18641461, 14657740, 13364795
21387964, 19490948, 22351572, 17346671, 17588480, 18235390, 26474853
18849970, 17889549, 19309466, 16472716, 20596234, 18331850, 18641451
17344412, 21179898, 19461270, 17546761, 24842886, 14521849, 18203835
18203838, 18964939, 18203837, 17313525, 22195457, 18139690, 16837842
22296366, 14106803, 17842825, 21352646, 22657942, 16360112, 20657441
22195441, 17389192, 26198926, 14565184, 17205719, 18440095, 14764829
22195448, 14354737, 13944971, 16571443, 21868720, 17186905, 17080436
18673342, 22905130, 17027426, 27374796, 19972569, 19972568, 20144308
19972566, 17282229, 19972564, 16870214, 21629064, 19615136, 21354456
17390431, 18762750, 23007241, 16613964, 17957017, 18098207, 18471685
19730508, 21538485, 18264060, 17323222, 17754782, 17600719, 18317531
17852463, 17596908, 17655634, 16228604, 27053456, 20074391, 19972570
18090142, 18996843, 19854503, 16042673, 17835627, 20334344, 17393683
20861693, 18000422, 17551709, 26575788, 23315889, 20506699, 19006849
18277454, 18456514, 19174430, 17258090, 17174582, 25654936, 17242746
16399083, 17824637, 21132297, 22465352, 17762296, 22168163, 17397545
16450169, 12364061, 20067212, 18856999, 19211724, 19463893, 19463897
21343775, 17853456, 18673304, 20004021, 26030218, 21668627, 16194160
17477958, 16538760, 12982566, 24570598, 20828947, 18259031, 20296213
18293054, 17610798, 19699191, 23065323, 17311728, 18135678, 18774543
23294548, 16785708, 10136473, 24560906, 22551446, 19777862, 17786518
18315328, 18334586, 12747740, 18096714, 19032867, 21641760, 18899974
17390160, 17232014, 20598042, 18673325, 16422541, 18155762, 14015842
19827973, 22683225, 17726838, 18554871, 23177648, 18051556, 20803583
21972320, 15990359, 17922254, 18282562, 16855292, 16668584, 21343838
20299015, 17446237, 18093615, 18043064, 23713236, 17694209, 17288409
20475845, 17274537, 13955826, 16934803, 17634921, 17501491, 16315398
22683212, 17006183, 13829543, 18191164, 17655240, 26746894, 22809871
18384391, 19393542, 21538567, 16198143, 21847223, 25823754, 17892268
20142975, 19584068, 17165204, 25165496, 18604493, 21756699, 18508861
16901385, 18554763, 21532755, 18189036, 17443671, 17385178, 14829250
17936109, 20925795, 20509482, 17478514, 27441326, 16850630, 13951456
16595641, 14054676, 15861775, 21142837, 16912439, 17299889, 17297939
23003979, 18619917, 16833527, 17798953, 17816865, 18607546, 17571306
21286665, 17341326, 26910644, 17851160, 20558005, 17586955, 19049453
21051840, 17587063, 16956380, 18328509, 25423453, 14133975, 18061914
18522509, 21051833, 18765602, 20860659, 20324049, 18199537, 17332800
13609098, 22502493, 18384537, 14338435, 17945983, 16392068, 21067387
17752995, 21051862, 16863422, 25505382, 17237521, 18244962, 19544839
24433711, 24717859, 17156148, 18973907, 23026585, 17877323, 17449815
18180390, 17088068, 17037130, 20004087, 21422580, 19466309, 11733603
25505371, 21051858, 18084625, 18674024, 21051852, 18091059, 25369547
```

```
16306373, 18306996, 18193833, 19915271, 17787259, 20513399, 20631274
25879656, 16344544, 14692762, 18614015, 17346091, 18228645, 17721717
18436307, 21756677, 19888853, 11883252, 17891943, 19475971, 22353199
16384983, 19121551, 12816846, 17982555, 17761775, 22243719, 17265217
25505394, 17071721, 16721594, 21756661, 18262334, 17891946, 15913355
17672719, 17602269, 17239687, 17042658, 17238511, 17811456, 17284817
17752121, 20879889, 21380789, 17394950, 17011832, 16579084, 22195465
14602788, 18325460, 24476265, 26569225, 24476274, 12611721, 16903536
17006570, 19689979, 16043574, 18783224, 24662775, 16494615, 21526048
17392698, 19197175, 16069901, 17811447, 17308789, 22195477, 24835538
17865671, 17343514, 19013183, 17325413, 18316692, 16180763, 17348614
14368995, 21983325, 17393915, 16285691, 19211433, 20331945, 17883081
17705023, 24316947, 17614227, 19578350, 22195485, 14084247, 13645875
16777840, 19727057, 14852021, 18744139, 18674047, 17716305, 19285025
18482502, 17622427, 19289642, 22195492, 25947799, 14458214, 20869721
21172913, 17767676, 18723434, 25505407, 17786278, 19258504, 17082983
21351877, 17365043, 13498382, 18331812, 16065166, 25489607, 16685417
18031668, 22893153, 16943711, 19272701, 21517440, 25897615, 17649265
13866822, 18094246, 24528741, 17783588, 14245531, 17082359, 18280813
20448824, 23330119, 16268425, 19487147, 25600421, 18018515, 17302277
17215560, 24411921, 19271443, 25764020, 17016369, 20777150, 23330124
16756406, 20441797, 19769489, 17545847, 25093656, 18260550, 13853126
17227277, 23536835, 25957038, 24652769, 19207117, 9756271, 18868646
17614134, 26667023, 17546973, 18704244, 19680952, 26667015, 17050888
18828868, 18273830, 17360606, 24563422, 16992075, 17375354, 12905058
18362222, 21429602, 27086138, 17571039, 17468141, 18436647, 17235750
21168487, 16220077, 16929165
```

Version 11.2.0.4.v15

La version 11.2.0.4.v15 inclut les éléments suivants :

- Correctif 26925576 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS DATABASE 11.2.0.4.180116
- Correctif 26925532 : MISE À JOUR D'ENSEMBLE DE CORRECTIFS OJVM 11.2.0.4.180116
- Correctif 27015449 : RDBMS - MISE À JOUR DSTV31 PROACTIVE - TZDATA2017C
- Correctif 27015468 : MISE À JOUR DSTV31 PROACTIVE - TZDATA2017C - CORRECTIF OJVM NÉCESSAIRE
- Correctif 27216420 : Oracle GoldenGate – Correctifs recommandés pour le serveur Oracle RDBMS
- Correctif 27244661 : GROUPE MES 405 SUR RDBMS 11.2.0.4.180116 PSU
- Correctif 19692824 : DBCONTROL ne sort pas sur OEL 7
- Prise en charge de `DBA_LOCKS` et des vues associées

Correctif Oracle 26925576, publié en janvier 2018

Bogues corrigés :

```
17288409, 21051852, 24316947, 17811429, 17205719, 18607546, 25654936
17816865, 20506699, 24835538, 25957038, 23330119, 17922254, 17754782
13364795, 16934803, 17311728, 20387265, 17284817, 17441661, 20671094
24560906, 16992075, 17446237, 14015842, 19972569, 21756677, 17375354
21538558, 20925795, 17449815, 26575788, 19463897, 13866822, 17235750
17982555, 17478514, 18317531, 14338435, 18235390, 20803583, 19461270
19475971, 13944971, 20142975, 17811789, 16929165, 18704244, 24662775
20506706, 21422580, 17546973, 20334344, 14054676, 25489607, 17088068
17346091, 18264060, 17343514, 21538567, 19680952, 18471685, 19211724
21132297, 13951456, 16315398, 21847223, 18744139, 16850630, 23177648
19049453, 18090142, 18673304, 17883081, 19915271, 18641419, 18262334
```

```
25600421, 17006183, 16065166, 18277454, 16833527, 10136473, 18051556
17865671, 18554871, 17852463, 17853498, 18334586, 20879889, 17551709
17588480, 19827973, 17344412, 17842825, 18828868, 20509482, 17025461
13609098, 11883252, 17239687, 23007241, 17602269, 19197175, 18316692
22195457, 17313525, 12611721, 21174504, 19544839, 18964939, 17600719
26667015, 18191164, 17571306, 19393542, 20777150, 18482502, 19466309
22243719, 17165204, 17040527, 18098207, 16785708, 17465741, 16180763
17174582, 12982566, 16777840, 19463893, 22195465, 16875449, 22148226
12816846, 17237521, 6599380, 19358317, 17811438, 25505394, 17811447
21983325, 17945983, 18762750, 16912439, 17184721, 20598042, 18061914
21380789, 17282229, 18948177, 18331850, 21142837, 18202441, 17082359
18723434, 21972320, 21532755, 19554106, 25505371, 14034426, 18339044
19458377, 17752995, 20448824, 17891943, 17767676, 17258090, 16668584
18384391, 17040764, 17381384, 15913355, 18356166, 14084247, 20596234
21641760, 20506715, 13853126, 21756661, 18203837, 14245531, 16043574
21756699, 22195441, 17848897, 17877323, 21453153, 19272701, 20569094
17468141, 17786518, 20861693, 17912217, 17037130, 16956380, 18155762
17478145, 17394950, 18641461, 18189036, 18619917, 17027426, 21352646
16268425, 24476274, 22195492, 19584068, 26544823, 18436307, 22507210
17265217, 13498382, 17634921, 19469538, 21526048, 19258504, 23003979
19174430, 18043064, 20004087, 17443671, 22195485, 18000422, 20004021
22321756, 17571039, 25897615, 27053456, 21067387, 16832076, 22905130
16344544, 21429602, 18009564, 14354737, 21286665, 18135678, 14521849
18614015, 20441797, 18362222, 25655390, 16472716, 17835048, 17050888
17936109, 14010183, 17325413, 18747196, 17761775, 16721594, 17082983
20067212, 21179898, 17302277, 18084625, 20717359, 24624166, 15990359
26746894, 24842886, 18203835, 23026585, 17297939, 17811456, 16731148
22380919, 21168487, 14133975, 13829543, 17215560, 17694209, 17385178
18091059, 8322815, 18259031, 25165496, 19689979, 17586955, 17201159
17655634, 18331812, 19730508, 18868646, 17648596, 16220077, 16069901
17393915, 17348614, 17957017, 17274537, 18096714, 17308789, 18436647
14285317, 19289642, 14764829, 17622427, 18328509, 16943711, 22195477
22502493, 14368995, 17346671, 18996843, 17783588, 21343838, 16618694
17672719, 18856999, 18783224, 17851160, 17546761, 22168163, 17798953
18273830, 22092979, 16596890, 19972566, 20828947, 13871092, 26667023
17726838, 16384983, 22296366, 17360606, 13645875, 22321741, 16542886
25879656, 18199537, 21787056, 17889549, 21172913, 14565184, 20475845
17071721, 21281607, 17610798, 20299015, 21343897, 22893153, 20657441
17397545, 18230522, 16360112, 19769489, 12905058, 18641451, 12747740
18430495, 25423453, 17016369, 17042658, 14602788, 17551063, 19972568
21517440, 19788842, 18508861, 14657740, 17332800, 13837378, 17186905
19972564, 19699191, 18315328, 17437634, 24570598, 22353199, 18093615
19006849, 19013183, 17296856, 18674024, 26569225, 17232014, 16855292
21051840, 14692762, 17762296, 17705023, 23294548, 22507234, 19121551
20324049, 21330264, 26198926, 19854503, 23315889, 26910644, 26030218
21868720, 19309466, 25764020, 18681862, 17365043, 20031873, 20558005
18554763, 17390160, 24717859, 21795111, 18456514, 16306373, 13955826
18139690, 17501491, 17752121, 21668627, 17299889, 23713236, 24652769
17889583, 18673325, 22551446, 19721304, 18293054, 17242746, 19211433
19888853, 17951233, 18094246, 17649265, 19615136, 17011832, 17477958
16870214, 18522509, 20631274, 16091637, 17323222, 16595641, 16524926
18228645, 18282562, 17596908, 18031668, 17156148, 16494615, 22683225
20869721, 17545847, 25093656, 17655240, 24528741, 17614134, 25427662
13558557, 22465352, 17341326, 17891946, 17716305, 22657942, 16392068
18440095, 19271443, 21351877, 20513399, 18092127, 17614227, 18440047
18849970, 16903536, 14106803, 18973907, 18673342, 22809871, 17389192
19032867, 25505382, 17612828, 17006570, 16194160, 25369547, 16685417
25505407, 17721717, 21354456, 17390431, 17570240, 16863422, 18325460
17008068, 19727057, 16422541, 19972570, 17267114, 18244962, 21538485
18203838, 18765602, 16198143, 17246576, 14829250, 17835627, 20860659
21629064, 18247991, 14458214, 21051862, 17786278, 16692232, 17227277
24476265, 16042673, 16314254, 19285025, 16228604, 16756406, 16837842
20144308, 17393683, 23536835, 25823754, 18899974, 17787259, 24719736
20331945, 19490948, 20074391, 15861775, 16399083, 25947799, 18018515
22683212, 21051858, 18260550, 17080436, 16613964, 17036973, 16579084
24433711, 18384537, 18280813, 20296213, 16901385, 15979965, 23330124
```

```
                    18441944, 16450169, 9756271, 17892268, 11733603, 16285691, 17587063
                    21343775, 18180390, 26474853, 16538760, 18193833, 21387964, 21051833
                    17238511, 19777862, 23065323, 17824637, 16571443, 17903598, 18306996
                    19578350, 14852021, 17853456, 18674047, 12364061, 19207117, 24411921,
22195448
```

Version 11.2.0.4.v14

La version 11.2.0.4.v14 comprend les éléments suivants :

- PSU Oracle d'octobre 2017, une combinaison de PSU de base de données (correctif 26392168) + PSU de composant OJVM (correctif 26635834)
- Oracle a recommandé les correctifs SGBDR pour Oracle GoldenGate (correctif 26950781)
- RSA Micro-Edition Suite Bundle (correctif 26963526)
- Fichier de fuseau horaire DSTv30 (correctif 25881255, correctif OJVM 25881271)

Correctif Oracle 26392168, publié en octobre 2017

Bogues corrigés :

```
    17288409, 21051852, 24316947, 17811429, 17205719, 18607546, 25654936
    20506699, 17816865, 25957038, 23330119, 17922254, 17754782, 13364795
    16934803, 17311728, 20387265, 17284817, 17441661, 24560906, 16992075
    17446237, 14015842, 19972569, 21756677, 17375354, 21538558, 20925795
    17449815, 26575788, 19463897, 13866822, 17235750, 17982555, 17478514
    18317531, 14338435, 18235390, 20803583, 19461270, 13944971, 20142975
    17811789, 16929165, 18704244, 24662775, 20506706, 17546973, 20334344
    25489607, 14054676, 17088068, 17346091, 18264060, 17343514, 21538567
    19680952, 18471685, 19211724, 21132297, 13951456, 21847223, 16315398
    18744139, 16850630, 23177648, 19049453, 18673304, 17883081, 19915271
    18641419, 18262334, 25600421, 17006183, 16065166, 18277454, 16833527
    10136473, 18051556, 17865671, 17852463, 18554871, 17853498, 18334586
    20879889, 17551709, 17588480, 19827973, 17344412, 17842825, 18828868
    20509482, 17025461, 11883252, 13609098, 17239687, 17602269, 19197175
    18316692, 22195457, 17313525, 12611721, 19544839, 18964939, 26667015
    17600719, 18191164, 19393542, 17571306, 20777150, 18482502, 19466309
    22243719, 17040527, 17165204, 18098207, 16785708, 17465741, 16180763
    17174582, 12982566, 16777840, 19463893, 22195465, 16875449, 22148226
    12816846, 17237521, 6599380, 19358317, 17811438, 25505394, 17811447
    17945983, 21983325, 18762750, 16912439, 17184721, 18061914, 17282229
    18331850, 18202441, 17082359, 18723434, 21532755, 21972320, 19554106
    25505371, 14034426, 18339044, 19458377, 17752995, 20448824, 17891943
    17258090, 17767676, 16668584, 18384391, 17040764, 17381384, 15913355
    18356166, 14084247, 20596234, 20506715, 21756661, 13853126, 18203837
    14245531, 16043574, 21756699, 22195441, 17848897, 17877323, 19272701
    21453153, 20569094, 17468141, 20861693, 17786518, 17912217, 17037130
    16956380, 18155762, 17478145, 17394950, 18641461, 18189036, 18619917
    17027426, 21352646, 16268425, 24476274, 22195492, 19584068, 26544823
    18436307, 22507210, 17265217, 17634921, 13498382, 19469538, 21526048
    19258504, 18043064, 20004087, 17443671, 22195485, 18000422, 20004021
    22321756, 17571039, 21067387, 16832076, 22905130, 16344544, 21429602
    18009564, 14354737, 21286665, 18135678, 14521849, 18614015, 20441797
    18362222, 25655390, 16472716, 17835048, 17050888, 17936109, 14010183
    17325413, 18747196, 17761775, 16721594, 17082983, 20067212, 21179898
    17302277, 18084625, 24624166, 15990359, 26746894, 24842886, 23026585
    18203835, 17297939, 17811456, 16731148, 22380919, 21168487, 14133975
    13829543, 17215560, 17694209, 17385178, 18091059, 8322815, 18259031
    19689979, 17586955, 17201159, 17655634, 18331812, 19730508, 18868646
    17648596, 16220077, 16069901, 17348614, 17393915, 17957017, 17274537
```

```
18096714, 17308789, 18436647, 14285317, 19289642, 14764829, 17622427
18328509, 16943711, 22195477, 14368995, 22502493, 17346671, 18996843
17783588, 21343838, 16618694, 17672719, 18856999, 18783224, 17851160
17546761, 22168163, 17798953, 18273830, 22092979, 16596890, 19972566
20828947, 13871092, 26667023, 17726838, 16384983, 22296366, 17360606
22321741, 13645875, 25879656, 18199537, 16542886, 21787056, 17889549
14565184, 20475845, 21281607, 17071721, 17610798, 20299015, 21343897
22893153, 20657441, 17397545, 18230522, 16360112, 19769489, 12905058
18641451, 12747740, 18430495, 25423453, 17016369, 17042658, 14602788
17551063, 19972568, 21517440, 19788842, 18508861, 14657740, 17332800
13837378, 17186905, 19972564, 19699191, 18315328, 17437634, 22353199
18093615, 19006849, 19013183, 17296856, 18674024, 17232014, 16855292
17762296, 14692762, 21051840, 17705023, 23294548, 22507234, 19121551
21330264, 26198926, 19854503, 23315889, 26030218, 21868720, 19309466
18681862, 17365043, 20558005, 18554763, 17390160, 18456514, 16306373
13955826, 18139690, 17501491, 17752121, 21668627, 17299889, 23713236
24652769, 17889583, 18673325, 22551446, 19721304, 18293054, 17242746
19211433, 19888853, 17951233, 18094246, 17649265, 19615136, 17011832
16870214, 17477958, 18522509, 20631274, 16091637, 17323222, 16595641
16524926, 18228645, 18282562, 17596908, 18031668, 17156148, 16494615
22683225, 20869721, 17545847, 25093656, 17655240, 24528741, 17614134
25427662, 13558557, 17341326, 17891946, 17716305, 22657942, 18440095
16392068, 19271443, 21351877, 18092127, 17614227, 18440047, 18849970
16903536, 14106803, 18973907, 18673342, 17389192, 25505382, 19032867
17612828, 16194160, 17006570, 25369547, 25505407, 16685417, 17721717
17390431, 17570240, 16863422, 18325460, 17008068, 19727057, 16422541
19972570, 17267114, 18244962, 21538485, 18203838, 18765602, 16198143
17246576, 14829250, 17835627, 18247991, 14458214, 21051862, 17786278
16692232, 17227277, 24476265, 16042673, 16314254, 19285025, 16228604
16837842, 20144308, 17393683, 23536835, 25823754, 18899974, 17787259
24719736, 20331945, 19490948, 20074391, 15861775, 16399083, 25947799
18018515, 22683212, 21051858, 18260550, 17080436, 16613964, 17036973
16579084, 24433711, 18384537, 18280813, 20296213, 16901385, 15979965
23330124, 18441944, 16450169, 9756271, 17892268, 11733603, 16285691
17587063, 21343775, 26474853, 18180390, 16538760, 18193833, 21387964
21051833, 17238511, 19777862, 23065323, 17824637, 17903598, 16571443
18306996, 19578350, 14852021, 17853456, 18674047, 12364061, 24411921
19207117, 22195448
```

Version 11.2.0.4.v13

La version 11.2.0.4.v13 comprend les éléments suivants :

- PSU Oracle de juillet 2017, une combinaison de PSU de base de données (correctif 26609445) + PSU du composant OJVM (correctif 26027154)
- Oracle a recommandé les correctifs SGBDR pour Oracle GoldenGate (correctif 26554712)
- RSA Micro-Edition Suite Bundle (correctif 26770426)
- Fichier de fuseau horaire DSTv30 (correctif 25881255, correctif OJVM 25881271)
- Prise en charge de Validation des fichiers d'instance de base de données (p. 1140) avec l'utilitaire de validation logique `RMAN`.
- Prise en charge de Définition de l'édition par défaut d'une instance de base de données (p. 1123)

Correctif Oracle 26609445, publié en juillet 2017

Bogues corrigés :

```
17288409, 21051852, 24316947, 17811429, 17205719, 18607546, 20506699
```

```
17816865, 25957038, 23330119, 17922254, 17754782, 13364795, 16934803
17311728, 20387265, 17284817, 17441661, 24560906, 16992075, 17446237
14015842, 19972569, 21756677, 17375354, 21538558, 20925795, 17449815
26575788, 19463897, 13866822, 17235750, 17982555, 17478514, 18317531
14338435, 18235390, 20803583, 19461270, 13944971, 20142975, 17811789
16929165, 18704244, 20506706, 17546973, 20334344, 14054676, 17088068
17346091, 18264060, 17343514, 21538567, 19680952, 18471685, 19211724
13951456, 21847223, 16315398, 18744139, 16850630, 23177648, 19049453
18673304, 17883081, 19915271, 18641419, 18262334, 25600421, 17006183
16065166, 18277454, 16833527, 10136473, 18051556, 17865671, 17852463
18554871, 17853498, 18334586, 20879889, 17551709, 17588480, 19827973
17344412, 17842825, 18828868, 20509482, 17025461, 11883252, 13609098
17239687, 17602269, 19197175, 18316692, 22195457, 17313525, 12611721
19544839, 18964939, 17600719, 18191164, 19393542, 17571306, 20777150
18482502, 19466309, 22243719, 17040527, 17165204, 18098207, 16785708
17465741, 16180763, 17174582, 12982566, 16777840, 19463893, 22195465
16875449, 22148226, 12816846, 17237521, 6599380, 19358317, 17811438
25505394, 17811447, 17945983, 21983325, 18762750, 16912439, 17184721
18061914, 17282229, 18331850, 18202441, 17082359, 18723434, 21972320
19554106, 25505371, 14034426, 18339044, 19458377, 17752995, 20448824
17891943, 17258090, 17767676, 16668584, 18384391, 17040764, 17381384
15913355, 18356166, 14084247, 20596234, 20506715, 21756661, 13853126
18203837, 14245531, 16043574, 21756699, 22195441, 17848897, 17877323
21453153, 17468141, 20861693, 17786518, 17912217, 17037130, 16956380
18155762, 17478145, 17394950, 18641461, 18189036, 18619917, 17027426
21352646, 16268425, 24476274, 22195492, 19584068, 26544823, 18436307
22507210, 17265217, 17634921, 13498382, 19469538, 21526048, 19258504
18043064, 20004087, 17443671, 22195485, 18000422, 20004021, 22321756
17571039, 21067387, 16832076, 22905130, 16344544, 18009564, 14354737
21286665, 18135678, 14521849, 18614015, 20441797, 18362222, 25655390
16472716, 17835048, 17050888, 17936109, 14010183, 17325413, 18747196
17761775, 16721594, 17082983, 20067212, 21179898, 17302277, 18084625
15990359, 24842886, 18203835, 17297939, 17811456, 16731148, 22380919
21168487, 14133975, 13829543, 17215560, 17694209, 17385178, 18091059
8322815, 18259031, 19689979, 17586955, 17201159, 17655634, 18331812
19730508, 18868646, 17648596, 16220077, 16069901, 17348614, 17393915
17957017, 17274537, 18096714, 17308789, 18436647, 14285317, 19289642
14764829, 17622427, 18328509, 16943711, 22195477, 14368995, 22502493
17346671, 18996843, 17783588, 21343838, 16618694, 17672719, 18856999
18783224, 17851160, 17546761, 22168163, 17798953, 18273830, 22092979
16596890, 19972566, 13871092, 17726838, 16384983, 22296366, 17360606
22321741, 13645875, 25879656, 18199537, 16542886, 21787056, 17889549
14565184, 17071721, 17610798, 20299015, 21343897, 22893153, 20657441
17397545, 18230522, 16360112, 19769489, 12905058, 18641451, 12747740
18430495, 25423453, 17016369, 17042658, 14602788, 17551063, 19972568
21517440, 19788842, 18508861, 14657740, 17332800, 13837378, 17186905
19972564, 19699191, 18315328, 17437634, 22353199, 18093615, 19006849
19013183, 17296856, 18674024, 17232014, 16855292, 17762296, 14692762
21051840, 17705023, 22507234, 19121551, 21330264, 19854503, 26030218
21868720, 19309466, 18681862, 17365043, 20558005, 18554763, 17390160
18456514, 16306373, 13955826, 18139690, 17501491, 17752121, 21668627
17299889, 17889583, 18673325, 19721304, 18293054, 17242746, 19888853
17951233, 18094246, 17649265, 19615136, 17011832, 16870214, 17477958
18522509, 20631274, 16091637, 17323222, 16595641, 16524926, 18228645
18282562, 17596908, 18031668, 17156148, 16494615, 22683225, 17545847
25093656, 17655240, 24528741, 17614134, 25427662, 13558557, 17341326
17891946, 17716305, 22657942, 18440095, 16392068, 19271443, 21351877
18092127, 17614227, 18440047, 16903536, 14106803, 18973907, 18673342
17389192, 25505382, 19032867, 17612828, 16194160, 17006570, 25369547
25505407, 16685417, 17721717, 17390431, 17570240, 16863422, 18325460
19727057, 16422541, 19972570, 17267114, 18244962, 21538485, 18203838
18765602, 16198143, 17246576, 14829250, 17835627, 18247991, 14458214
21051862, 16692232, 17786278, 17227277, 24476265, 16042673, 16314254
16228604, 16837842, 17393683, 23536835, 25823754, 18899974, 17787259
20331945, 20074391, 15861775, 16399083, 18018515, 22683212, 21051858
18260550, 17080436, 16613964, 17036973, 16579084, 24433711, 18384537
```

```
18280813, 20296213, 16901385, 15979965, 23330124, 18441944, 16450169
9756271, 17892268, 11733603, 16285691, 17587063, 21343775, 18180390
16538760, 18193833, 21387964, 21051833, 17238511, 19777862, 17824637
16571443, 18306996, 19578350, 14852021, 17853456, 18674047, 12364061
24411921, 19207117, 22195448
```

Version 11.2.0.4.v12

La version 11.2.0.4.v12 comprend les éléments suivants :

- Correctif Oracle 25440428, une combinaison de PSU de base de données (correctif 24732075) + PSU de composant OJVM (correctif 25434033)
- Oracle a recommandé les correctifs SGBDR pour Oracle GoldenGate (correctif 25734992)
- Groupe MES (correctif 24975421 pour 11.2.0.4)
- Fichier de fuseau horaire DSTv28 (correctif 24701840)
- Prise en charge du package `DBMS_CHANGE_NOTIFICATION`
- Prise en charge des packages et vues `XSTREAM` (peut nécessiter des licences supplémentaires)

Correctif Oracle 24732075, publié en avril 2017

Bogues corrigés :

```
17288409, 21051852, 24316947, 17811429, 17205719, 18607546, 20506699
17816865, 17922254, 23330119, 17754782, 16934803, 13364795, 17311728
17284817, 17441661, 24560906, 16992075, 17446237, 14015842, 19972569
21756677, 17375354, 20925795, 21538558, 17449815, 19463897, 13866822
17235750, 17982555, 17478514, 18317531, 14338435, 18235390, 20803583
13944971, 20142975, 17811789, 16929165, 18704244, 20506706, 17546973
20334344, 14054676, 17088068, 17346091, 18264060, 17343514, 21538567
19680952, 18471685, 19211724, 13951456, 21847223, 16315398, 18744139
16850630, 23177648, 19049453, 18673304, 17883081, 19915271, 18641419
18262334, 17006183, 16065166, 18277454, 16833527, 10136473, 18051556
17865671, 17852463, 18554871, 17853498, 18334586, 17551709, 17588480
19827973, 17344412, 17842825, 18828868, 17025461, 11883252, 13609098
17239687, 17602269, 19197175, 18316692, 22195457, 17313525, 12611721
19544839, 18964939, 17600719, 18191164, 19393542, 17571306, 20777150
18482502, 19466309, 22243719, 17040527, 17165204, 18098207, 16785708
17465741, 17174582, 16180763, 12982566, 16777840, 19463893, 22195465
16875449, 12816846, 22148226, 17237521, 6599380, 19358317, 25505394
17811438, 17811447, 17945983, 21983325, 18762750, 16912439, 17184721
18061914, 17282229, 18331850, 18202441, 17082359, 18723434, 21972320
19554106, 25505371, 14034426, 18339044, 19458377, 17752995, 20448824
17891943, 17258090, 17767676, 16668584, 18384391, 17040764, 17381384
15913355, 18356166, 14084247, 20596234, 20506715, 21756661, 13853126
18203837, 14245531, 16043574, 21756699, 22195441, 17848897, 17877323
21453153, 17468141, 20861693, 17786518, 17912217, 17037130, 16956380
18155762, 17478145, 17394950, 18641461, 18189036, 18619917, 17027426
21352646, 16268425, 24476274, 22195492, 19584068, 18436307, 22507210
17265217, 17634921, 13498382, 21526048, 19258504, 20004087, 17443671
22195485, 18000422, 22321756, 20004021, 17571039, 21067387, 22905130
16344544, 18009564, 14354737, 21286665, 18135678, 18614015, 20441797
18362222, 17835048, 16472716, 17936109, 17050888, 14010183, 17325413
18747196, 17761775, 16721594, 17082983, 20067212, 21179898, 17302277
18084625, 15990359, 24842886, 18203835, 17297939, 17811456, 22380919
16731148, 21168487, 14133975, 13829543, 17215560, 17694209, 17385178
18091059, 8322815, 17586955, 17201159, 17655634, 18331812, 19730508
18868646, 17648596, 16220077, 16069901, 17348614, 17393915, 17274537
17957017, 18096714, 17308789, 18436647, 14285317, 19289642, 14764829
```

```
17622427, 18328509, 16943711, 22195477, 14368995, 22502493, 17346671
18996843, 17783588, 21343838, 16618694, 17672719, 18856999, 18783224
17851160, 17546761, 17798953, 18273830, 22092979, 16596890, 19972566
16384983, 17726838, 22296366, 17360606, 22321741, 13645875, 18199537
16542886, 21787056, 17889549, 14565184, 17071721, 17610798, 20299015
21343897, 22893153, 20657441, 17397545, 18230522, 16360112, 19769489
12905058, 18641451, 12747740, 18430495, 17016369, 17042658, 14602788
17551063, 19972568, 21517440, 18508861, 19788842, 14657740, 17332800
13837378, 19972564, 17186905, 18315328, 19699191, 17437634, 22353199
18093615, 19006849, 19013183, 17296856, 18674024, 17232014, 16855292
17762296, 14692762, 21051840, 17705023, 22507234, 19121551, 21330264
19854503, 21868720, 19309466, 18681862, 20558005, 18554763, 17390160
18456514, 16306373, 13955826, 18139690, 17501491, 17752121, 21668627
17299889, 17889583, 18673325, 19721304, 18293054, 17242746, 17951233
18094246, 17649265, 19615136, 17011832, 16870214, 17477958, 18522509
20631274, 16091637, 17323222, 16595641, 16524926, 18228645, 18282562
17596908, 18031668, 17156148, 16494615, 22683225, 17545847, 25093656
17655240, 24528741, 17614134, 13558557, 17341326, 17891946, 17716305
22657942, 18440095, 16392068, 19271443, 21351877, 18092127, 17614227
18440047, 16903536, 14106803, 18973907, 18673342, 25505382, 19032867
17389192, 17612828, 16194160, 17006570, 25369547, 25505407, 17721717
17390431, 17570240, 16863422, 18325460, 19727057, 16422541, 19972570
17267114, 18244962, 21538485, 18765602, 18203838, 16198143, 17246576
14829250, 17835627, 18247991, 14458214, 21051862, 16692232, 17786278
17227277, 24476265, 16042673, 16314254, 16228604, 16837842, 17393683
23536835, 17787259, 20331945, 20074391, 15861775, 16399083, 18018515
22683212, 18260550, 21051858, 17080436, 16613964, 17036973, 16579084
24433711, 18384537, 18280813, 20296213, 16901385, 15979965, 23330124
18441944, 16450169, 9756271, 17892268, 11733603, 16285691, 17587063
21343775, 18180390, 16538760, 18193833, 21387964, 21051833, 17238511
17824637, 16571443, 18306996, 14852021, 17853456, 18674047, 12364061
24411921, 22195448
```

Version 11.2.0.4.v11

La version 11.2.0.4.v11 comprend les éléments suivants :

- Correctif Oracle 24918033, une combinaison de PSU de base de données (correctif 24006111) + PSU de composant OJVM (correctif 24917954)
- Oracle a recommandé les correctifs SGBDR pour Oracle GoldenGate (correctif 24491261)
- Groupe MES (correctif 24975421 pour 11.2.0.4)

Correctif Oracle 24918033, publié en janvier 2017

Bogues corrigés :

```
18933818, 19176885, 17201047, 25067795, 14774730, 19153980, 21911849
23727132, 18166577, 24448240, 17056813, 21811517, 19909862, 22675136
24534298, 19895326, 22253904, 17804361, 19231857, 17528315, 19058059
19554117, 19007266, 17285560, 22670385, 18458318, 19187988, 23265914
19006757, 19374518, 19223010, 25076732, 22118835, 19852360, 20408829
21047766, 21566944,
17288409, 21051852, 24316947, 17811429, 18607546, 17205719, 20506699
17816865, 17922254, 23330119, 17754782, 16934803, 13364795, 17311728
17441661, 17284817, 16992075, 17446237, 14015842, 19972569, 21756677
17375354, 20925795, 21538558, 17449815, 19463897, 13866822, 17235750
17982555, 17478514, 18317531, 14338435, 18235390, 20803583, 13944971
20142975, 17811789, 16929165, 18704244, 20506706, 17546973, 20334344
14054676, 17088068, 17346091, 18264060, 17343514, 21538567, 19680952
```

```
18471685, 19211724, 13951456, 21847223, 16315398, 18744139, 16850630
23177648, 19049453, 18673304, 17883081, 19915271, 18641419, 18262334
17006183, 16065166, 18277454, 16833527, 10136473, 18051556, 17865671
17852463, 18554871, 17853498, 18334586, 17551709, 17588480, 19827973
17344412, 17842825, 18828868, 17025461, 11883252, 13609098, 17239687
17602269, 19197175, 22195457, 18316692, 17313525, 12611721, 19544839
18964939, 17600719, 18191164, 19393542, 17571306, 20777150, 18482502
19466309, 22243719, 17040527, 17165204, 18098207, 16785708, 17465741
17174582, 16180763, 16777840, 12982566, 19463893, 22195465, 22148226
16875449, 12816846, 17237521, 6599380, 19358317, 17811438, 17811447
17945983, 21983325, 18762750, 16912439, 17184721, 18061914, 17282229
18331850, 18202441, 17082359, 18723434, 21972320, 19554106, 14034426
18339044, 19458377, 17752995, 20448824, 17891943, 17258090, 17767676
16668584, 18384391, 17040764, 17381384, 15913355, 18356166, 14084247
20596234, 20506715, 21756661, 13853126, 18203837, 14245531, 16043574
21756699, 22195441, 17848897, 17877323, 21453153, 17468141, 20861693
17786518, 17912217, 17037130, 16956380, 18155762, 17478145, 17394950
18641461, 18189036, 18619917, 17027426, 21352646, 16268425, 24476274
22195492, 19584068, 18436307, 22507210, 17265217, 17634921, 13498382
21526048, 19258504, 20004087, 17443671, 22195485, 18000422, 22321756
20004021, 17571039, 21067387, 16344544, 18009564, 14354737, 21286665
18135678, 18614015, 20441797, 18362222, 17835048, 16472716, 17936109
17050888, 17325413, 14010183, 18747196, 17761775, 16721594, 17082983
20067212, 21179898, 17302277, 18084625, 15990359, 18203835, 17297939
17811456, 22380919, 16731148, 21168487, 14133975, 13829543, 17215560
17694209, 17385178, 18091059, 8322815, 17586955, 17201159, 17655634
18331812, 19730508, 18868646, 17648596, 16220077, 16069901, 17348614
17393915, 17274537, 17957017, 18096714, 17308789, 18436647, 14285317
19289642, 14764829, 18328509, 17622427, 16943711, 22195477, 14368995
22502493, 17346671, 18996843, 17783588, 21343838, 16618694, 17672719
18856999, 18783224, 17851160, 17546761, 17798953, 18273830, 22092979
16596890, 19972566, 16384983, 17726838, 22296366, 17360606, 22321741
13645875, 18199537, 16542886, 21787056, 17889549, 14565184, 17071721
17610798, 20299015, 21343897, 22893153, 20657441, 17397545, 18230522
16360112, 19769489, 12905058, 18641451, 12747740, 18430495, 17016369
17042658, 14602788, 17551063, 19972568, 21517440, 18508861, 19788842
14657740, 17332800, 13837378, 19972564, 17186905, 18315328, 19699191
17437634, 22353199, 18093615, 19006849, 19013183, 17296856, 18674024
17232014, 16855292, 17762296, 14692762, 21051840, 17705023, 22507234
19121551, 21330264, 19854503, 21868720, 19309466, 18681862, 20558005
18554763, 17390160, 18456514, 16306373, 13955826, 18139690, 17501491
17752121, 21668627, 17299889, 17889583, 18673325, 19721304, 18293054
17242746, 17951233, 18094246, 17649265, 19615136, 17011832, 16870214
17477958, 18522509, 20631274, 16091637, 17323222, 16595641, 16524926
18228645, 18282562, 17596908, 18031668, 17156148, 16494615, 22683225
17545847, 17655240, 24528741, 17614134, 13558557, 17341326, 17891946
17716305, 22657942, 16392068, 19271443, 21351877, 18092127, 17614227
18440047, 16903536, 14106803, 18973907, 18673342, 19032867, 17389192
17612828, 16194160, 17006570, 17721717, 17390431, 17570240, 16863422
18325460, 19727057, 16422541, 19972570, 17267114, 18244962, 21538485
18765602, 18203838, 16198143, 17246576, 14829250, 17835627, 18247991
14458214, 21051862, 16692232, 17786278, 17227277, 24476265, 16042673
16314254, 16228604, 16837842, 17393683, 23536835, 17787259, 20331945
20074391, 15861775, 16399083, 18018515, 22683212, 18260550, 21051858
17080436, 16613964, 17036973, 16579084, 24433711, 18384537, 18280813
20296213, 16901385, 15979965, 23330124, 18441944, 16450169, 9756271
17892268, 11733603, 16285691, 17587063, 21343775, 18180390, 16538760
18193833, 21387964, 21051833, 17238511, 17824637, 16571443, 18306996
14852021, 17853456, 18674047, 12364061, 22195448
```

Version 11.2.0.4.v10

La version 11.2.0.4.v10 comprend les éléments suivants :

- Correctif Oracle 24436313, une combinaison de PSU de base de données (correctif 24006111) + PSU de composant OJVM (correctif 24315821)
- Oracle a recommandé les correctifs SGBDR pour Oracle GoldenGate (correctif 24491261)
- Groupe MES (correctif 24975421 pour 11.2.0.4)

Référence : mise à jour d'ensemble de correctifs Oracle Database 11.2.0.4.161018 (correctif 24006111, publié en octobre 2016)

Bogues corrigés :

```
17288409, 21051852, 24316947, 17811429, 18607546, 17205719, 20506699
17816865, 17922254, 23330119, 17754782, 16934803, 13364795, 17311728
17441661, 17284817, 16992075, 17446237, 14015842, 19972569, 21756677
17375354, 20925795, 21538558, 17449815, 19463897, 13866822, 17235750
17982555, 17478514, 18317531, 14338435, 18235390, 20803583, 13944971
20142975, 17811789, 16929165, 18704244, 20506706, 17546973, 20334344
14054676, 17088068, 17346091, 18264060, 17343514, 21538567, 19680952
18471685, 19211724, 13951456, 21847223, 16315398, 18744139, 16850630
23177648, 19049453, 18673304, 17883081, 19915271, 18641419, 18262334
17006183, 16065166, 18277454, 16833527, 10136473, 18051556, 17865671
17852463, 18554871, 17853498, 18334586, 17551709, 17588480, 19827973
17344412, 17842825, 18828868, 17025461, 11883252, 13609098, 17239687
17602269, 19197175, 22195457, 18316692, 17313525, 12611721, 19544839
18964939, 17600719, 18191164, 19393542, 17571306, 20777150, 18482502
19466309, 22243719, 17040527, 17165204, 18098207, 16785708, 17465741
17174582, 16180763, 16777840, 12982566, 19463893, 22195465, 22148226
16875449, 12816846, 17237521, 6599380, 19358317, 17811438, 17811447
17945983, 21983325, 18762750, 16912439, 17184721, 18061914, 17282229
18331850, 18202441, 17082359, 18723434, 21972320, 19554106, 14034426
18339044, 19458377, 17752995, 20448824, 17891943, 17258090, 17767676
16668584, 18384391, 17040764, 17381384, 15913355, 18356166, 14084247
20596234, 20506715, 21756661, 13853126, 18203837, 14245531, 16043574
21756699, 22195441, 17848897, 17877323, 21453153, 17468141, 20861693
17786518, 17912217, 17037130, 16956380, 18155762, 17478145, 17394950
18641461, 18189036, 18619917, 17027426, 21352646, 16268425, 24476274
22195492, 19584068, 18436307, 22507210, 17265217, 17634921, 13498382
21526048, 19258504, 20004087, 17443671, 22195485, 18000422, 22321756
20004021, 17571039, 21067387, 16344544, 18009564, 14354737, 21286665
18135678, 18614015, 20441797, 18362222, 17835048, 16472716, 17936109
17050888, 17325413, 14010183, 18747196, 17761775, 16721594, 17082983
20067212, 21179898, 17302277, 18084625, 15990359, 18203835, 17297939
17811456, 22380919, 16731148, 21168487, 14133975, 13829543, 17215560
17694209, 17385178, 18091059, 8322815, 17586955, 17201159, 17655634
18331812, 19730508, 18868646, 17648596, 16220077, 16069901, 17348614
17393915, 17274537, 17957017, 18096714, 17308789, 18436647, 14285317
19289642, 14764829, 18328509, 17622427, 16943711, 22195477, 14368995
22502493, 17346671, 18996843, 17783588, 21343838, 16618694, 17672719
18856999, 18783224, 17851160, 17546761, 17798953, 18273830, 22092979
16596890, 19972566, 16384983, 17726838, 22296366, 17360606, 22321741
13645875, 18199537, 16542886, 21787056, 17889549, 14565184, 17071721
17610798, 20299015, 21343897, 22893153, 20657441, 17397545, 18230522
16360112, 19769489, 12905058, 18641451, 12747740, 18430495, 17016369
17042658, 14602788, 17551063, 19972568, 21517440, 18508861, 19788842
14657740, 17332800, 13837378, 19972564, 17186905, 18315328, 19699191
17437634, 22353199, 18093615, 19006849, 19013183, 17296856, 18674024
17232014, 16855292, 17762296, 14692762, 21051840, 17705023, 22507234
19121551, 21330264, 19854503, 21868720, 19309466, 18681862, 20558005
18554763, 17390160, 18456514, 16306373, 13955826, 18139690, 17501491
17752121, 21668627, 17299889, 17889583, 18673325, 19721304, 18293054
17242746, 17951233, 18094246, 17649265, 19615136, 17011832, 16870214
17477958, 18522509, 20631274, 16091637, 17323222, 16595641, 16524926
```

```
18228645, 18282562, 17596908, 18031668, 17156148, 16494615, 22683225
17545847, 17655240, 24528741, 17614134, 13558557, 17341326, 17891946
17716305, 22657942, 16392068, 19271443, 21351877, 18092127, 17614227
18440047, 16903536, 14106803, 18973907, 18673342, 19032867, 17389192
17612828, 16194160, 17006570, 17721717, 17390431, 17570240, 16863422
18325460, 19727057, 16422541, 19972570, 17267114, 18244962, 21538485
18765602, 18203838, 16198143, 17246576, 14829250, 17835627, 18247991
14458214, 21051862, 16692232, 17786278, 17227277, 24476265, 16042673
16314254, 16228604, 16837842, 17393683, 23536835, 17787259, 20331945
20074391, 15861775, 16399083, 18018515, 22683212, 18260550, 21051858
17080436, 16613964, 17036973, 16579084, 24433711, 18384537, 18280813
20296213, 16901385, 15979965, 23330124, 18441944, 16450169, 9756271
17892268, 11733603, 16285691, 17587063, 21343775, 18180390, 16538760
18193833, 21387964, 21051833, 17238511, 17824637, 16571443, 18306996
14852021, 17853456, 18674047, 12364061, 22195448
```

Version 11.2.0.4.v9

La version 11.2.0.4.v9 comprend les éléments suivants :

- Correctif Oracle 23615392, une combinaison de PSU de base de données (correctif 23054359) + PSU de composant OJVM (correctif 23177551)
- Fichier de fuseau horaire DSTv26 (correctif 22873635 pour 11.2.0.4)
- Oracle a recommandé les correctifs SGBDR pour Oracle GoldenGate (correctif 24320398 pour 11.2.0.4.160719)
- Groupe MES (correctif 22695784 pour 11.2.0.4)
- Ajout de la possibilité de créer des fonctions personnalisées de vérification de mot de passe. Pour plus d'informations, consultez Création de fonctions personnalisées pour vérifier les mots de passe (p. 1110).
- Correction d'un bogue qui empêchait la recompilation implicite de vues détenues par SYS

Référence : mise à jour d'ensemble de correctifs Oracle Database 11.2.0.4.160719 (correctif 23054359, publié en juillet 2016)

Bogues corrigés :

```
17288409, 21051852, 17811429, 18607546, 17205719, 20506699, 17816865
23330119, 17922254, 17754782, 16934803, 13364795, 17311728, 17441661
17284817, 16992075, 17446237, 14015842, 19972569, 21756677, 17375354
21538558, 20925795, 17449815, 19463897, 13866822, 17982555, 17235750
17478514, 18317531, 14338435, 18235390, 20803583, 13944971, 20142975
17811789, 16929165, 18704244, 20506706, 17546973, 20334344, 14054676
17088068, 17346091, 18264060, 17343514, 21538567, 19680952, 18471685
19211724, 13951456, 21847223, 16315398, 18744139, 16850630, 23177648
19049453, 18673304, 17883081, 19915271, 18641419, 18262334, 17006183
16065166, 18277454, 16833527, 10136473, 18051556, 17865671, 17852463
18554871, 17853498, 18334586, 17551709, 17588480, 19827973, 17344412
17842825, 18828868, 17025461, 11883252, 13609098, 17239687, 17602269
19197175, 22195457, 18316692, 17313525, 12611721, 19544839, 18964939
17600719, 18191164, 19393542, 17571306, 18482502, 20777150, 19466309
17040527, 17165204, 18098207, 16785708, 17465741, 17174582, 16180763
16777840, 12982566, 19463893, 22195465, 16875449, 12816846, 17237521
19358317, 17811438, 17811447, 17945983, 21983325, 18762750, 16912439
17184721, 18061914, 17282229, 18331850, 18202441, 17082359, 18723434
21972320, 19554106, 14034426, 18339044, 19458377, 17752995, 20448824
17891943, 17258090, 17767676, 16668584, 18384391, 17040764, 17381384
15913355, 18356166, 14084247, 20596234, 20506715, 21756661, 13853126
18203837, 14245531, 16043574, 21756699, 22195441, 17848897, 17877323
```

```
21453153, 17468141, 20861693, 17786518, 17912217, 17037130, 16956380
18155762, 17478145, 17394950, 18641461, 18189036, 18619917, 17027426
21352646, 16268425, 22195492, 19584068, 18436307, 22507210, 17265217
17634921, 13498382, 21526048, 19258504, 20004087, 17443671, 22195485
18000422, 22321756, 20004021, 17571039, 21067387, 16344544, 18009564
14354737, 21286665, 18135678, 18614015, 20441797, 18362222, 17835048
16472716, 17936109, 17050888, 17325413, 14010183, 18747196, 17761775
16721594, 17082983, 20067212, 21179898, 17302277, 18084625, 15990359
18203835, 17297939, 22380919, 17811456, 16731148, 21168487, 13829543
17215560, 14133975, 17694209, 17385178, 18091059, 8322815, 17586955
17201159, 17655634, 18331812, 19730508, 18868646, 17648596, 16220077
16069901, 17348614, 17393915, 17274537, 17957017, 18096714, 17308789
18436647, 14285317, 19289642, 14764829, 18328509, 17622427, 16943711
22195477, 14368995, 22502493, 17346671, 18996843, 17783588, 21343838
16618694, 17672719, 18856999, 18783224, 17851160, 17546761, 17798953
18273830, 22092979, 16596890, 19972566, 16384983, 17726838, 22296366
17360606, 22321741, 13645875, 18199537, 16542886, 21787056, 17889549
14565184, 17071721, 17610798, 20299015, 21343897, 22893153, 20657441
17397545, 18230522, 16360112, 19769489, 12905058, 18641451, 12747740
18430495, 17016369, 17042658, 14602788, 17551063, 19972568, 21517440
18508861, 19788842, 14657740, 17332800, 13837378, 19972564, 17186905
18315328, 19699191, 17437634, 22353199, 18093615, 19006849, 19013183
17296856, 18674024, 17232014, 16855292, 17762296, 14692762, 21051840
17705023, 22507234, 19121551, 21330264, 19854503, 21868720, 19309466
18681862, 18554763, 20558005, 17390160, 18456514, 16306373, 13955826
18139690, 17501491, 17752121, 21668627, 17299889, 17889583, 18673325
19721304, 18293054, 17242746, 17951233, 18094246, 17649265, 19615136
17011832, 16870214, 17477958, 18522509, 20631274, 16091637, 17323222
16595641, 16524926, 18228645, 18282562, 17596908, 18031668, 17156148
16494615, 22683225, 17545847, 17655240, 17614134, 13558557, 17341326
17891946, 17716305, 16392068, 19271443, 21351877, 18092127, 17614227
18440047, 16903536, 14106803, 18973907, 18673342, 19032867, 17389192
17612828, 16194160, 17006570, 17721717, 17390431, 17570240, 16863422
18325460, 19727057, 16422541, 19972570, 17267114, 18244962, 21538485
18765602, 18203838, 16198143, 17246576, 14829250, 17835627, 18247991
14458214, 21051862, 16692232, 17786278, 17227277, 16042673, 16314254
16228604, 16837842, 17393683, 23536835, 17787259, 20331945, 20074391
15861775, 16399083, 18018515, 22683212, 18260550, 21051858, 17080436
16613964, 17036973, 16579084, 18384537, 18280813, 20296213, 16901385
15979965, 23330124, 18441944, 16450169, 9756271, 17892268, 11733603
16285691, 17587063, 21343775, 16538760, 18180390, 18193833, 21387964
21051833, 17238511, 17824637, 16571443, 18306996, 14852021, 17853456
18674047, 12364061, 22195448
```

Version 11.2.0.4.v8

La version 11.2.0.4.v8 comprend les éléments suivants :

- PSU Oracle 11.2.0.4.160419 (22502456)
- Fichier de fuseau horaire DSTv25 (correctif 22037014)
- Oracle a recommandé les correctifs SGBDR pour Oracle GoldenGate (correctif 22576728)
- Groupe MES (correctif 22695784 pour 11.2.0.4)
- Ajoute la possibilité pour l'utilisateur principal d'accorder des privilèges sur les objets SYS avec l'option appropriée à l'aide de la procédure RDSADMIN.RDSADMIN_UTIL.GRANT_SYS_OBJECT
- Ajoute des privilèges d'utilisateur principal pour prendre en charge les schémas les plus courants créés par l'utilitaire Oracle Fusion Middleware Repository Creation Utility (RCU)

Référence : mise à jour d'ensemble de correctifs Oracle Database 11.2.0.4.160419 (correctif 22502456, publié en avril 2016)

Bogues corrigés :

```
17288409, 21051852, 17811429, 18607546, 17205719, 20506699, 17816865
17922254, 17754782, 16934803, 13364795, 17311728, 17441661, 17284817
16992075, 17446237, 14015842, 19972569, 21756677, 21538558, 20925795
17449815, 17375354, 19463897, 13866822, 17982555, 17235750, 17478514
18317531, 14338435, 18235390, 20803583, 13944971, 20142975, 17811789
16929165, 18704244, 20506706, 17546973, 20334344, 14054676, 17088068
17346091, 18264060, 17343514, 21538567, 19680952, 18471685, 19211724
13951456, 21847223, 16315398, 18744139, 16850630, 19049453, 18673304
17883081, 19915271, 18641419, 18262334, 17006183, 16065166, 18277454
16833527, 10136473, 18051556, 17865671, 17852463, 18554871, 17853498
18334586, 17551709, 17588480, 19827973, 17344412, 17842825, 18828868
17025461, 11883252, 13609098, 17239687, 17602269, 19197175, 22195457
18316692, 17313525, 12611721, 19544839, 18964939, 17600719, 18191164
19393542, 17571306, 18482502, 20777150, 19466309, 17040527, 17165204
18098207, 16785708, 17465741, 17174582, 16180763, 16777840, 12982566
19463893, 22195465, 16875449, 12816846, 17237521, 19358317, 17811438
17811447, 21983325, 17945983, 18762750, 16912439, 17184721, 18061914
17282229, 18331850, 18202441, 17082359, 18723434, 21972320, 19554106
14034426, 18339044, 19458377, 17752995, 20448824, 17891943, 17258090
17767676, 16668584, 18384391, 17040764, 17381384, 15913355, 18356166
14084247, 20596234, 20506715, 21756661, 13853126, 18203837, 14245531
21756699, 16043574, 22195441, 17848897, 17877323, 21453153, 17468141
20861693, 17786518, 17912217, 17037130, 18155762, 16956380, 17478145
17394950, 18641461, 18189036, 18619917, 17027426, 21352646, 16268425
22195492, 19584068, 18436307, 17265217, 17634921, 13498382, 21526048
19258504, 20004087, 17443671, 22195485, 18000422, 20004021, 22321756
17571039, 21067387, 16344544, 18009564, 14354737, 21286665, 18135678
18614015, 20441797, 18362222, 17835048, 16472716, 17936109, 17050888
17325413, 14010183, 18747196, 17761775, 16721594, 17082983, 20067212
21179898, 17302277, 18084625, 15990359, 18203835, 17297939, 17811456
16731148, 21168487, 13829543, 17215560, 14133975, 17694209, 17385178
18091059, 8322815, 17586955, 17201159, 17655634, 18331812, 19730508
18868646, 17648596, 16220077, 16069901, 17348614, 17393915, 17274537
17957017, 18096714, 17308789, 18436647, 14285317, 19289642, 14764829
18328509, 17622427, 22195477, 16943711, 22502493, 14368995, 17346671
18996843, 17783588, 21343838, 16618694, 17672719, 18856999, 18783224
17851160, 17546761, 17798953, 18273830, 22092979, 16596890, 19972566
16384983, 17726838, 17360606, 22321741, 13645875, 18199537, 16542886
21787056, 17889549, 14565184, 17071721, 17610798, 20299015, 21343897
22893153, 20657441, 17397545, 18230522, 16360112, 19769489, 12905058
18641451, 12747740, 18430495, 17016369, 17042658, 14602788, 17551063
19972568, 21517440, 18508861, 19788842, 14657740, 17332800, 13837378
19972564, 17186905, 18315328, 19699191, 17437634, 22353199, 18093615
19006849, 19013183, 17296856, 18674024, 17232014, 16855292, 17762296
14692762, 21051840, 17705023, 19121551, 21330264, 19854503, 21868720
19309466, 18681862, 18554763, 20558005, 17390160, 18456514, 16306373
13955826, 18139690, 17501491, 17752121, 21668627, 17299889, 17889583
18673325, 19721304, 18293054, 17242746, 17951233, 17649265, 18094246
19615136, 17011832, 16870214, 17477958, 18522509, 20631274, 16091637
17323222, 16595641, 16524926, 18228645, 18282562, 17596908, 17156148
18031668, 16494615, 22683225, 17545847, 17655240, 17614134, 13558557
17341326, 17891946, 17716305, 16392068, 19271443, 21351877, 18092127
18440047, 17614227, 14106803, 16903536, 18973907, 18673342, 19032867
17389192, 17612828, 16194160, 17006570, 17721717, 17390431, 17570240
16863422, 18325460, 19727057, 16422541, 19972570, 17267114, 18244962
21538485, 18765602, 18203838, 16198143, 17246576, 14829250, 17835627
18247991, 14458214, 21051862, 16692232, 17786278, 17227277, 16042673
16314254, 16228604, 16837842, 17393683, 17787259, 20331945, 20074391
```

```
15861775, 16399083, 18018515, 22683212, 18260550, 21051858, 17036973
16613964, 17080436, 16579084, 18384537, 18280813, 20296213, 16901385
15979965, 18441944, 16450169, 9756271, 17892268, 11733603, 16285691
17587063, 21343775, 16538760, 18180390, 18193833, 21387964, 21051833
17238511, 17824637, 16571443, 18306996, 14852021, 18674047, 17853456
12364061, 22195448
```

Version 11.2.0.4.v7

La version 11.2.0.4.v7 comprend les éléments suivants :

- PSU Oracle 11.2.0.4.160119 (21948347)
- DSTv25 fichier de fuseau horaire - correctif 22037014 pour 11.2.0.4 et 12.1.0.2 (12.1.0.1 inclut DSTv24, correctif 20875898 (pas de modification par rapport à 12.1.0.1.v3), comme rétroportage de DSTv25 n'était pas disponible au moment de la version)
- Correction d'un problème qui empêchait les clients de créer plus de 10 objets de répertoire dans la base de données
- Correction d'un problème qui empêchait les clients de réaccorder des privilèges de lecture sur les objets de répertoire ADUMP et BDUMP

Référence : mise à jour d'ensemble de correctifs Oracle Database 11.2.0.4.160119 (correctif 21948347, publié en janvier 2016)

Bogues corrigés :

```
17288409, 21051852, 18607546, 17205719, 17811429, 17816865, 20506699
17922254, 17754782, 16934803, 13364795, 17311728, 17441661, 17284817
16992075, 17446237, 14015842, 19972569, 17449815, 21538558, 20925795
17375354, 19463897, 17982555, 17235750, 13866822, 17478514, 18317531
18235390, 14338435, 20803583, 13944971, 20142975, 17811789, 16929165
18704244, 20506706, 17546973, 20334344, 14054676, 17088068, 18264060
17346091, 17343514, 21538567, 19680952, 18471685, 19211724, 13951456
21847223, 16315398, 18744139, 16850630, 19049453, 18673304, 17883081
19915271, 18641419, 18262334, 17006183, 16065166, 18277454, 16833527
10136473, 18051556, 17865671, 17852463, 18554871, 17853498, 18334586
17588480, 17551709, 19827973, 17842825, 17344412, 18828868, 17025461
11883252, 13609098, 17239687, 17602269, 19197175, 22195457, 18316692
17313525, 12611721, 19544839, 18964939, 17600719, 18191164, 19393542
17571306, 18482502, 20777150, 19466309, 17040527, 17165204, 18098207
16785708, 17174582, 16180763, 17465741, 16777840, 12982566, 19463893
22195465, 12816846, 16875449, 17237521, 19358317, 17811438, 17811447
17945983, 18762750, 17184721, 16912439, 18061914, 17282229, 18331850
18202441, 17082359, 18723434, 21972320, 19554106, 14034426, 18339044
19458377, 17752995, 20448824, 17891943, 17258090, 17767676, 16668584
18384391, 17040764, 17381384, 15913355, 18356166, 14084247, 20506715
13853126, 18203837, 14245531, 21756699, 16043574, 22195441, 17848897
17877323, 21453153, 17468141, 20861693, 17786518, 17912217, 17037130
18155762, 16956380, 17478145, 17394950, 18189036, 18641461, 18619917
17027426, 21352646, 16268425, 22195492, 19584068, 18436307, 17265217
17634921, 13498382, 21526048, 20004087, 22195485, 17443671, 18000422
22321756, 20004021, 17571039, 21067387, 16344544, 18009564, 14354737
18135678, 18614015, 20441797, 18362222, 17835048, 16472716, 17936109
17050888, 17325413, 14010183, 18747196, 17761775, 16721594, 17082983
20067212, 21179898, 17302277, 18084625, 15990359, 18203835, 17297939
17811456, 16731148, 21168487, 17215560, 13829543, 14133975, 17694209
18091059, 17385178, 8322815, 17586955, 17201159, 17655634, 18331812
19730508, 18868646, 17648596, 16220077, 16069901, 17348614, 17393915
```

```
17274537, 17957017, 18096714, 17308789, 18436647, 14285317, 19289642
14764829, 18328509, 17622427, 22195477, 16943711, 14368995, 17346671
18996843, 17783588, 21343838, 16618694, 17672719, 18856999, 18783224
17851160, 17546761, 17798953, 18273830, 22092979, 19972566, 16384983
17726838, 17360606, 22321741, 13645875, 18199537, 16542886, 21787056
17889549, 14565184, 17071721, 17610798, 20299015, 21343897, 20657441
17397545, 18230522, 16360112, 19769489, 12905058, 18641451, 12747740
18430495, 17042658, 17016369, 14602788, 17551063, 19972568, 21517440
18508861, 19788842, 14657740, 17332800, 13837378, 19972564, 17186905
18315328, 19699191, 17437634, 19006849, 19013183, 17296856, 18674024
17232014, 16855292, 21051840, 14692762, 17762296, 17705023, 19121551
21330264, 19854503, 19309466, 18681862, 18554763, 20558005, 17390160
18456514, 16306373, 13955826, 18139690, 17501491, 21668627, 17299889
17752121, 17889583, 18673325, 18293054, 17242746, 17951233, 17649265
18094246, 19615136, 17011832, 16870214, 17477958, 18522509, 20631274
16091637, 17323222, 16595641, 16524926, 18228645, 18282562, 17596908
17156148, 18031668, 16494615, 17545847, 17655240, 17614134, 13558557
17341326, 17891946, 17716305, 16392068, 19271443, 21351877, 18092127
18440047, 17614227, 14106803, 16903536, 18973907, 18673342, 19032867
17389192, 17612828, 16194160, 17006570, 17721717, 17570240, 17390431
16863422, 18325460, 19727057, 16422541, 19972570, 17267114, 18244962
21538485, 18765602, 18203838, 16198143, 17246576, 14829250, 17835627
18247991, 14458214, 21051862, 16692232, 17786278, 17227277, 16042673
16314254, 16228604, 16837842, 17393683, 17787259, 20331945, 20074391
15861775, 16399083, 18018515, 21051858, 18260550, 17036973, 16613964
17080436, 16579084, 18384537, 18280813, 20296213, 16901385, 15979965
18441944, 16450169, 9756271, 17892268, 11733603, 16285691, 17587063
21343775, 16538760, 18180390, 18193833, 21051833, 17238511, 17824637
16571443, 18306996, 14852021, 18674047, 17853456, 12364061, 22195448
```

Version 11.2.0.4.v6

La version 11.2.0.4.v6 inclut les éléments suivants :

- Permet le chiffrement SSL pour Standard Edition et Standard Edition One

Version 11.2.0.4.v5

La version 11.2.0.4.v5 comprend les éléments suivants :

- PSU Oracle 11.2.0.4.8 (21352635)
- Inclut le correctif de l'heure d'été, correctif 20875898 : DST-24, sorti après la PSU Avril 2015.

Référence : mise à jour d'ensemble de correctifs Oracle Database 11.2.0.4.8 (correctif 21352635, publié en octobre 2015)

Bogues corrigés :

```
17288409, 21051852, 18607546, 17205719, 17811429, 17816865, 20506699
17922254, 17754782, 16934803, 13364795, 17311728, 17441661, 17284817
16992075, 17446237, 14015842, 19972569, 21538558, 20925795, 17449815
17375354, 19463897, 17982555, 17235750, 13866822, 18317531, 17478514
18235390, 14338435, 20803583, 13944971, 20142975, 17811789, 16929165
18704244, 20506706, 17546973, 20334344, 14054676, 17088068, 18264060
17346091, 17343514, 21538567, 19680952, 18471685, 19211724, 13951456
16315398, 18744139, 16850630, 19049453, 18673304, 17883081, 19915271
```

```
18641419, 18262334, 17006183, 16065166, 18277454, 16833527, 10136473
18051556, 17865671, 17852463, 18554871, 17853498, 18334586, 17588480
17551709, 19827973, 17842825, 17344412, 18828868, 17025461, 11883252
13609098, 17239687, 17602269, 19197175, 18316692, 17313525, 12611721
19544839, 18964939, 17600719, 18191164, 19393542, 17571306, 18482502
20777150, 19466309, 17040527, 17165204, 18098207, 16785708, 17174582
16180763, 17465741, 16777840, 12982566, 19463893, 12816846, 16875449
17237521, 19358317, 17811438, 17811447, 17945983, 18762750, 17184721
16912439, 18061914, 17282229, 18331850, 18202441, 17082359, 18723434
19554106, 14034426, 18339044, 19458377, 17752995, 20448824, 17891943
17258090, 17767676, 16668584, 18384391, 17040764, 17381384, 15913355
18356166, 14084247, 20506715, 13853126, 18203837, 14245531, 16043574
17848897, 17877323, 17468141, 17786518, 17912217, 17037130, 18155762
16956380, 17478145, 17394950, 18189036, 18641461, 18619917, 17027426
21352646, 16268425, 19584068, 18436307, 17265217, 17634921, 13498382
20004087, 17443671, 18000422, 20004021, 17571039, 21067387, 16344544
18009564, 14354737, 18135678, 18614015, 20441797, 18362222, 17835048
16472716, 17936109, 17050888, 17325413, 14010183, 18747196, 17761775
16721594, 17082983, 20067212, 21179898, 17302277, 18084625, 15990359
18203835, 17297939, 17811456, 16731148, 17215560, 13829543, 14133975
17694209, 18091059, 17385178, 8322815, 17586955, 17201159, 17655634
18331812, 19730508, 18868646, 17648596, 16220077, 16069901, 17348614
17393915, 17274537, 17957017, 18096714, 17308789, 18436647, 14285317
19289642, 14764829, 18328509, 17622427, 16943711, 14368995, 17346671
18996843, 17783588, 16618694, 17672719, 18856999, 18783224, 17851160
17546761, 17798953, 18273830, 19972566, 16384983, 17726838, 17360606
13645875, 18199537, 16542886, 17889549, 14565184, 17071721, 20299015
17610798, 20657441, 17397545, 18230522, 16360112, 19769489, 12905058
18641451, 12747740, 18430495, 17042658, 17016369, 14602788, 19972568
18508861, 19788842, 14657740, 17332800, 13837378, 19972564, 17186905
18315328, 19699191, 17437634, 19006849, 19013183, 17296856, 18674024
17232014, 16855292, 21051840, 14692762, 17762296, 17705023, 19121551
19854503, 19309466, 18681862, 18554763, 20558005, 17390160, 18456514
16306373, 13955826, 18139690, 17501491, 17299889, 17752121, 17889583
18673325, 18293054, 17242746, 17951233, 17649265, 18094246, 19615136
17011832, 16870214, 17477958, 18522509, 20631274, 16091637, 17323222
16595641, 16524926, 18228645, 18282562, 17596908, 17156148, 18031668
16494615, 17545847, 17614134, 13558557, 17341326, 17891946, 17716305
16392068, 19271443, 18092127, 18440047, 17614227, 14106803, 16903536
18973907, 18673342, 17389192, 16194160, 17006570, 17612828, 17721717
17570240, 17390431, 16863422, 18325460, 19727057, 16422541, 19972570
17267114, 18244962, 21538485, 18765602, 18203838, 16198143, 17246576
14829250, 17835627, 18247991, 14458214, 21051862, 16692232, 17786278
17227277, 16042673, 16314254, 16228604, 16837842, 17393683, 17787259
20331945, 20074391, 15861775, 16399083, 18018515, 18260550, 21051858
17036973, 16613964, 17080436, 16579084, 18384537, 18280813, 20296213
16901385, 15979965, 18441944, 16450169, 9756271, 17892268, 11733603
16285691, 17587063, 16538760, 18180390, 18193833, 21051833, 17238511
17824637, 16571443, 18306996, 14852021, 18674047, 17853456, 12364061
```

Version 11.2.0.4.v4

La version 11.2.0.4.v4 comprend les éléments suivants :

- PSU Oracle 11.2.0.4.6 (20299013)
- Installe des bases de connaissances Oracle Text supplémentaires depuis Oracle Database. Exemples de média (anglais et français)
- Accès fourni à DBMS_REPAIR via RDSADMIN.RDSADMIN_DBMS_REPAIR
- Accorde ALTER DATABASE LINK, ALTER PUBLIC DATABASE LINK, EXEMPT ACCESS POLICY, EXEMPT IDENTITY POLICY et EXEMPT REDACTION POLICY à l'utilisateur maître

Référence : mise à jour d'ensemble de correctifs Oracle Database 11.2.0.4.6 (correctif 20299013, publié en avril 2015)

Bogues corrigés :

```
17288409, 17798953, 18273830, 18607546, 17811429, 17205719, 20506699
17816865, 19972566, 17922254, 17754782, 16384983, 17726838, 13364795
16934803, 17311728, 17284817, 17441661, 17360606, 13645875, 18199537
16992075, 16542886, 17446237, 14015842, 17889549, 14565184, 19972569
17071721, 20299015, 17610798, 17375354, 17449815, 17397545, 19463897
18230522, 13866822, 17235750, 17982555, 16360112, 18317531, 17478514
19769489, 12905058, 14338435, 18235390, 13944971, 18641451, 20142975
17811789, 16929165, 18704244, 12747740, 18430495, 20506706, 17546973
14054676, 17088068, 17346091, 18264060, 17016369, 17042658, 17343514
14602788, 19972568, 19680952, 18471685, 19788842, 18508861, 14657740
17332800, 19211724, 13837378, 13951456, 16315398, 17186905, 18744139
19972564, 16850630, 18315328, 17437634, 19049453, 18673304, 17883081
19006849, 19915271, 19013183, 18641419, 17296856, 18674024, 18262334
17006183, 18277454, 16833527, 17232014, 16855292, 10136473, 17762296
14692762, 17705023, 18051556, 17865671, 17852463, 18554871, 17853498
19121551, 18334586, 19854503, 17551709, 19309466, 17588480, 19827973
17344412, 17842825, 18828868, 18681862, 18554763, 17390160, 18456514
16306373, 17025461, 13955826, 18139690, 11883252, 13609098, 17501491
17239687, 17752121, 17299889, 17602269, 19197175, 17889583, 18316692
17313525, 18673325, 12611721, 19544839, 18293054, 17242746, 18964939
17600719, 18191164, 19393542, 17571306, 18482502, 19466309, 17951233
17649265, 18094246, 19615136, 17040527, 17011832, 17165204, 18098207
16785708, 16870214, 17465741, 16180763, 17174582, 17477958, 12982566
16777840, 18522509, 20631274, 16091637, 17323222, 19463893, 16595641
16875449, 12816846, 16524926, 17237521, 18228645, 18282562, 17596908
19358317, 17811438, 17811447, 17945983, 18762750, 17156148, 18031668
16912439, 17184721, 16494615, 18061914, 17282229, 17545847, 18331850
18202441, 17082359, 18723434, 19554106, 17614134, 13558557, 17341326
14034426, 17891946, 18339044, 17716305, 19458377, 17752995, 16392068
19271443, 17891943, 18092127, 17258090, 17767676, 16668584, 18384391
17614227, 17040764, 16903536, 17381384, 14106803, 15913355, 18973907
18356166, 18673342, 17389192, 14084247, 16194160, 17612828, 17006570
20506715, 17721717, 13853126, 17390431, 18203837, 17570240, 14245531
16043574, 16863422, 17848897, 17877323, 18325460, 19727057, 17468141
17786518, 17912217, 16422541, 19972570, 17267114, 17037130, 18244962
18765602, 18203838, 18155762, 16956380, 16198143, 17246576, 17478145
17394950, 14829250, 18189036, 18641461, 18619917, 17835627, 17027426
16268425, 18247991, 19584068, 14458214, 18436307, 17265217, 17634921
13498382, 16692232, 17786278, 17227277, 16042673, 16314254, 17443671
18000422, 16228604, 16837842, 17571039, 17393683, 16344544, 17787259
18009564, 20074391, 14354737, 15861775, 18135678, 18614015, 16399083
18362222, 18018515, 16472716, 17835048, 17050888, 17936109, 14010183
17325413, 18747196, 17080436, 16613964, 17036973, 17761775, 16579084
16721594, 17082983, 18384537, 18280813, 20296213, 17302277, 16901385
18084625, 15979965, 15990359, 18203835, 17297939, 17811456, 16731148
13829543, 14133975, 17215560, 17694209, 18091059, 17385178, 8322815
17586955, 18441944, 17201159, 16450169, 9756271, 17655634, 19730508
17892268, 18868646, 17648596, 16220077, 16069901, 11733603, 16285691
17587063, 18180390, 16538760, 18193833, 17348614, 17393915, 17957017
17274537, 18096714, 17308789, 17238511, 18436647, 17824637, 14285317
19289642, 14764829, 17622427, 18328509, 16571443, 16943711, 14368995
18306996, 17346671, 14852021, 18996843, 17783588, 16618694, 17853456
18674047, 17672719, 18856999, 12364061, 18783224, 17851160, 17546761
```

Version 11.2.0.4.v3

La version 11.2.0.4.v3 inclut les éléments suivants :

- PSU Oracle 11.2.0.4.4 (19121551)
- Fichier DST le plus récent (DSTv23 – correctif 19396455, publié en octobre 2014). Ce correctif est intégré par défaut dans de nouvelles instances uniquement.

Référence : mise à jour d'ensemble de correctifs Oracle Database 11.2.0.4.4 (correctif 19121551, publié en octobre 2014)

Bogues corrigés :

```
19396455, 18759211, 17432124, 16799735,
17288409, 17205719, 17811429, 17754782, 17726838, 13364795, 17311728
17284817, 17441661, 13645875, 18199537, 16992075, 16542886, 17446237
14565184, 17071721, 17610798, 17375354, 17449815, 17397545, 19463897
18230522, 17235750, 16360112, 13866822, 17982555, 17478514, 12905058
14338435, 13944971, 16929165, 12747740, 17546973, 14054676, 17088068
18264060, 17343514, 17016369, 17042658, 14602788, 14657740, 17332800
19211724, 13951456, 16315398, 17186905, 18744139, 16850630, 17437634
19049453, 18673304, 17883081, 18641419, 17296856, 18262334, 17006183
18277454, 17232014, 16855292, 10136473, 17705023, 17865671, 18554871
19121551, 17588480, 17551709, 17344412, 17842825, 18681862, 17390160
13955826, 13609098, 18139690, 17501491, 17239687, 17752121, 17299889
17602269, 18673325, 17313525, 17242746, 19544839, 17600719, 18191164
17571306, 19466309, 17951233, 18094246, 17165204, 17011832, 17040527
16785708, 16180763, 17477958, 17174582, 17465741, 18522509, 17323222
19463893, 16875449, 16524926, 17237521, 17596908, 17811438, 17811447
18031668, 16912439, 16494615, 18061914, 17545847, 17082359, 19554106
17614134, 17341326, 17891946, 19458377, 17716305, 17752995, 16392068
19271443, 17767676, 17614227, 17040764, 17381384, 18973907, 18673342
14084247, 17389192, 17006570, 17612828, 17721717, 13853126, 18203837
17390431, 17570240, 14245531, 16043574, 16863422, 19727057, 17468141
17786518, 17037130, 17267114, 18203838, 16198143, 16956380, 17478145
14829250, 17394950, 17027426, 16268425, 18247991, 19584068, 14458214
18436307, 17265217, 13498382, 16692232, 17786278, 17227277, 16042673
16314254, 17443671, 16228604, 16837842, 17393683, 17787259, 18009564
15861775, 16399083, 18018515, 16472716, 17050888, 14010183, 17325413
16613964, 17080436, 17036973, 17761775, 16721594, 18280813, 15979965
18203835, 17297939, 16731148, 17811456, 14133975, 17385178, 17586955
16450169, 17655634, 9756271, 17892268, 17648596, 16220077, 16069901
11733603, 16285691, 17587063, 18180390, 17393915, 18096714, 17238511
17824637, 14285317, 19289642, 14764829, 18328509, 17622427, 16943711
17346671, 18996843, 14852021, 17783588, 16618694, 17672719, 17546761
```

Version 11.2.0.4.v2 (obsolète)

La version 11.2.0.4.v2 comprend les éléments suivants :

- PSU Oracle 11.2.0.4.3 (18522509)
- Accès utilisateur au package DBMS_TRANSACTION pour nettoyer des échecs de transactions distribuées
- Fichier DST le plus récent (DSTv22 – correctif 18759211, publié en juin 2014). Ce correctif est intégré par défaut uniquement dans de nouvelles instances de base de données Oracle.
- Accorde DBMS_REPUTIL au rôle DBA (mise à niveau vers 11.2.0.4 entraîne une révocation du public)

- Privilèges accordés sur DBMS_TRANSACTION, `v$pending_xatrans$` et `v$xatrans$`
- Résout un problème avec des commandes DDL lorsque des objets utilisateur ont « SYSTEM » dans leurs noms
- Installe des objets de schéma pour prendre en charge des transactions XA, ce qui permet la gestion de transactions par un gestionnaire de transaction externe
- Permet la troncation d'objets SYS et SYSTEM temporaires, autorisant des outils tels que LogMiner à fonctionner correctement

Référence : mise à jour d'ensemble de correctifs Oracle Database 11.2.0.4.3 (correctif 18522509, publié en juillet 2014)

Bogues corrigés :

```
17432124, 18759211, 18522509, 18031668, 17478514,
17752995, 17288409, 16392068, 17205719, 17811429, 17767676, 17614227
17040764, 17381384, 17754782, 17726838, 13364795, 17311728, 17389192
17006570, 17612828, 17284817, 17441661, 13853126, 17721717, 13645875
18203837, 17390431, 16542886, 16992075, 16043574, 17446237, 16863422
14565184, 17071721, 17610798, 17468141, 17786518, 17375354, 17397545
18203838, 16956380, 17478145, 16360112, 17235750, 17394950, 13866822
17478514, 17027426, 12905058, 14338435, 16268425, 13944971, 18247991
14458214, 16929165, 17265217, 13498382, 17786278, 17227277, 17546973
14054676, 17088068, 16314254, 17016369, 14602788, 17443671, 16228604
16837842, 17332800, 17393683, 13951456, 16315398, 18744139, 17186905
16850630, 17437634, 19049453, 17883081, 15861775, 17296856, 18277454
16399083, 16855292, 18018515, 10136473, 16472716, 17050888, 17865671
17325413, 14010183, 18554871, 17080436, 16613964, 17761775, 16721594
17588480, 17551709, 17344412, 18681862, 15979965, 13609098, 18139690
17501491, 17239687, 17752121, 17602269, 18203835, 17297939, 17313525
16731148, 17811456, 14133975, 17600719, 17385178, 17571306, 16450169
17655634, 18094246, 17892268, 17165204, 17011832, 17648596, 16785708
17477958, 16180763, 16220077, 17465741, 17174582, 18522509, 16069901
16285691, 17323222, 18180390, 17393915, 16875449, 18096714, 17238511
```

Version 11.2.0.4.v1

La version 11.2.0.4.v1 comprend les éléments suivants :

- PSU Oracle 11.2.0.4.1
- Création et suppression de répertoires dans l'espace de stockage de données principal (p. 1164)

Référence : mise à jour d'ensemble de correctifs Oracle Database 11.2.0.4.1 (publié en janvier 2014)

Bogues corrigés :

```
17432124, 16850630, 17551709, 13944971, 17811447, 13866822, 17811429,
16069901
16721594, 17443671, 17478514, 17612828, 17610798, 17239687, 17501491
17446237, 16450169, 17811438, 17288409, 17811456, 12905058, 17088068
16285691, 17332800
```

PostgreSQL sur Amazon RDS

Amazon RDS prend en charge les instances de bases de données qui exécutent plusieurs versions de PostgreSQL. Vous pouvez créer des instances de bases de données et des instantanés de base de données, ainsi que des restaurations et des sauvegardes à un moment donné. Les instances de base de données qui exécutent PostgreSQL prennent en charge les déploiements multi-AZ, les réplicas en lecture et les IOPS provisionnés, et peuvent être créées au sein d'un VPC. Vous pouvez également utiliser le protocole SSL pour vous connecter à une instance de base de données exécutant PostgreSQL.

Avant de créer une instance de base de données, vous devez suivre la procédure de la section Configuration pour Amazon RDS (p. 62) du présent guide.

Vous pouvez utiliser une application cliente SQL standard quelconque pour exécuter les commandes pour l'instance à partir de votre ordinateur client. De telles applications incluent pgAdmin, un outil d'administration et de développement Open Source fréquemment utilisé pour PostgreSQL, ou psql, un utilitaire de ligne de commande inclus dans une installation PostgreSQL. Pour offrir une expérience de service géré, Amazon RDS ne fournit pas d'accès d'hôte aux instances de base de données et il restreint l'accès à certaines procédures de systèmes et à des tables qui nécessitent des privilèges avancés. Amazon RDS prend en charge l'accès aux bases de données sur une instance de base de données qui utilise toute application de client SQL standard. Amazon RDS ne permet pas l'accès direct des hôtes à une instance de base de données à l'aide de Telnet ou Secure Shell (SSH).

Amazon RDS pour PostgreSQL est conforme à de nombreuses normes du secteur. Par exemple, vous pouvez utiliser Amazon RDS pour les bases de données PostgreSQL afin de créer des applications conformes à HIPAA et de stocker des informations liées à la santé, y compris des informations de santé protégées (ISP) sous un Accord BAA (Business Associate Agreement) conclu avec AWS. Amazon RDS pour PostgreSQL satisfait également les exigences de sécurité du Programme de gestion de risque et d'autorisation fédérale (FedRAMP). Amazon RDS pour PostgreSQL a reçu l'autorité provisoire du Conseil d'autorisation conjoint (CAC) de FedRAMP d'opérer (P-ATO) au niveau de la base de références FedRAMP HIGH au sein de la région AWS GovCloud (USA Ouest). Pour de plus amples informations sur les normes de conformité prises en charge, veuillez consulter Conformité du Cloud AWS.

Pour importer des données PostgreSQL dans une instance de base de données, suivez les informations fournies dans la section Importation de données dans PostgreSQL sur Amazon RDS (p. 1388).

Rubriques

- Tâches courantes de gestion pour PostgreSQL sur Amazon RDS (p. 1362)
- Connexion à une instance de base de données exécutant le moteur de base de données PostgreSQL (p. 1364)
- Mise à jour des applications pour se connecter aux instances de bases de données PostgreSQL à l'aide des nouveaux certificats SSL/TLS (p. 1369)
- Mise à niveau du moteur de base de données PostgreSQL pour Amazon RDS (p. 1373)
- Mise à niveau d'un instantané de base de données PostgreSQL (p. 1382)
- Utilisation de réplicas en lecture PostgreSQL dans Amazon RDS (p. 1384)
- Importation de données dans PostgreSQL sur Amazon RDS (p. 1388)
- Exportation de données à partir d'une instance de base de données RDS for PostgreSQL vers Amazon S3 (p. 1409)
- Tâches DBA courantes pour PostgreSQL (p. 1419)
- Utilisation de l'authentification Kerberos avec Amazon RDS pour PostgreSQL (p. 1450)
- Utilisation de l'environnement en préversion de base de données (p. 1465)

- Versions et extensions Amazon RDS pour PostgreSQL (p. 1468)

Tâches courantes de gestion pour PostgreSQL sur Amazon RDS

Vous trouverez ci-dessous les tâches courantes de gestion que vous exécutez avec une instance de base de données Amazon RDS pour PostgreSQL, avec des liens vers la documentation appropriée relative à chaque tâche.

Type de tâche	Documentation
Configuration d'Amazon RDS pour la première utilisation Des prérequis doivent être effectués avant la création de votre instance de base de données. Par exemple, des instances de bases de données sont créées par défaut avec un pare-feu qui empêche d'y accéder. Vous devez donc créer un groupe de sécurité avec les adresses IP correctes et la configuration réseau permettant d'accéder à l'instance de base de données.	Configuration pour Amazon RDS (p. 62)
Présentation des instances de bases de données d'Amazon RDS Si vous créez une instance de base de données à des fins de production, vous devez comprendre comment les classes d'instance, les types de stockage et les IOPS provisionnées fonctionnent dans Amazon RDS.	Classes d'instances de base de données (p. 6) Types de stockage Amazon RDS (p. 30) Stockage SSD d'I/O par seconde provisionnées (p. 33)
Recherche de versions de PostgreSQL prises en charge Amazon RDS prend en charge plusieurs versions de PostgreSQL.	Versions de base de données PostgreSQL prises en charge (p. 1468)
Configuration de la haute disponibilité et de la prise en charge du basculement Une instance de base de données de production doit utiliser des déploiements Multi-AZ. Les déploiements Multi-AZ améliorent la disponibilité, la durabilité des données et la tolérance aux pannes pour les instances de bases de données.	Haute disponibilité (multi-AZ) pour Amazon RDS (p. 43)
Présentation du réseau Amazon Virtual Private Cloud (VPC) Si votre compte AWS possède un VPC par défaut, votre instance de base de données est automatiquement créée dans le VPC par défaut. Dans certains cas, votre compte peut ne pas avoir de VPC par défaut, et vous pouvez souhaiter que l'instance de base de données soit dans un VPC. Dans ce cas, créez le VPC et les groupes de sous-réseau avant de créer l'instance de base de données.	Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611) Utilisation d'une instance de base de données dans un VPC (p. 1620)
Importation de données dans Amazon RDS PostgreSQL Vous pouvez utiliser différents outils pour importer des données dans votre instance de base de données PostgreSQL sur Amazon RDS.	Importation de données dans PostgreSQL sur Amazon RDS (p. 1388)

Type de tâche	Documentation
Configuration des réplicas en lecture (principaux et de secours) en lecture seule PostgreSQL sur Amazon RDS prend en charge les réplicas en lecture se trouvant dans la même région AWS et dans une région AWS différente de l'instance principale.	Utilisation des réplicas en lecture (p. 275) Utilisation de réplicas en lecture PostgreSQL dans Amazon RDS (p. 1384) Création d'un réplica en lecture dans une autre région AWS (p. 284)
Présentation des groupes de sécurité Par défaut, les instances de bases de données sont créées avec un pare-feu qui empêche d'y accéder. Vous devez donc créer un groupe de sécurité avec les adresses IP correctes et la configuration réseau permettant d'accéder à l'instance de base de données. En général, si votre instance de base de données se trouve sur la plateforme EC2-Classic, vous devez créer un groupe de sécurité de base de données. Si votre instance de base de données se trouve sur la plateforme EC2-VPC, vous devez créer un groupe de sécurité VPC.	Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611) Contrôle d'accès par groupe de sécurité (p. 1590)
Configuration des fonctionnalités et des groupes de paramètres Si votre instance de base de données doit nécessiter des paramètres de base de données spécifiques, vous devez créer un groupe de paramètres avant de créer l'instance de base de données.	Utilisation de groupes de paramètres de base de données (p. 225)
Exécution des tâches d'administration de base de données courantes pour PostgreSQL Parmi les tâches de bases de données d'un DBA PostgreSQL, citons : • Création de rôles (p. 1420) • Gestion d'un accès à la base de données PostgreSQL (p. 1420) • Utilisation des paramètres PostgreSQL (p. 1421) • Utilisation de la fonction autovacuum de PostgreSQL sur Amazon RDS (p. 1431) • Journalisation d'audit pour une instance de base de données PostgreSQL (p. 1440) • Utilisation de PostGIS (p. 1443) • Utilisation de pgBadger pour l'analyse de journal serveur avec PostgreSQL (p. 1445) • Utilisation d'un serveur DNS personnalisé pour l'accès réseau sortant. (p. 1448)	Tâches DBA courantes pour PostgreSQL (p. 1419)

Type de tâche	Documentation
Connexion à votre instance de base de données PostgreSQL Après avoir créé un groupe de sécurité et l'avoir associé à une instance de base de données, vous pouvez vous connecter à l'instance de base de données en utilisant une application cliente SQL standard quelconque comme pgadmin III.	Connexion à une instance de base de données exécutant le moteur de base de données PostgreSQL (p. 1364) Utilisation de SSL avec une instance de base de données PostgreSQL (p. 1515)
Sauvegarde et restauration de votre instance de base de données Vous pouvez configurer votre instance de base de données pour que les sauvegardes soient exécutées automatiquement ou que les instantanés soient créés manuellement, puis que les instances soient restaurées à partir des sauvegardes ou des instantanés.	Sauvegarde et restauration d'une instance de base de données Amazon RDS (p. 317)
Surveillance de l'activité et des performances de votre instance de base de données Vous pouvez surveiller une instance de base de données PostgreSQL en utilisant les métriques CloudWatch Amazon RDS, les événements et la supervision améliorée.	Affichage des métriques d'instances de base de données (p. 384) Affichage d'événements Amazon RDS (p. 486)
Mise à niveau de la version de base de données PostgreSQL Vous pouvez procéder à la mise à niveau des versions majeures et mineures de votre instance de base de données PostgreSQL.	Mise à niveau d'une instance de base de données PostgreSQL (p. 1515) Choix d'une mise à niveau de version majeure pour PostgreSQL (p. 1375)
Utilisation des fichiers journaux Vous pouvez accéder aux fichiers journaux de votre instance de base de données PostgreSQL.	Fichiers journaux de base de données PostgreSQL (p. 521)
Présentation des bonnes pratiques pour les instances de bases de données PostgreSQL Découvrez certaines des meilleures pratiques pour l'utilisation de PostgreSQL sur Amazon RDS.	Bonnes pratiques pour utiliser les moteurs de stockage PostgreSQL (p. 142)

Connexion à une instance de base de données exécutant le moteur de base de données PostgreSQL

Après qu'Amazon RDS a provisionné votre instance de base de données, vous pouvez utiliser n'importe quelle application cliente SQL standard pour vous connecter à l'instance. Pour répertorier les détails d'une instance de base de données Amazon RDS, vous pouvez utiliser l'AWS Management Console, la commande describe-db-instances de l'AWS CLI ou l'opération d'API Amazon RDS DescribeDBInstances. Vous avez besoin des informations suivantes pour vous connecter :

- L'hôte ou le nom d'hôte de l'instance de base de données, par exemple :

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

- Le port au niveau duquel l'instance de base de données écoute. Par exemple, le port PostgreSQL par défaut est 5432.
- Le nom d'utilisateur et le mot de passe de l'instance de base de données.

Voici deux façons de se connecter à une instance de base de données PostgreSQL. Le premier exemple utilise pgAdmin, célèbre outil open source d'administration et de développement pour PostgreSQL. Le second exemple utilise psql, utilitaire de ligne de commande qui fait partie d'une installation PostgreSQL.

Utilisation de pgAdmin pour se connecter à une instance de base de données PostgreSQL

Vous pouvez utiliser l'outil open source pgAdmin pour vous connecter à une instance de base de données PostgreSQL.

Pour vous connecter à une instance de base de données PostgreSQL avec pgAdmin

1. Trouvez le point de terminaison (nom DNS) et le numéro de port pour votre instance de base de données.
   a. Ouvrez la console RDS et choisissez Bases de données pour afficher une liste de vos instances de bases de données.
   b. Choisissez le nom de l'instance de base de données PostgreSQL pour afficher ses détails.
   c. Dans l'onglet Connectivity & security (Connectivité et sécurité), copiez le point de terminaison. Notez également le numéro du port. Vous avez besoin du point de terminaison et du numéro de port pour vous connecter à l'instance de base de données.

2. Installez pgAdmin depuis http://www.pgadmin.org/. Vous pouvez télécharger et utiliser pgAdmin sans avoir une instance locale de PostgreSQL sur votre ordinateur client.
3. Lancez l'application pgAdmin sur votre ordinateur client.
4. Dans l'onglet Tableau de bord, choisissez Add New Server (Ajouter un nouveau serveur).
5. Dans la boîte de dialogue Create - Server (Créer - Serveur), entrez un nom sur l'onglet Général pour identifier le serveur dans pgAdmin.
6. Dans l'onglet Connexion, tapez les informations suivantes depuis votre instance de base de données :
   - Pour Hôte, tapez le point de terminaison, par exemple `mypostgresql.c6c8dntfzzhgv0.us-east-2.rds.amazonaws.com`.
   - Pour Port, tapez le port attribué.
   - Pour Nom d'utilisateur, tapez le nom d'utilisateur entré lors de la création de l'instance de base de données.

- Pour Mot de passe, tapez le mot de passe entré lors de la création de l'instance de base de données.

7. Choisissez Enregistrer.

   Si vous rencontrez des problèmes de connexion, consultez Résolution des problèmes de connexion à votre instance PostgreSQL (p. 1368).

8. Pour accéder à la base de données dans le navigateur pgAdmin, développez Serveurs, l'instance de base de données et Bases de données. Choisissez le nom de la base de données de l'instance de base de données.

9. Pour ouvrir un panneau dans lequel vous pouvez entrer des commandes SQL, choisissez Outils, Query Tool (Outil de requête).

Utilisation de psql pour se connecter à une instance de base de données PostgreSQL

Vous pouvez utiliser une instance locale de l'utilitaire de ligne de commande psql pour vous connecter à une instance de base de données PostgreSQL. Vous devez avoir installé PostgreSQL ou le client psql sur votre ordinateur client. Pour vous connecter à votre instance de base de données PostgreSQL avec psql, vous devez fournir les informations sur l'hôte et les informations d'identification de l'accès.

Utilisez l'un des formats suivants pour vous connecter à une instance de base de données PostgreSQL sur Amazon RDS. Lorsque vous vous connectez, vous êtes invité à entrer un mot de passe. Pour les tâches de traitement par lots ou les scripts, utilisez l'option `--no-password`.

Si vous vous connectez à cette instance de base de données pour la première fois, essayez d'utiliser le nom par défaut de la base de données postgres pour l'option `--dbname`.

Pour Unix, utilisez le format suivant.

```
psql \
   --host=<DB instance endpoint> \
   --port=<port> \
   --username=<master username> \
   --password \
   --dbname=<database name>
```

Pour Windows, utilisez le format suivant.

```
psql ^
   --host=<DB instance endpoint> ^
   --port=<port> ^
   --username=<master username> ^
   --password ^
   --dbname=<database name>
```

Par exemple, la commande suivante se connecte à une base de données appelée `mypgdb` sur une instance de base de données PostgreSQL appelée `mypostgresql` à l'aide d'informations d'identification fictives.

```
psql --host=mypostgresql.c6c8mwvfdgv0.us-west-2.rds.amazonaws.com --port=5432 --
username=awsuser --password --dbname=mypgdb
```

Résolution des problèmes de connexion à votre instance PostgreSQL

Si vous ne parvenez pas à vous connecter à l'instance de base de données, l'erreur la plus courante est `Could not connect to server: Connection timed out.` Si vous recevez cette erreur, procédez comme suit :

- Vérifiez que le nom d'hôte utilisé est le point de terminaison de l'instance de base de données et que le numéro de port utilisé est correct.
- Assurez-vous que l'accessibilité publique de l'instance de base de données est définie sur Oui.
- Vérifiez que le groupe de sécurité affecté à l'instance de base de données possède les règles pour autoriser l'accès via tout pare-feu que votre connexion peut traverser. Par exemple, si l'instance de base

de données a été créée à l'aide du port par défaut 5432, et votre entreprise peut disposer de règles de pare-feu bloquant les connexions à ce port depuis les appareils de votre entreprise.

Pour corriger le problème, modifiez l'instance de base de données afin qu'elle utilise un port différent. De plus, assurez-vous que les groupes de sécurité appliqués à l'instance de base de données autorisent les connexions au nouveau port.

- Vérifiez si l'instance de base de données a été créée grâce à un groupe de sécurité qui interdit les connexions depuis l'appareil ou l'instance Amazon EC2 où l'application s'exécute. Pour que la connexion s'établisse, le groupe de sécurité que vous avez assigné à l'instance de base de données à sa création doit autoriser l'accès à l'instance de base de données. Par exemple, si l'instance de base de données a été créée à l'intérieur d'un VPC, elle doit avoir un groupe de sécurité VPC qui autorise les connexions.

  Vous pouvez ajouter ou modifier une règle entrante dans le groupe de sécurité. La sélection de Mon IP comme Source permet d'accéder à l'instance de base de données à partir de l'adresse IP détectée dans votre navigateur. Pour de plus amples informations, veuillez consulter Créer un groupe de sécurité qui autorise l'accès à votre instance de base de données dans votre VPC (p. 66).

  Sinon, si l'instance de base de données a été créée à l'extérieur d'un VPC, elle doit avoir un groupe de sécurité de bases de données qui autorise ces connexions.

Le problème de connexion qui intervient le plus fréquemment concerne les règles d'accès du groupe de sécurité assigné à l'instance de base de données. Si vous avez utilisé le groupe de sécurité de bases de données par défaut lorsque vous avez créé l'instance de base de données, ce groupe de sécurité ne dispose vraisemblablement pas de règles d'accès vous autorisant à accéder à l'instance. Pour de plus amples informations sur les groupes de sécurité Amazon RDS, veuillez consulter Contrôle d'accès par groupe de sécurité (p. 1590).

Si vous recevez une erreur telle que `FATAL: database` *`some-name`* `does not exist` lors de la connexion, essayez d'utiliser le nom par défaut de la base de données postgres pour l'option `--dbname`.

Mise à jour des applications pour se connecter aux instances de bases de données PostgreSQL à l'aide des nouveaux certificats SSL/TLS

Le 19 septembre 2019, Amazon RDS a publié de nouveaux certificats de l'autorité de certification (CA) à connecter à vos instances de bases de données RDS à l'aide du protocole Secure Socket Layer ou Transport Layer Security (SSL/TLS). Vous trouverez ci-après des informations sur la mise à jour de vos applications afin d'utiliser les nouveaux certificats.

Cette rubrique peut vous aider à déterminer si des applications clientes utilisent un protocole SSL/TLS pour se connecter à vos instances de bases de données. Si tel est le cas, il vous est alors possible de vérifier si ces applications nécessitent une vérification du certificat pour se connecter.

> Note
>
> Certaines applications sont configurées pour se connecter aux instances de bases de données PostgreSQL uniquement si la vérification du certificat sur le serveur s'effectue avec succès. Pour ces applications, vous devez mettre à jour les magasins d'approbations des applications clientes afin d'inclure les nouveaux certificats de l'autorité de certification.

Une fois que vous avez mis à jour les certificats de l'autorité de certification dans les magasins d'approbations des applications clientes, vous pouvez soumettre les certificats de vos instances de

bases de données à une rotation. Nous vous recommandons vivement de tester ces procédures dans un environnement de développement ou intermédiaire avant de les implémenter dans vos environnements de production.

Pour de plus amples informations sur la rotation de certificats, veuillez consulter Rotation de votre certificat SSL/TLS (p. 1527). Pour en savoir plus sur le téléchargement de certificats, consultez Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525). Pour de plus amples informations sur l'utilisation des protocoles SSL/TLS avec les instances de bases de données PostgreSQL, veuillez consulter Utilisation de SSL avec une instance de base de données PostgreSQL (p. 1515).

Rubriques

- Contrôle de la connexion des applications aux instances de bases de données PostgreSQL avec le protocole SSL (p. 1370)
- Contrôle de la nécessité d'une vérification du certificat du client pour qu'il puisse se connecter (p. 1371)
- Mise à jour du magasin d'approbations de votre application (p. 1371)
- Utilisation des connexions SSL/TLS pour différents types d'application (p. 1372)

Contrôle de la connexion des applications aux instances de bases de données PostgreSQL avec le protocole SSL

Dans la configuration de l'instance de base de données, vérifiez la valeur du paramètre `rds.force_ssl`. Par défaut, le paramètre `rds.force_ssl` est défini sur `0` (désactivé). Si le paramètre `rds.force_ssl` est défini sur `1` (activé), les clients doivent utiliser le protocole SSL/TLS pour se connecter. Pour plus d'informations sur les groupes de paramètres, consultez Utilisation de groupes de paramètres de base de données (p. 225).

Si vous utilisez RDS PostgreSQL version 9.5 ou ultérieure et que `rds.force_ssl` n'est pas défini sur `1` (activé), interrogez la vue `pg_stat_ssl` afin de vérifier les connexions à l'aide du protocole SSL. Par exemple, la requête suivante retourne uniquement les connexions SSL et les informations sur les clients utilisant un protocole 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';
```

Seules les lignes utilisant des connexions SSL/TLS s'affichent avec les informations sur la connexion. Voici un exemple de sortie.

```
 datname  | username | ssl | client_addr
----------+----------+-----+-------------
 benchdb  | pgadmin | t   | 53.95.6.13
 postgres | pgadmin | t   | 53.95.6.13
(2 rows)
```

La requête n'affiche que les connexions actives au moment de la requête. L'absence de résultats n'implique pas forcément qu'aucune application n'utilise de connexions SSL. D'autres connexions SSL peuvent avoir été établies à un moment différent.

Contrôle de la nécessité d'une vérification du certificat du client pour qu'il puisse se connecter

Quand un client, tel que psql ou JDBC, est configuré avec la prise en charge du protocole SSL, le comportement par défaut est le suivant : le client essaie d'abord de se connecter à la base de données avec le protocole SSL. En cas d'impossibilité, le client revient à la connexion sans protocole SSL. Le mode `sslmode` utilisé par défaut diffère selon qu'il s'agit de clients libpq (comme psql) ou de clients JDBC. Pour les clients libpq, la valeur par défaut est `prefer`, alors qu'elle est `verify-full` pour les clients JDBC. Le certificat sur le serveur n'est vérifié que lorsque `sslrootcert` est fourni avec `sslmode` défini sur `require`, `verify-ca` ou `verify-full`. En cas de non-validité du certificat, une erreur est déclenchée.

Utilisez `PGSSLROOTCERT` pour vérifier le certificat avec la variable d'environnement `PGSSLMODE`, avec `PGSSLMODE` défini sur `require`, `verify-ca` ou `verify-full`.

```
PGSSLMODE=require PGSSLROOTCERT=/fullpath/rds-ca-2019-root.pem psql -h
 pgdbidentifier.cxxxxxxxx.us-east-2.rds.amazonaws.com -U masteruser -d postgres
```

Utilisez l'argument `sslrootcert` pour vérifier le certificat ayant `sslmode` comme format de chaîne de connexion, avec `sslmode` défini sur `require`, `verify-ca` ou `verify-full`.

```
psql "host=pgdbidentifier.cxxxxxxxx.us-east-2.rds.amazonaws.com sslmode=require
 sslrootcert=/full/path/rds-ca-2019-root.pem user=masteruser dbname=postgres"
```

Par exemple, dans le cas précédent, si vous utilisez un certificat racine non valide, une erreur similaire à celle qui suit s'affiche sur votre client.

```
psql: SSL error: certificate verify failed
```

Mise à jour du magasin d'approbations de votre application

Pour de plus amples informations sur la mise à jour du magasin d'approbations pour les applications PostgreSQL, veuillez consulter Secure TCP/IP Connections with SSL dans la documentation PostgreSQL.

> **Note**
>
> Lors de la mise à jour du magasin d'approbations, vous pouvez conserver les certificats plus anciens en complément de l'ajout des nouveaux certificats.

Mise à jour du magasin d'approbations de votre application pour JDBC

Vous pouvez mettre à jour le magasin d'approbations pour les applications qui utilisent JDBC dans le cadre de connexions SSL/TLS.

Pour mettre à jour le magasin d'approbations pour les applications JDBC

1. Téléchargez le certificat racine 2019 qui fonctionne pour toutes les régions AWS et placez le fichier dans le répertoire du magasin d'approbations.

   Pour plus d'informations sur le téléchargement du certificat racine, consultez Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).
2. Convertissez le certificat au format .der à l'aide de la commande suivante.

```
openssl x509 -outform der -in rds-ca-2019-root.pem -out rds-ca-2019-root.der
```

   Remplacez le nom du fichier par celui du fichier téléchargé.
3. Importez le certificat dans le magasin de clés à l'aide de la commande suivante.

```
keytool -import -alias rds-root -keystore clientkeystore -file rds-ca-2019-root.der
```

4. Vérifiez que le magasin de clés a été mis à jour avec succès.

```
keytool -list -v -keystore clientkeystore.jks
```

   Entrez le mot de passe du magasin de clés lorsque vous y êtes invité.

   La sortie doit contenir les lignes suivantes :

```
rds-root,date, trustedCertEntry,
Certificate fingerprint (SHA1):
 D4:0D:DB:29:E3:75:0D:FF:A6:71:C3:14:0B:BF:5F:47:8D:1C:80:96
# This fingerprint should match the output from the below command
openssl x509 -fingerprint -in rds-ca-2019-root.pem -noout
```

Utilisation des connexions SSL/TLS pour différents types d'application

Les informations suivantes se rapportent à l'utilisation de connexions SSL/TLS pour différents types d'application.

- psql

  Le client est appelé depuis la ligne de commande en spécifiant des options comme chaîne de connexion ou comme variables d'environnement. Pour les connexions SSL/TLS, les options pertinentes sont `sslmode` (variable d'environnement `PGSSLMODE`) et `sslrootcert` (variable d'environnement `PGSSLROOTCERT`).

Pour obtenir la liste complète des options, veuillez consulter Parameter Key Words dans la documentation PostgreSQL. Pour obtenir la liste complète des variables d'environnement, veuillez consulter Environment Variables dans la documentation PostgreSQL.

- pgAdmin

  Ce client basé sur un navigateur est une interface plus conviviale pour se connecter à une base de données PostgreSQL.

  Pour de plus amples informations sur la configuration des connexions, veuillez consulter la documentation pgAdmin.

- JDBC

  JDBC permet de se connecter à la base de données avec des applications Java.

  Pour obtenir des informations générales sur la connexion à une base de données PostgreSQL avec JDBC, veuillez consulter Connecting to the Database dans la documentation PostgreSQL. Pour de plus amples informations sur la connexion avec un protocole SSL/TLS, veuillez consulter Configuring the Client dans la documentation PostgreSQL.

- Python

  `psycopg2` est une bibliothèque Python bien connue pour se connecter aux bases de données PostgreSQL.

  Pour de plus amples informations sur l'utilisation de `psycopg2`, veuillez consulter la documentation psycopg2. Pour obtenir un bref didacticiel sur la connexion à une base de données PostgreSQL, veuillez consulter Psycopg2 Tutorial. Vous trouverez des informations sur les options acceptées par la commande de connexion dans The psycopg2 module content.

  > **Important**
  >
  > Une fois que vous avez déterminé que vos connexions de base de données utilisent un protocole SSL/TLS et que vous avez mis à jour le magasin d'approbations de votre application, vous pouvez mettre à jour votre base de données de sorte qu'elle utilise les certificats rds-ca-2019. Pour obtenir des instructions, veuillez consulter l'étape 3 dans Mise à jour de votre certificat CA en modifiant votre instance de base de données (p. 1528).

Mise à niveau du moteur de base de données PostgreSQL pour Amazon RDS

Lorsque Amazon RDS prend en charge une nouvelle version d'un moteur de base de données, vous pouvez mettre à niveau vos instances de base de données vers cette nouvelle version. Il existe deux types de mises à niveau pour les instances de base de données PostgreSQL : les mises à niveau de version majeure et les mises à niveau de version mineure.

Les mises à niveau de version majeure peuvent contenir des modifications de base de données qui ne sont pas rétrocompatibles avec les applications existantes. En conséquence, vous devez effectuer manuellement les mises à niveau de version majeure de vos instances de base de données. Vous pouvez lancer une mise à niveau de version majeure en modifiant votre instance de base de données. Cependant, avant d'effectuer une mise à niveau de version majeure, nous vous recommandons de suivre les étapes décrites dans Choix d'une mise à niveau de version majeure pour PostgreSQL (p. 1375). Lors d'une mise à niveau de version majeure, Amazon RDS met également à niveau tous vos réplicas en lecture dans la région ainsi que l'instance de base de données principale.

En revanche, une mise à niveau de version mineure contient uniquement des modifications rétrocompatibles avec les applications existantes. Vous pouvez lancer manuellement une mise à niveau de version mineure en modifiant votre instance de base de données. Vous pouvez également activer l'option Mise à niveau automatique des versions mineures lorsque vous créez ou modifiez une instance de base de données. Dans ce cas, votre instance de base de données est automatiquement mise à niveau une fois que Amazon RDS a testé et approuvé la nouvelle version. Si votre instance de base de données PostgreSQL utilise des réplicas en lecture, vous devez mettre à niveau tous les réplicas en lecture avant la mise à niveau de la version mineure de l'instance source. Pour en savoir plus, consultez Mises à niveau automatiques des versions mineures pour PostgreSQL (p. 1381). Pour de plus amples informations sur l'exécution manuelle d'une mise à niveau de version mineure, veuillez consulter Mise à niveau manuelle de la version du moteur (p. 268).

Rubriques

- Présentation de la mise à niveau de PostgreSQL (p. 1374)
- Numéros de version PostgreSQL (p. 1375)
- Choix d'une mise à niveau de version majeure pour PostgreSQL (p. 1375)
- Comment effectuer une mise à niveau de version majeure (p. 1377)
- Mises à niveau automatiques des versions mineures pour PostgreSQL (p. 1381)
- Mise à niveau des extensions PostgreSQL (p. 1382)

Présentation de la mise à niveau de PostgreSQL

Pour mettre à niveau vos instances de base de données en toute sécurité, Amazon RDS utilise l'utilitaire `pg_upgrade` décrit dans la documentation PostgreSQL.

Amazon RDS prend deux instantanés de base de données au cours du processus de mise à niveau si la période de rétention des sauvegardes est supérieure à 0. Le premier instantané de base de données porte sur l'instance de base de données avant que toute modification de mise à niveau soit apportée. Si la mise à niveau ne fonctionne pas pour vos bases de données, vous pouvez restaurer cet instantané pour créer une instance de base de données exécutant l'ancienne version. Le second instantané de base de données est pris à la fin de la mise à niveau.

> **Note**
>
> Amazon RDS ne prend des instantanés de base de données pendant le processus de mise à niveau que si vous avez défini la période de rétention des sauvegardes de votre instance de base de données sur un nombre supérieur à 0. Pour modifier la période de rétention des sauvegardes, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Lorsque vous mettez à niveau l'instance de base de donnée principale, tous les réplicas en lecture dans la région sont également automatiquement mis à niveau. Une fois que le flux de travail de mise à niveau a démarré, les instances de réplica attendent que `pg_upgrade` se termine correctement sur l'instance de base de données principale. Ensuite, la mise à niveau de l'instance principale attend que les mises à niveau d'instance de réplica se terminent. Vous faites face à une panne tant que la mise à niveau n'est pas terminée. Si vous avez des réplicas plus anciens provenant de versions principales antérieures, ils ne sont pas mis à niveau.

Si votre instance de base de données se trouve dans un déploiement multi-AZ, l'instance de base de données enregistreur principale et l'instance de secours sont toutes deux mises à niveau. Les instances de base de données enregistreur et de secours sont mises à niveau en même temps.

Une fois une mise à niveau terminée, vous ne pouvez pas rétablir la version précédente du moteur de base de données. Si vous souhaitez revenir à la version précédente, restaurez l'instantané de base de données pris avant la mise à niveau pour créer une nouvelle instance de base de données.

Numéros de version PostgreSQL

La séquence de numérotation des versions du moteur de base de données PostgreSQL est la suivante :

- Pour les versions 10 et ultérieures de PostgreSQL, le format du numéro de version du moteur est majeure.mineure. Le numéro de version majeure est la partie entière du numéro de version. Le numéro de version mineure est la partie fractionnaire du numéro de version.

  Une mise à niveau de version majeure augmente la partie entière du numéro de version, par exemple la mise à niveau de 10.mineure à 11.mineure.
- Pour les versions de PostgreSQL antérieures à 10, le format du numéro de version du moteur est majeure.majeure.mineure. Le numéro de version majeure du moteur est à la fois l'entier et la première partie fractionnaire du numéro de version. Par exemple, 9.6 est une version majeure. Le numéro de version mineure est la troisième partie du numéro de version. Par exemple, pour la version 9.6.12, le numéro 12 est le numéro de version mineure.

  Une mise à niveau majeure augmente la partie majeure du numéro de version. Par exemple, une mise à niveau de 9.6.12 vers 10.11 est une mise à niveau de version majeure, où 9.6 et 10 sont les numéros de version majeure.

Choix d'une mise à niveau de version majeure pour PostgreSQL

Les mises à niveau de version majeure peuvent contenir des modifications de base de données qui ne sont pas rétrocompatibles avec les versions antérieures de la base de données. Cette fonctionnalité peut empêcher le bon fonctionnement de vos applications existantes.

En conséquence, Amazon RDS n'applique pas les mise à niveau de version majeure automatiquement. Pour effectuer une mise à niveau de version majeure, modifiez votre instance de base de données manuellement. Veillez à tester soigneusement toute mise à niveau pour vérifier que vos applications fonctionnent correctement avant d'appliquer la mise à niveau à vos instances de base de données de production. Lorsque vous effectuez une mise à niveau de version majeure de PostgreSQL, nous vous recommandons de suivre les étapes décrites dans Comment effectuer une mise à niveau de version majeure (p. 1377).

Vous pouvez mettre à niveau une base de données PostgreSQL vers sa version majeure suivante. À partir de certaines versions de la base de données PostgreSQL, vous pouvez passer à une version majeure ultérieure lors de la mise à niveau. Si votre mise à niveau ignore une version majeure, les réplicas en lecture sont également mis à niveau vers cette version majeure cible. Le tableau suivant répertorie les versions source de la base de données PostgreSQL et les versions majeures cibles associées pour la mise à niveau.

> **Note**
>
> Les mises à niveau sont possibles vers une version ultérieure publiée en même temps que la version mineure source ou ultérieurement.
> Si une base de données utilise l'extension `PostGIS`, vous ne pouvez pas omettre les versions majeures pour certaines combinaisons source-cible. Dans ce cas, effectuez la mise à niveau étape par étape pour passer à la version majeure suivante jusqu'à ce que vous atteigniez la version cible voulue.
> L'extension `pgRouting` n'est pas prise en charge pour une mise à niveau qui fait omet une version majeure et passe directement aux versions 11.x. Une version majeure est omise lorsque la mise à niveau passe des versions 9.4.x, 9.5.x ou 9.6.x aux versions 11.x. Vous pouvez supprimer l'extension `pgRouting` puis l'ajouter à nouveau une fois la mise à niveau exécutée.

Les extensions `tsearch2` et `chkpass` ne sont pas prises en charge dans PostgreSQL 11 ou version ultérieure. Si vous effectuez une mise à niveau vers la version 11.x, supprimez ces extensions avant la mise à niveau.

Version source actuelle	Cibles de mise à niveau préférées	Cible de mise à niveau la plus récente
9.4.7	9.5.20, 9.6.11	9.6.11
9.4.9, 9.4.11, 9.4.12, 9.4.14, 9.4.15, 9.4.17, 9.4.18, 9.4.19	9.5.20	9.5.22
9.4.20	9.5.20, 11.1	11.1
9.4.21	9.5.20, 10.7, 11.2	11.2
9.4.23	9.5.20, 10.9, 11.4	11.4
9.4.24	9.5.20, 10.10, 11.5	11.5
9.5.2, 9.5.4, 9.5.6, 9.5.7, 9.5.9, 9.5.10, 9.5.12, 9.5.13, 9.5.14	9.6.18	9.6.19
9.5.15	9.6.18	11.2
9.5.16	9.6.18	11.2
9.5.18	9.6.18	11.4
9.5.19	9.6.18	11.5
9.5.21	9.6.18	12.2
9.5.22	9.6.18, 10.13, 11.8, 12.3	12.3
9.5.23	9.6.19, 10.14, 11.9, 12.4	12.4
9.6.1, 9.6.2, 9.6.3, 9.6.5, 9.6.6, 9.6.8, 9.6.9, 9.6.10	10.13	10.14
9.6.11	10.11, 11.1	11.1
9.6.12	10.13, 11.2	11.2
9.6.14	10.13, 11.4	11.4
9.6.15	10.13, 11.5	11.5
9.6.16	10.13, 11.6	11.6
9.6.17	10.13, 11.7, 12.2	12.2
9.6.18	10.13, 11.8, 12.3	12.3
9.6.19	10.14, 11.9, 12.4	12.4
10.1, 10.3, 10.4, 10.5, 10.6, 10.7, 10.9, 10.10, 10.11	11.8	11.9
10.12	11.8, 12.2	12.2
10.13	11.8, 12.3	12.3

Version source actuelle	Cibles de mise à niveau préférées	Cible de mise à niveau la plus récente
10.14	11.9, 12.4	12.4
11.1, 11.2, 11.4, 11.5, 11.6, 11.7	12.3	12.4
11.8	12.3	12.4
11.9	12.4	12.4

Pour obtenir une liste de toutes les cibles de mise à niveau valides pour une version source actuelle, utilisez la commande d'interface de ligne de commande `describe-db-engine-versions`. Exemples :

```
export REGION=AWS-Region
export ENDPOINT=https://rds.AWS-Region.amazonaws.com

aws rds describe-db-engine-versions --engine postgres --region $REGION --endpoint
 $ENDPOINT --output text --query '*[].ValidUpgradeTarget[?IsMajorVersionUpgrade==`true`].
{EngineVersion:EngineVersion}' --engine-version DB-current-version
```

Comment effectuer une mise à niveau de version majeure

Nous vous recommandons de suivre le processus ci-dessous lors de la mise à niveau d'une instance de base de données PostgreSQL Amazon RDS :

1. Préparez un groupe de paramètres compatible avec la version – Si vous utilisez un groupe de paramètres personnalisé, vous avez deux options. Vous pouvez spécifier un groupe de paramètres par défaut pour la nouvelle version du moteur de base de données. Ou vous pouvez créer votre propre groupe de paramètres personnalisé pour la nouvelle version du moteur de base de données

   Si vous associez un nouveau groupe de paramètres à une instance de base de données, redémarrez la base de données à la fin de la mise à niveau. Si l'instance doit être redémarrée pour appliquer les modifications du groupe de paramètres, le statut du groupe de paramètres de l'instance indique `pending-reboot`. Vous pouvez afficher le statut du groupe de paramètres d'une instance dans la console ou en utilisant une commande describe, comme .`describe-db-instances`.
2. Vérifiez les classes d'instance de base de données non prises en charge – Vérifiez que la classe d'instance de votre base de données est compatible avec la version PostgreSQL vers laquelle vous effectuez la mise à niveau. Pour de plus amples informations, veuillez consulter Moteurs de base de données pris en charge pour les classes d'instance de base de données (p. 7).
3. Recherchez une utilisation non prise en charge :
   - Transactions préparées – Validez ou restaurez toutes les transactions préparées ouvertes avant d'essayer d'effectuer une mise à niveau.

     Vous pouvez utiliser la requête suivante pour vérifier qu'aucune transaction préparée ouverte ne figure sur votre instance.

     ```
     SELECT count(*) FROM pg_catalog.pg_prepared_xacts;
     ```
   - Types de données Reg* – Supprimez toutes les utilisations des types de données reg* avant d'essayer d'effectuer une mise à niveau. À l'exception de `regtype` et `regclass`, vous ne pouvez pas mettre à niveau les types de données reg*. L'utilitaire pg_upgrade ne peut pas conserver ce type de données, qui est utilisé par Amazon RDS pour effectuer la mise à niveau.

Pour vérifier l'absence de toute utilisation des types de données reg* non pris en charge, utilisez la requête suivante pour chaque base de données.

```
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. Gérer les réplicas en lecture – Une mise à niveau met également à niveau les réplicas en lecture dans la région ainsi que l'instance principale.

   Vous ne pouvez pas mettre à niveau les réplicas en lecture séparément. Si vous le pouviez, cela pourrait générer des situations où les instances principales et les réplicas auraient des versions majeures différentes de PostgreSQL. Toutefois, les mises à niveau de réplica peuvent augmenter les temps d'arrêt sur l'instance principale. Pour éviter la mise à niveau d'un réplica, promouvez le réplica en instance autonome ou supprimez-le avant de démarrer le processus de mise à niveau.

   Le processus de mise à niveau recrée le groupe de paramètres du réplica en fonction du groupe de paramètres actuel de l'instance de réplica. Vous pouvez appliquer un groupe de paramètres personnalisé à un réplica uniquement une fois la mise à niveau terminée à l'aide de la commande CLI `modify-db-parameter-group`.

   Les réplicas en lecture sur la plateforme de cloud privé virtuel (VPC) sont mis à niveau, mais les réplicas sur la plateforme EC2-Classic ne sont pas mis à niveau. Tous les réplicas EC2-Classic gardent l'état de réplication résiliée une fois le processus de mise à niveau terminé. Pour déplacer une instance de base de données de la plateforme EC2-Classic vers un VPC, veuillez consulter Déplacement vers un VPC d'une instance de base de données n'appartenant pas à un VPC (p. 1627). Pour de plus amples informations, veuillez consulter Utilisation de réplicas en lecture PostgreSQL dans Amazon RDS (p. 1384).

5. Effectuez une sauvegarde – Nous vous recommandons d'effectuer une sauvegarde avant d'effectuer la mise à niveau de version majeure, afin de disposer d'un point de restauration connu pour votre base de données. Si la période de rétention des sauvegardes est supérieure à 0, le processus de mise à niveau crée des instantanés de base de données de votre instance de base de données avant et après la mise à niveau. Pour modifier la période de rétention des sauvegardes, consultez Modification d'une instance de base de données Amazon RDS (p. 243). Pour effectuer une sauvegarde manuellement, consultez Création d'un instantané de base de données (p. 327).

6. Mise à niveau de certaines extensions avant une mise à niveau de version majeure – Si vous envisagez d'omettre une version majeure avec la mise à niveau, vous devez mettre à jour certaines extensions avant d'effectuer la mise à niveau de version majeure. La mise à niveau des versions 9.4.x, 9.5.x ou 9.6.x vers les versions 11.x entraîne une omission de la version majeure. Les extensions à mettre à jour incluent :

   - `address_standardizer`
   - `address_standardizer_data_us`
   - `postGIS`
   - `postgis_tiger_geocoder`
   - `postgis_topology`

Exécutez la commande suivante pour chaque extension que vous utilisez.

```
ALTER EXTENSION PostgreSQL-extension UPDATE TO 'new-version'
```

Pour plus d'informations, consultez Mise à niveau des extensions PostgreSQL (p. 1382).

7. Supprimez certaines extensions avant une mise à niveau de version majeure – Une mise à niveau qui omet une version majeure pour passer directement à la version 11.x ne prend pas en charge la mise à jour de l'extension `pgRouting`. La mise à niveau des versions 9.4.x, 9.5.x ou 9.6.x vers les versions 11.x entraîne une omission de la version majeure. Il est plus sûr de supprimer l'extension `pgRouting` puis de la réinstaller sur une version compatible une fois la mise à niveau effectuée. Pour connaître les versions d'extension vers lesquelles vous pouvez effectuer une mise à jour, veuillez consulter Extensions et modules PostgreSQL pris en charge sur Amazon RDS (p. 1488).

   Les extensions `tsearch2` et `chkpass` ne sont plus prises en charge pour PostgreSQL versions 11 ou ultérieures. Si vous effectuez une mise à niveau vers la version 11.x, supprimez les extensions `tsearch2` et `chkpass` avant la mise à niveau.

8. Supprimer les types de données inconnus – Supprimez les types de données `unknown` en fonction de la version cible.

   PostgreSQL version 10 a cessé de prendre en charge le type de données `unknown`. Si une base de données version 9.6 utilise le type de données `unknown`, une mise à niveau vers une version 10 affiche un message d'erreur tel que :

```
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."
```

   Pour rechercher le type de données `unknown` dans votre base de données afin de pouvoir supprimer la colonne incriminée ou la remplacer par un type de données pris en charge, utilisez le code SQL suivant :

```
SELECT DISTINCT data_type FROM information_schema.columns WHERE data_type ILIKE
 'unknown';
```

9. Réalisez un essai de mise à niveau – Nous vous recommandons fortement de tester la mise à niveau de version majeure sur un doublon de votre base de données de production avant d'essayer d'effectuer la mise à niveau sur votre base de données de production. Pour créer un doublon d'instance de test, vous pouvez restaurer votre base de données à partir d'un instantané récent ou réaliser une restauration de votre base de données à sa date de restauration possible la plus récente. Pour de plus amples informations, veuillez consulter Restaurer à partir d'un instantané (p. 331) ou Restauration d'une instance de base de données à une date spécifiée (p. 365). Pour en savoir plus sur la procédure de mise à niveau, consultez Mise à niveau manuelle de la version du moteur (p. 268).

   Durant la mise à niveau de version majeure, les bases de données `public` et `template1`, ainsi que le schéma `public` figurant dans chaque base de données de l'instance, sont renommés temporairement. Ces objets apparaissent dans les journaux avec leur nom d'origine et une chaîne aléatoire ajoutée. Cette chaîne est ajoutée afin que les paramètres personnalisés tels que `locale` et `owner` soient conservés au cours de la mise à niveau de version majeure. À la fin de la mise à niveau, les objets reprennent leurs noms d'origine.

   > **Note**
   >
   > Au cours du processus de mise à niveau de version majeure, vous ne pouvez pas effectuer de restauration à un moment donné de votre instance. Après avoir effectué la mise à niveau, Amazon RDS réalise une sauvegarde automatique de l'instance. Vous pouvez effectuer une

restauration à un moment donné pour revenir à un moment antérieur au début de la mise à niveau et postérieur à la sauvegarde automatique de votre instance.

10. Résolvez les problèmes si une mise à niveau échoue avec des erreurs de procédure de pré-vérification – Au cours du processus de mise à niveau de version majeure, Amazon RDS pour PostgreSQL exécute d'abord une procédure de pré-vérification pour identifier les éventuels problèmes pouvant provoquer un échec de la mise à niveau. Le procédure de pré-vérification recherche les éventuelles conditions d'incompatibilité entre toutes les bases de données de l'instance.

    Si la pré-vérification détecte un problème, elle crée un événement de journal indiquant l'échec de la pré-vérification de mise à niveau. Les détails de la procédure de pré-vérification se trouvent dans un journal de mise à niveau nommé `pg_upgrade_precheck.log` pour toutes les bases de données d'une instance de base de données. Amazon RDS ajoute un horodatage au nom du fichier. Pour de plus amples informations sur l'affichage des journaux, veuillez consulter Amazon RDS Fichiers journaux de base de données (p. 490).

    Si la mise à niveau d'un réplica échoue au stade de la vérification préalable, la réplication sur le réplica défaillant est interrompue et le réplica est mis à l'état résilié. Supprimez le réplica et recréez un nouveau réplica basé sur l'instance principale mise à niveau.

    Résolvez tous les problèmes identifiés dans le journal de pré-vérification puis relancez la mise à niveau de version majeure. Voici un exemple de journal de pré-vérification.

```
-----------------------------------------------------------------------
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 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.
```

11. Si une mise à niveau de réplica échoue lors de la mise à niveau de la base de données, résolvez le problème – Un réplica en échec est placé à l'état `incompatible-restore` et la réplication est résiliée sur l'instance de base de données. Supprimez le réplica et recréez un nouveau réplica basé sur l'instance principale mise à niveau.

    Une mise à niveau de réplica peut échouer pour les raisons suivantes :

    - Elle n'a pas pu s'aligner sur l'instance principale même après un temps d'attente.
    - Elle était dans un état de mise hors service ou de cycle de vie incompatible, tel que storage-full, incompatible-restore, etc.
    - Lorsque la mise à niveau de l'instance principale a démarré, une mise à niveau de version mineure distincte était en cours d'exécution sur le réplica.
    - L'instance de réplica utilisait des paramètres incompatibles.
    - L'instance de réplica n'a pas pu communiquer avec l'instance principale pour synchroniser le dossier de données.

12. Mettez à niveau votre instance de production – Si l'essai de mise à niveau de version majeure est un succès, vous devez être en mesure de mettre à niveau en toute confiance votre base de données de production. Pour de plus amples informations, veuillez consulter Mise à niveau manuelle de la version du moteur (p. 268).

Une fois la mise à niveau de version majeure effectuée, nous vous recommandons d'effectuer les tâches suivantes :

- Exécutez l'opération `ANALYZE` pour actualiser la table `pg_statistic`.
- Une mise à niveau de PostgreSQL ne met à niveau aucune extension PostgreSQL. Pour mettre à niveau les extensions, veuillez consulter Mise à niveau des extensions PostgreSQL (p. 1382).
- Vous pouvez utiliser Amazon RDS pour afficher deux journaux produits par l'utilitaire pg_upgrade. Il s'agit des journaux `pg_upgrade_internal.log` et `pg_upgrade_server.log`. Amazon RDS ajoute un horodatage au nom de fichier de ces journaux. Vous pouvez consultez ces journaux comme tout autre journal. Pour plus d'informations, consultez Amazon RDS Fichiers journaux de base de données (p. 490).

  Vous pouvez également charger les journaux de mise à niveau dans Amazon CloudWatch Logs. Pour de plus amples informations, veuillez consulter Publication de journaux PostgreSQL dans CloudWatch Logs (p. 523).
- Pour vérifier si tout fonctionne comme prévu, testez votre application sur la base de données mise à niveau avec une charge de travail similaire. Une fois la mise à niveau vérifiée, vous pouvez supprimer l'instance de test.

Mises à niveau automatiques des versions mineures pour PostgreSQL

Si vous activez l'option Mise à niveau automatique des versions mineures au moment de créer ou modifier une instance de base de données, votre instance de base de données peut être mise à niveau automatiquement.

Pour chaque version majeure de RDS for PostgreSQL, une seule version mineure est désignée par RDS comme étant la version de mise à niveau automatique. Une fois qu'une version mineure a été testée et approuvée par Amazon RDS, la mise à niveau de la version mineure se produit automatiquement pendant votre fenêtre de maintenance. RDS ne définit pas automatiquement les dernières versions mineures publiées comme version de mise à niveau automatique. Avant de désigner une publication de version récente comme version de mise à niveau automatique, RDS prend en compte plusieurs critères, à savoir :

- Problèmes de sécurité connus
- Bogues dans la version de la communauté PostgreSQL
- Stabilité globale du parc depuis la publication de la version mineure

Vous pouvez utiliser le script et la commande AWS CLI ci-dessous pour déterminer quelles sont les versions mineures de mise à jour automatique actuelles.

```
aws rds describe-db-engine-versions --engine postgres | grep -A 1 AutoUpgrade| grep -A 2
 true |grep PostgreSQL | sort --unique | sed -e 's/"Description": "//g'
```

> **Note**
>
> Si aucun résultat n'est renvoyé, aucune mise à niveau automatique de version mineure n'est disponible et planifiée.

Une instance de base de données PostgreSQL est automatiquement mise à niveau pendant votre fenêtre de maintenance si les critères suivants sont réunis :

- L'option Mise à niveau automatique des versions mineures est activée pour l'instance de base de données.
- L'instance de base de données exécute une version mineure du moteur de base de données qui est inférieure à la version mineure de la mise à niveau automatique actuelle.

Pour plus d'informations, consultez Mise à niveau automatique de la version mineure du moteur (p. 269).

> **Note**
>
> Une mise à niveau de PostgreSQL ne met pas à niveau les extensions PostgreSQL. Pour mettre à niveau les extensions, veuillez consulter Mise à niveau des extensions PostgreSQL (p. 1382).

Mise à niveau des extensions PostgreSQL

Une mise à niveau du moteur PostgreSQL ne met pas à niveau la plupart des extensions PostgreSQL. Pour mettre à jour une extension après une mise à niveau de version, utilisez la commande `ALTER EXTENSION UPDATE`.

> **Note**
>
> Si vous exécutez l'extension `PostGIS` dans votre instance de base de données Amazon RDS PostgreSQL, veillez à respecter les instructions de mise à niveau PostGIS fournies dans la documentation PostGIS avant d'effectuer la mise à niveau de l'extension.

Pour mettre à niveau une extension, utilisez la commande suivante.

```
ALTER EXTENSION extension_name UPDATE TO 'new_version'
```

Pour voir la liste des versions prises en charge des extensions PostgreSQL, consultez Extensions et modules PostgreSQL pris en charge sur Amazon RDS (p. 1488).

Pour afficher une liste des extensions actuellement installées, utilisez le catalogue pg_extension PostgreSQL dans la commande suivante.

```
SELECT * FROM pg_extension;
```

Pour afficher une liste des versions d'extensions spécifiques disponibles pour votre installation, utilisez la vue pg_available_extension_versions PostgreSQL dans la commande suivante.

```
SELECT * FROM pg_available_extension_versions;
```

Mise à niveau d'un instantané de base de données PostgreSQL

Amazon RDS vous permet de créer un instantané de base de données de volume de stockage de votre instance de base de données PostgreSQL. Lorsque vous créez un instantané de base de données, l'instantané est basé sur la version du moteur utilisée par votre instance Amazon RDS. Outre la mise à niveau de la version du moteur DB de votre instance de base de données, vous pouvez également mettre à niveau la version du moteur de vos instantanés DB.

Après avoir restauré un instantané de base de données mis à niveau vers une nouvelle version de moteur, veillez à vérifier que la mise à jour est réussie. Pour de plus amples informations sur une mise à niveau des versions majeures, veuillez consulter Mise à niveau du moteur de base de données PostgreSQL pour Amazon RDS (p. 1373). Pour savoir comment restaurer un instantané de base de données, consultez Restauration à partir d'un instantané de base de données (p. 329).

Vous pouvez mettre à niveau des instantanés de base de données manuels chiffrés ou non chiffrés.

Pour obtenir la liste des versions de moteur disponibles pour la mise à niveau d'un instantané de base de données, veuillez consulter Mise à niveau du moteur de base de données PostgreSQL pour Amazon RDS.

> Note
>
> - L'instantané de base de données doit provenir de la même région AWS que le compte.
> - Vous ne pouvez pas mettre à niveau d'instantanés de base de données copiés dans la région, copiés entre régions ou partagés entre comptes.
> - Vous ne pouvez pas mettre à niveau des instantanés DB automatisés qui sont créés lors du processus de sauvegarde automatique.

Console

Pour mettre à niveau un instantané de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Snapshots.
3. Choisissez l'instantané que vous souhaitez mettre à niveau.
4. Pour Actions, choisissez Upgrade Snapshot (Mettre à niveau l'instantané). La page Upgrade Snapshot (Mettre à niveau l'instantané) s'affiche.
5. Choisissez la New engine version (Version du nouveau moteur) vers laquelle mettre à niveau.
6. Choisissez Save changes (Enregistrer les changements) pour mettre à niveau l'instantané.

   Pendant le processus de mise à niveau, toutes les actions d'instantané sont désactivées pour l'instantané de base de données. De même, le statut de l'instantané de base de données passe de disponible à upgrading (mise à niveau), puis passe à active, une fois la mise à niveau terminée. Si l'instantané de base de données ne peut pas être mis à jour en raison d'un problème d'instantané endommagé, le statut devient indisponible. Vous ne pouvez pas récupérer l'instantané lorsqu'il a ce statut.

   > Note
   >
   > Si la mise à niveau de l'instantané de base de données échoue, l'instantané revient à l'état d'origine avec la version originale.

AWS CLI

Pour mettre à niveau un instantané de base de données vers une nouvelle version du moteur de base de données, utilisez la commande modify-db-snapshot de l'AWS CLI.

Paramètres

- `--db-snapshot-identifier` – L'identifiant de l'instantané de base de données à mettre à niveau. L'identifiant doit être unique pour un Amazon Resource Name (ARN). Pour plus d'informations, consultez Utilisation des Amazon Resource Names (ARN) dans Amazon RDS (p. 298).
- `--engine-version` – La version du moteur vers laquelle la mise à niveau de l'instantané de base de données doit être effectuée.

Example

Pour Linux, macOS ou Unix :

```
aws rds modify-db-snapshot \
    --db-snapshot-identifier my_db_snapshot \
    --engine-version new_version
```

Pour Windows :

```
aws rds modify-db-snapshot ^
    --db-snapshot-identifier my_db_snapshot ^
    --engine-version new_version
```

API RDS

Pour mettre à niveau un instantané de base de données vers une nouvelle version du moteur de base de données, appelez l'opération ModifyDBSnapshot de l'API Amazon RDS.

- `DBSnapshotIdentifier` – L'identifiant de l'instantané de base de données à mettre à niveau. L'identifiant doit être unique pour un Amazon Resource Name (ARN). Pour plus d'informations, consultez Utilisation des Amazon Resource Names (ARN) dans Amazon RDS (p. 298).
- `EngineVersion` – La version du moteur vers laquelle la mise à niveau de l'instantané de base de données doit être effectuée.

Example

```
https://rds.us-west-2.amazonaws.com/
   ?Action=ModifyDBSnapshot
   &DBSnapshotIdentifier=mydbsnapshot
   &EngineVersion=newversion
   &SignatureVersion=4
   &Version=2014-10-31
   &X-Amz-Algorithm=AWS4-HMAC-SHA256
   &X-Amz-Credential=AKIADQKE4SARGYLE/20161222/us-west-1/rds/aws4_request
   &X-Amz-Date=20161222T233051Z
   &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
   &X-Amz-Signature=8052a76dfb18469393c5f0182cdab0ebc224a9c7c5c949155376c1c250fc7ec3
```

Utilisation de réplicas en lecture PostgreSQL dans Amazon RDS

Vous utilisez généralement des réplicas en lecture pour configurer la réplication entre instances de base de données Amazon RDS. Pour obtenir des informations générales sur les réplicas en lecture, veuillez consulter Utilisation des réplicas en lecture (p. 275).

Cette section contient des informations spécifiques sur l'utilisation des réplicas en lecture dans PostgreSQL.

Rubriques

- Configuration de réplicas en lecture avec PostgreSQL (p. 1385)
- Surveillance des réplicas en lecture PostgreSQL (p. 1386)

- Limites des réplicas en lecture avec PostgreSQL (p. 1386)
- Interruption de réplication avec les réplicas en lecture PostgreSQL (p. 1386)
- Dépannage d'un problème de réplica en lecture PostgreSQL (p. 1387)

Configuration de réplicas en lecture avec PostgreSQL

Amazon RDS PostgreSQL utilise la réplication de streaming native de PostgreSQL pour créer une copie en lecture seule d'une instance de bases de données source. Cette instance de base de données de réplica en lecture (« instance de secours » dans le jargon de PostgreSQL) est une réplication physique créée de façon asynchrone de l'instance de base de données source. Elle est créée par une connexion spéciale qui transmet les données WAL (write-ahead log) entre l'instance de base de données source et le réplica en lecture, avec PostgreSQL qui diffuse en continu de façon asynchrone les modifications de base de données au fur et à mesure qu'elles sont apportées.

PostgreSQL utilise un rôle de « réplication » pour effectuer la réplication de streaming. Ce rôle dispose de privilèges, mais ne peut pas être utilisé pour modifier des données. PostgreSQL utilise un processus unique pour traiter la réplication.

Avant qu'une instance de bases de données puisse servir d'instance de bases de données source, vous devez activer les sauvegardes automatiques sur l'instance de bases de données source en affectant à la période de rétention des sauvegardes une valeur différente de 0.

La création d'un réplica en lecture PostgreSQL ne nécessite pas de coupure pour l'instance de base de données source. Amazon RDS définit les paramètres et les autorisations nécessaires pour l'instance de base de données source et le réplica en lecture sans aucune interruption de service. Un instantané de l'instance de base de données source est pris, et devient le réplica en lecture. Aucune interruption de service ne se produit lorsque vous supprimez un réplica en lecture.

Vous pouvez créer jusqu'à cinq réplicas en lecture à partir d'une seule instance de base de données source. Pour que la réplication fonctionne de façon efficace, chaque réplica en lecture doit avoir la même quantité de ressources de calcul et de stockage que l'instance de base de données source. Si vous mettez à l'échelle l'instance de base de données source, faites-le également pour les réplicas en lecture.

Amazon RDS remplace tout paramètre incompatible sur un réplica en lecture s'il empêche ce dernier de démarrer. Par exemple, supposons que la valeur du paramètre `max_connections` est supérieure dans l'instance de base de données source à celle du réplica en lecture. Dans ce cas, Amazon RDS met à jour le paramètre dans le réplica en lecture sur la même valeur que celle de l'instance de base de données source.

Les instances de base de données PostgreSQL utilisent une connexion sécurisée que vous pouvez chiffrer en définissant le paramètre `ssl` sur `1` pour les instances de la source et du réplica en lecture.

Vous pouvez créer un réplica en lecture à partir de déploiements d'instance de base de données mono-AZ ou multi-AZ. Vous utilisez des déploiements multi-AZ pour améliorer la durabilité et la disponibilité des données critiques, mais vous ne pouvez pas utiliser une instance secondaire multi-AZ pour servir les requêtes en lecture seule. À la place, vous pouvez créer des réplicas en lecture à partir d'instances de base de données multi-AZ à trafic élevé pour décharger les requêtes en lecture seule. Si l'instance source d'un déploiement multi-AZ bascule vers l'instance secondaire, tous les réplicas en lecture associés se mettent automatiquement à utiliser l'instance secondaire (désormais principale) comme source de réplication. Pour plus d'informations, consultez Haute disponibilité (multi-AZ) pour Amazon RDS (p. 43).

Vous pouvez désormais créer un réplica en lecture en tant qu'instance de base de données multi-AZ. Amazon RDS crée une instance de secours de votre réplica dans une autre zone de disponibilité pour la prise en charge du basculement pour le réplica. La création de votre réplica en lecture en tant qu'instance de base de données multi-AZ est indépendante du fait que la base de données source soit ou non une instance de base de données multi-AZ.

Si vous utilisez l'extension postgres_fdw pour accéder aux données à partir d'un serveur distant, le réplica en lecture aura également accès au serveur distant. Pour plus d'informations sur l'utilisation de `postgres_fdw`, consultez Accès aux données externes à l'aide de l'extension postgres_fdw (p. 1447).

Surveillance des réplicas en lecture PostgreSQL

Pour les réplicas en lecture PostgreSQL, vous pouvez surveiller le délai de réplication dans Amazon CloudWatch en observant la métrique Amazon RDS `ReplicaLag`. La métrique `ReplicaLag` contient la valeur de `SELECT extract(epoch from now() - pg_last_xact_replay_timestamp()) AS replica_lag`.

Limites des réplicas en lecture avec PostgreSQL

Les limites des réplicas en lecture pour PostgreSQL sont les suivantes :

- Chaque réplica en lecture PostgreSQL est accessible en lecture seule et il est impossible de le rendre accessible en écriture.
- Vous ne pouvez pas créer un réplica en lecture à partir d'un autre réplica en lecture (en d'autres termes, vous ne pouvez pas créer de réplicas en lecture en cascade).
- Vous pouvez promouvoir un réplica en lecture PostgreSQL comme nouvelle instance de base de données source. Néanmoins, le réplica en lecture ne devient pas automatiquement la nouvelle instance de base de données source. Le réplica en lecture, lorsqu'il est promu, arrête de recevoir les communications WAL et cesse d'être une instance en lecture seule. Vous devez configurer toute réplication que vous souhaitez voir continuer, car le réplica en lecture promu est, à présent, une nouvelle instance de base de données source.
- Un réplica en lecture PostgreSQL consigne un délai de réplication pouvant atteindre cinq minutes si aucune transaction utilisateur ne se produit sur l'instance de base de données source.

Interruption de réplication avec les réplicas en lecture PostgreSQL

Dans plusieurs situations, une instance de base de données source PostgreSQL peut interrompre involontairement la réplication avec un réplica en lecture. Ces situations incluent les suivantes :

- Le paramètre `max_wal_senders` a une valeur trop basse pour fournir suffisamment de données aux différents réplicas en lecture. Cette situation entraîne l'arrêt de la réplication.
- Le paramètre PostgreSQL `wal_keep_segments` indique le nombre de fichiers WAL à conserver pour fournir les données aux réplicas en lecture. La valeur de ce paramètre spécifie le nombre de journaux à conserver. Si vous affectez à ce paramètre une valeur trop basse, vous pouvez entraîner un tel retard du réplica en lecture que la réplication de streaming s'arrête. Dans ce cas, Amazon RDS signale une erreur de réplication et commence la récupération des données sur le réplica en lecture en relisant les journaux WAL archivés de l'instance de base de données source. Ce processus de récupération se poursuit jusqu'à ce que le réplica en lecture ait rattrapé suffisamment de retard pour continuer la réplication de streaming. Pour plus d'informations, consultez Dépannage d'un problème de réplica en lecture PostgreSQL (p. 1387).
- Un réplica en lecture PostgreSQL doit être redémarré en cas de changement de l'adresse IP du point de terminaison de l'instance de base de données source.

Lorsque le flux WAL qui fournit les données à un réplica en lecture est interrompu, PostgreSQL bascule en mode de récupération pour restaurer le réplica en lecture à l'aide des fichiers WAL archivés. Quand ce processus terminé, PostgreSQL tente de rétablir la réplication de streaming.

Dépannage d'un problème de réplica en lecture PostgreSQL

Étant donné que PostgreSQL utilise des emplacements de réplication pour la réplication entre régions, le processus de résolution des problèmes de réplication diffère selon qu'il s'agit d'une même région ou de régions différentes.

Dépannage des problèmes de réplica en lecture PostgreSQL au sein d'une même région AWS

Le paramètre PostgreSQL `wal_keep_segments` indique le nombre de fichiers WAL (Write Ahead Log) à conserver pour fournir les données aux réplicas en lecture. La valeur de ce paramètre spécifie le nombre de journaux à conserver. Si vous affectez à ce paramètre une valeur trop basse, vous pouvez entraîner un tel retard du réplica en lecture que la réplication de streaming s'arrête. Dans ce cas, Amazon RDS signale une erreur de réplication et commence la récupération des données sur le réplica en lecture en relisant les journaux WAL archivés de l'instance de base de données source. Ce processus de récupération se poursuit jusqu'à ce que le réplica en lecture ait rattrapé suffisamment de retard pour continuer la réplication de streaming.

Le journal PostgreSQL sur le réplica en lecture indique le moment où Amazon RDS récupère un réplica en lecture présentant cet état en relisant les fichiers WAL archivés.

```
 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
```

Après un certain délai, le nombre de fichiers WAL archivés relus par Amazon RDS sur le réplica est suffisant pour rattraper le retard et permettre au réplica en lecture de recommencer le streaming. PostgreSQL reprend alors le streaming et écrit une ligne similaire à la suivante dans le fichier journal.

```
 2014-11-07 19:41:36 UTC::@:[24714]:LOG:  started streaming WAL from primary at 1B/
B6000000
     on timeline 1
```

Vous pouvez déterminer le nombre de fichiers WAL que vous devez conserver en examinant les informations de point de contrôle dans le journal. Le journal PostgreSQL indique les informations suivantes à chaque point de contrôle. En examinant les fichiers journaux des transactions « # recycled » de ces instructions de journalisation, vous pouvez comprendre combien de fichiers de transaction seront recyclées au cours d'une période et peut utiliser ces informations pour ajuster le paramètre `wal_keep_segments`.

```
 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
```

Par exemple, supposons que le journal PostgreSQL montre que 35 fichiers sont recyclés à partir des déclarations de journaux « vérification terminée » dans un délai de 5 minutes. Dans ce cas, nous savons qu'avec ce motif d'utilisation un réplica en lecture s'appuie sur 35 fichiers de transactions en cinq minutes. Un réplica en lecture ne peut pas survivre cinq minutes dans un état de non-streaming si l'instance de base de données source est définie sur la valeur du paramètre `wal_keep_segments` par défaut de 32.

Dépannage des problèmes de réplica en lecture PostgreSQL entre plusieurs régions AWS

PostgreSQL version 9.5.2 utilise des emplacements de réplication physiques pour gérer la rétention WAL (Write Ahead Log) sur l'instance de base de données source. Pour chaque instance de réplica en lecture entre régions, Amazon RDS crée et associe un emplacement physique de réplication. Vous pouvez utiliser deux métriques Amazon CloudWatch, `Oldest Replication Slot Lag` et `Transaction Logs Disk Usage`, pour connaître le retard du dernier réplica en termes de données WAL reçues et le volume de stockage utilisé pour les données WAL. La valeur `Transaction Logs Disk Usage` peut considérablement augmenter lorsqu'un réplica en lecture entre régions présente un retard important.

Si la charge de travail sur votre instance de base de données génère une grande quantité de données WAL, vous devrez peut-être modifier la classe de votre instance de base de données source et de votre instance de base de données de réplica en lecture. Dans ce cas, vous la modifiez en une classe présentant des performances réseau élevées (10 Go/s) pour que le réplica s'adapte. La métrique Amazon CloudWatch `Transaction Logs Generation` peut vous aider à comprendre le débit auquel les données WAL sont générées par votre charge de travail.

Pour déterminer le statut d'un réplica en lecture entre régions, vous pouvez exécuter la requête `pg_replication_slots` sur l'instance source, comme dans l'exemple suivant :

```
postgres=# select * from pg_replication_slots;

                  slot_name                  | plugin | slot_type | datoid | database |
 active | active_pid | xmin | catalog_xmin | restart_lsn
-------------------------------------------------------------------------------------------
 rds_us_east_1_db_uzwlholddgpblksce6hgw4nkte |        | physical  |        |          | t
    |      12598 |      |              | 4E/95000060
(1 row)
```

Importation de données dans PostgreSQL sur Amazon RDS

Supposons que vous disposez d'un déploiement PostgreSQL existant que vous souhaitez transférer dans Amazon RDS. La complexité de votre tâche dépend de la taille de votre base de données et des types d'objets de base de données que vous transférez. Prenons l'exemple d'une base de données qui contient des jeux de données se mesurant en gigaoctets, ainsi que des déclencheurs et des procédures stockés. Une telle base de données va être plus compliquée qu'une base de données simple avec seulement quelques mégaoctets de données de test et pas de déclencheurs, ni de procédures stockés.

Nous vous recommandons d'utiliser les outils de migration de base de données PostgreSQL natifs dans les conditions suivantes :

- Vous avez une migration homogène, dans le sens où vous migrez depuis une base de données avec le même moteur de base de données que la base de données cible.
- Vous migrez une base de données entière.

- Les outils natifs vous permettent de migrer votre système avec une interruption minimale.

Dans la plupart des autres cas, l'exécution d'une migration de base de données à l'aide de AWS Database Migration Service (AWS DMS) est la meilleure approche. AWS DMS peut migrer les bases de données sans interruption et, pour de nombreux moteurs de bases de données, poursuivre la réplication en cours jusqu'à ce que vous soyez prêt à basculer sur la base de données cible. Vous pouvez migrer vers le même moteur de base de données ou vers un moteur de base de données différent avec AWS DMS. Si vous migrez vers un moteur de base de données différent de votre base de données source, vous pouvez utiliser AWS Schema Conversion Tool (AWS SCT). Vous utilisez AWS SCT pour migrer des objets de schéma qui ne sont pas migrés par AWS DMS. Pour plus d'informations sur AWS DMS, consultez Qu'est-ce que AWS Database Migration Service ?

Modifiez votre groupe de paramètres de base de données pour inclure les paramètres suivants pour votre importation uniquement. Vous devez tester les réglages des paramètres pour déterminer les réglages les plus efficaces pour la taille de votre instance de base de données. Vous devez également revenir aux valeurs de production pour ces paramètres une fois votre importation terminée.

Modifiez les paramètres de l'instance de base de données comme suit :

- Désactivez les sauvegardes de l'instance de base de données (affectez la valeur 0 à backup_retention).
- Désactivez le mode multi-AZ.

Modifiez votre groupe de paramètres DB pour inclure les paramètres suivants. Vous devez utiliser ces paramètres uniquement lors de l'importation des données. Vous devez tester les réglages des paramètres pour déterminer les réglages les plus efficaces pour la taille de votre instance de base de données. Vous devez également revenir aux valeurs de production pour ces paramètres une fois votre importation terminée.

Paramètre	Valeur recommandée lors de l'importation	Description
`maintenance_work_mem`	524288, 1048576, 2097152 ou 4194304 (en Ko). Ces paramètres sont comparables à 512 Mo, 1 Go, 2 Go et 4 Go.	La valeur de ce paramètre dépend de la taille de votre hôte. Ce paramètre est utilisé lors des instructions CREATE INDEX et chaque commande parallèle peut utiliser cette quantité de mémoire. Calculez la meilleure valeur afin de ne pas définir de valeur si élevée et risquer de manquer de mémoire.
`checkpoint_segments`	256	La valeur de ce paramètre consomme plus d'espace disque mais limite les conflits sur vos journaux WAL (write ahead log). Pour PostgreSQL versions 9.5.x et 9.6.x, cette valeur est `max_wal_size`.
`checkpoint_timeout`	1800	La valeur de ce paramètre vous permet une rotation WAL moins fréquente.
`synchronous_commit`	Désactivé	Désactivez ce paramètre pour accélérer les écritures. Le fait de désactiver ce paramètre peut augmenter le risque de perte de données en cas de défaillance du serveur (ne désactivez pas FSYNC).
`wal_buffers`	8192	Cette valeur est en unités de 8 Ko. Cela permet de nouveau d'accélérer la génération WAL

Paramètre	Valeur recommandée lors de l'importation	Description
`autovacuum`	Désactivé	Désactivez le paramètre auto-vacuum de PostgreSQL lorsque vous chargez des données afin qu'il n'utilise pas de ressources

Utilisez les commandes `pg_dump -Fc` (compressé) ou `pg_restore -j` (parallèle) avec ces paramètres.

> **Note**
>
> La commande PostgreSQL `pg_dumpall` requiert des autorisations super_user qui ne sont pas accordées lorsque vous créez une instance de base de données, si bien qu'elle ne peut pas être utilisée pour importer des données.

Rubriques

- Importation d'une base de données PostgreSQL à partir d'une instance Amazon EC2 (p. 1390)
- Utilisation de la commande \copy pour importer des données dans une table sur une instance de base de données PostgreSQL (p. 1392)
- Importation de données Amazon S3 dans une instance de base de données RDS for PostgreSQL d'un (p. 1393)
- Transport de bases de données PostgreSQL entre des instances de base de données (p. 1405)

Importation d'une base de données PostgreSQL à partir d'une instance Amazon EC2

Si vous possédez des données sur un serveur PostgreSQL sur une instance Amazon EC2 et que vous souhaitez les déplacer vers une instance de base de données PostgreSQL, vous pouvez utiliser le processus suivant. La liste suivante montre les étapes à suivre. Chaque étape est présentée plus en détail dans les sections suivantes.

1. Créez un fichier contenant les données à charger à l'aide de pg_dump
2. Créez l'instance de base de données cible
3. Utilisez psql pour créer la base de données sur l'instance de base de données et pour charger les données
4. Créez un instantané de base de données de l'instance de base de données

Étape 1 : Créer un fichier contenant les données à charger à l'aide de pg_dump

L'utilitaire `pg_dump` utilise la commande COPY pour créer un schéma et un vidage des données d'une base de données PostgreSQL. Le script de vidage généré par `pg_dump` charge les données dans une base de données dotée du même nom et recrée les tables, les index et les clés étrangères. Vous pouvez utiliser la commande `pg_restore` et le paramètre `-d` pour restaurer les données dans une base de données dotée d'un nom différent.

Avant de créer le vidage des données, vous devez interroger les tables à vider pour obtenir le nombre de lignes afin de pouvoir confirmer ce nombre sur l'instance de base de données cible.

La commande suivante crée un fichier de vidage mydb2dump.sql pour une base de données nommée mydb2.

```
prompt>pg_dump dbname=mydb2 -f mydb2dump.sql
```

Étape 2 : Créer l'instance de bases de données cible

Créez l'instance de base de données PostgreSQL cible à l'aide soit de la console Amazon RDS, de AWS CLI ou de l'API. Créez l'instance avec le paramètre de rétention des sauvegardes défini sur 0 et désactivez le mode multi-AZ. Cela vous permet d'effectuer une importation plus rapide des données. Vous devez créer une base de données sur l'instance avant de pouvoir vider les données. La base de données peut avoir le même nom que celle qui contenait les données vidées. Sinon, vous pouvez créer une base de données avec un autre nom. Dans ce cas, vous pouvez utiliser la commande `pg_restore` et le paramètre `-d` pour restaurer les données dans une base de données dotée d'un nouveau nom.

Par exemple, les commandes suivantes permettent de vider, de restaurer et de renommer une base de données.

```
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
```

Étape 3 : Utiliser psql pour créer la base de données sur l'instance de base de données et charger les données

Vous pouvez utiliser la même connexion que vous avez utilisée pour exécuter la commande pg_dump pour vous connecter à l'instance de base de données cible et recréer la base de données. Grâce à psql, vous pouvez utiliser l'identifiant principal et le mot de passe principal pour créer la base de données sur l'instance de base de données.

L'exemple suivant utilise psql et un fichier de vidage nommé mydb2dump.sql pour créer une base de données appelée mydb2 sur une instance de base de données PostgreSQL nommée mypginstance :

Pour Linux, macOS ou Unix :

```
psql \
   -f mydb2dump.sql \
   --host mypginstance.c6c8mntzhgv0.us-west-2.rds.amazonaws.com \
   --port 8199 \
   --username myawsuser \
   --password password \
   --dbname mydb2
```

Pour Windows :

```
psql ^
   -f mydb2dump.sql ^
   --host mypginstance.c6c8mntzhgv0.us-west-2.rds.amazonaws.com ^
   --port 8199 ^
   --username myawsuser ^
   --password password ^
   --dbname mydb2
```

Étape 4 : Créer un instantané de base de données de l'instance de bases de données

Une fois que vous avez vérifié que les données ont été chargées dans votre instance de base de données, nous vous conseillons de créer un instantané de base de données de l'instance de base de données

PostgreSQL cible. Les snapshots DB sont des sauvegardes complètes de votre instance de base de données qui peuvent être utilisées pour restaurer l'instance de base de données à un état connu. Un instantané de base de données pris immédiatement après le chargement vous évite de devoir charger les données à nouveau en cas d'incident. Vous pouvez également l'utiliser pour créer de nouvelles instances de base de données. Pour plus d'informations sur la création d'un instantané de base de données, consultez Création d'un instantané de base de données (p. 327).

Utilisation de la commande \copy pour importer des données dans une table sur une instance de base de données PostgreSQL

Vous pouvez exécuter la commande `\copy` dans l'invite de commandes psql pour importer des données dans un tableau sur une instance de base de données PostgreSQL. La table doit déjà exister sur l'instance de base de données. Pour plus d'informations sur la commande \copy, consultez la documentation sur PostgreSQL.

> **Note**
>
> La commande `\copy` ne fournit pas la confirmation des actions, telle qu'un nombre de lignes insérées. PostgreSQL ne fournit pas de messages d'erreur si la commande copy échoue en raison d'une erreur.

Créez un fichier .csv à partir des données dans le tableau source, connectez-vous à la base de données cible sur l'instance PostgreSQL à l'aide de psql, puis exécutez la commande suivante. Cet exemple utilise source-table comme nom de tableau source, source-table.csv comme fichier .csv et target-db comme base de données cible :

```
target-db=> \copy source-table from 'source-table.csv' with DELIMITER ',';
```

Vous pouvez également exécuter la commande suivante à partir de l'invite de commandes de votre ordinateur client. Cet exemple utilise source-table comme nom de tableau source, source-table.csv comme fichier .csv et target-db comme base de données cible :

Pour Linux, macOS ou Unix :

```
$psql target-db \
    -U <admin user> \
    -p <port> \
    -h <DB instance name> \
    -c "\copy source-table from 'source-table.csv' with DELIMITER ','"
```

Pour Windows :

```
$psql target-db ^
    -U <admin user> ^
    -p <port> ^
    -h <DB instance name> ^
    -c "\copy source-table from 'source-table.csv' with DELIMITER ','"
```

Importation de données Amazon S3 dans une instance de base de données RDS for PostgreSQL d'un

Vous pouvez importer des données d'Amazon S3 vers une table appartenant à une instance de base de données RDS pour PostgreSQL. Pour ce faire, utilisez l'extension PostgreSQL `aws_s3` fournie par Amazon RDS.

> **Note**
>
> Pour importer d'Amazon S3 vers RDS for PostgreSQL, votre base de données doit exécuter PostgreSQL version 10.7 ou ultérieure.

Pour plus d'informations sur le stockage de données avec Amazon S3, consultez Créer un compartiment dans le Amazon Simple Storage Service Guide de mise en route. Pour savoir comment charger un fichier dans un compartiment Amazon S3, consultez Ajouter un objet à un compartiment dans le Amazon Simple Storage Service Guide de mise en route.

Rubriques

- Présentation de l'importation de données Amazon S3 (p. 1393)
- Configuration de l'accès à un compartiment Amazon S3 (p. 1394)
- Utilisation de la fonction aws_s3.table_import_from_s3 pour importer des données Amazon S3 (p. 1399)
- Guide de référence des fonctions (p. 1401)

Présentation de l'importation de données Amazon S3

Pour importer des donnes stockées dans un compartiment Amazon S3 dans une table de base de données PostgreSQL, suivez ces étapes.

Pour importer des données S3 dans Amazon RDS

1. Installez les extensions PostgreSQL nécessaires. Il s'agit notamment des extensions `aws_s3` et `aws_commons`. Pour cela, démarrez psql et utilisez la commande suivante.

   ```
   psql=> CREATE EXTENSION aws_s3 CASCADE;
   NOTICE: installing required extension "aws_commons"
   ```

   L'extension `aws_s3` fournit la fonction aws_s3.table_import_from_s3 (p. 1401) que vous utilisez pour importer des données Amazon S3. L'extension `aws_commons` offre des fonctions d'assistant supplémentaires.
2. Identifiez la table de base de données et le fichier Amazon S3 à utiliser.

   La fonction aws_s3.table_import_from_s3 (p. 1401) a besoin du nom de la table de base de données PostgreSQL dans laquelle vous voulez importer les données. La fonction vous demande également d'identifier le fichier Amazon S3 à importer. Pour fournir ces informations, effectuez les étapes suivantes.

   a. Identifiez la table de base de données PostgreSQL dans laquelle placer les données. Par exemple, la table de base de données `t1` ci-dessous est utilisée dans les exemples de cette rubrique.

      ```
      psql=> CREATE TABLE t1 (col1 varchar(80), col2 varchar(80), col3 varchar(80));
      ```

b. Obtenez les informations suivantes pour identifier le fichier Amazon S3 que vous voulez importer :

- Nom du compartiment – Un compartiment est un conteneur d'objets ou de fichiers Amazon S3.
- Chemin du fichier – Le chemin du fichier permet de localiser le fichier dans le compartiment Amazon S3.
- Région AWS – La région AWS représente l'emplacement du compartiment Amazon S3. Par exemple, si le compartiment S3 se trouve dans la région USA Est (Virginie du Nord), utilisez `us-east-1`. Pour obtenir la liste des noms de régions AWS et les valeurs associées, consultez Régions, zones de disponibilité et zones locales (p. 39)

Pour savoir comment obtenir ces informations, consultez Affichage d'un objet dans le Amazon Simple Storage Service Guide de mise en route. Vous pouvez confirmer ces informations en utilisant la commande AWS CLI `aws s3 cp`. Si les informations sont correctes, cette commande télécharge une copie du fichier Amazon S3.

```
aws s3 cp s3://sample_s3_bucket/sample_file_path ./
```

c. Utilisez la fonction aws_commons.create_s3_uri (p. 1403) pour créer une structure `aws_commons._s3_uri_1` permettant d'accueillir les informations sur le fichier Amazon S3. Vous fournissez cette structure `aws_commons._s3_uri_1` comme paramètre dans l'appel à la fonction aws_s3.table_import_from_s3 (p. 1401).

Vous trouverez ci-dessous un exemple psql.

```
psql=> SELECT aws_commons.create_s3_uri(
   'sample_s3_bucket',
   'sample.csv',
   'us-east-1'
) AS s3_uri \gset
```

3. Fournissez une autorisation d'accès au fichier Amazon S3.

   Pour importer des données à partir d'un fichier Amazon S3, vous devez accorder à l'instance de base de données RDS for PostgreSQL une autorisation d'accès au compartiment Amazon S3 dans lequel se trouve le fichier. Pour cela, utilisez des informations d'identification de sécurité ou un rôle AWS Identity and Access Management (IAM). Pour plus d'informations, consultez Configuration de l'accès à un compartiment Amazon S3 (p. 1394).

4. Importez les données Amazon S3 en appelant la fonction `aws_s3.table_import_from_s3`.

   Après avoir effectué les tâches de préparation précédentes, utilisez la fonction aws_s3.table_import_from_s3 (p. 1401) pour importer les données Amazon S3. Pour plus d'informations, consultez Utilisation de la fonction aws_s3.table_import_from_s3 pour importer des données Amazon S3 (p. 1399).

Configuration de l'accès à un compartiment Amazon S3

Pour importer des données à partir d'un fichier Amazon S3, vous devez accorder à l'instance de base de données RDS for PostgreSQL une autorisation d'accès au compartiment Amazon S3 dans lequel se trouve le fichier. Pour accorder l'accès à un compartiment Amazon S3, vous pouvez employer une des deux méthodes décrites dans les rubriques suivantes.

Rubriques

- Utilisation d'un rôle IAM pour accéder à un compartiment Amazon S3 (p. 1395)
- Utilisation d'informations d'identification de sécurité pour accéder à un compartiment Amazon S3 (p. 1398)

- Résolution des problèmes d'accès à Amazon S3 (p. 1399)

Utilisation d'un rôle IAM pour accéder à un compartiment Amazon S3

Avant de charger des données à partir d'un fichier Amazon S3, accordez à votre instance de base de données RDS pour PostgreSQL l'autorisation d'accéder au compartiment Amazon S3 dans lequel se trouve le fichier. De cette façon, vous n'avez pas à gérer d'informations d'identification supplémentaires ni à les fournir dans l'appel de fonction aws_s3.table_import_from_s3 (p. 1401).

Pour ce faire, créez une stratégie IAM qui donne accès au compartiment Amazon S3. Créez un rôle IAM et attachez la stratégie à ce rôle. Attribuez ensuite le rôle IAM à votre instance de base de données.

Pour permettre à une instance de base de données RDS pour PostgreSQL d'accéder à Amazon S3 via un rôle IAM

1. Créez une stratégie IAM. Celle-ci fournit au compartiment et à l'objet les autorisations permettant à votre instance de base de données RDS pour PostgreSQL d'accéder à Amazon S3.

   Incluez à la stratégie les actions obligatoires suivantes pour permettre le transfert de fichiers d'un compartiment Amazon S3 vers Amazon RDS :

   - `s3:GetObject`
   - `s3:ListBucket`

   Incluez à la stratégie les ressources suivantes pour identifier le compartiment Amazon S3 et les objets qu'il contient. Voici le format Amazon Resource Name (ARN) permettant d'accéder à Amazon S3 :

   - arn:aws:s3:::*your-s3-bucket*
   - arn:aws:s3:::*your-s3-bucket*/*

   Pour plus d'informations sur la création d'une stratégie IAM pour Amazon RDS pour PostgreSQL, consultez Création et utilisation d'une stratégie IAM pour l'accès à une base de données IAM (p. 1558). Veuillez consulter également Didacticiel : Créer et attacher votre première stratégie gérée par le client dans le IAM Guide de l'utilisateur.

   La commande AWS CLI suivante crée une stratégie IAM nommée `rds-s3-import-policy` avec ces options. Elle accorde un accès à un compartiment nommé `your-s3-bucket`.

   > **Note**
   >
   > Après avoir créé la stratégie, notez son ARN (Amazon Resource Name). Vous en aurez besoin par la suite pour attacher la stratégie à un rôle IAM.

   Example

   Pour Linux, macOS ou 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/*"
        ]
      }
    ]
  }'
```

Pour 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. Créez un rôle IAM. L'objectif est ici de permettre à Amazon RDS d'endosser ce rôle IAM en votre nom pour accéder à vos compartiments Amazon S3. Pour de plus amples informations, veuillez consulter Création d'un rôle pour déléguer les autorisations à un utilisateur IAM dans le IAM Guide de l'utilisateur.

   L'exemple suivant montre comment utiliser la commande AWS CLI pour créer un rôle nommé `rds-s3-import-role`.

   Example

   Pour Linux, macOS ou 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"
       }
     ]
   }'
```

   Pour 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"
       }
     ]
   }'
```

3. Attachez la stratégie IAM que vous avez créée au rôle IAM que vous venez de créer.

   La commande AWS CLI suivante attache la stratégie créée précédemment au rôle nommé `rds-s3-import-role`. Remplacez *`your-policy-arn`* par l'ARN de la stratégie que vous avez noté à une étape précédente.

   Example

   Pour Linux, macOS ou Unix :

```
aws iam attach-role-policy \
   --policy-arn your-policy-arn \
   --role-name rds-s3-import-role
```

   Pour Windows :

```
aws iam attach-role-policy ^
   --policy-arn your-policy-arn ^
   --role-name rds-s3-import-role
```

4. Ajoutez le rôle IAM à l'instance de base de données. Pour ce faire, utilisez AWS Management Console ou AWS CLI, comme décrit à la suite.

Console

Pour ajouter un rôle IAM à l'instance du de base de données PostgreSQL à l'aide de la console

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Choisissez le nom de l'instance du de base de données PostgreSQL pour afficher ses détails.
3. Dans l'onglet Connectivity & security (Connexion & sécurité) de la section Manage IAM roles (Gérer les rôles IAM), choisissez le rôle à ajouter sous Add IAM roles to this instance (Ajouter les rôles IAM à cette instance).
4. Sous Feature (Fonctionnalité), choisissez s3Import.
5. Choisissez Add role (Ajouter un rôle).

AWS CLI

Pour ajouter un rôle IAM à une instance de base de données PostgreSQL à l'aide de l'interface de ligne de commande

- Utilisez la commande suivante pour ajouter le rôle à l'instance de base de données PostgreSQL nommée `my-db-instance`. Remplacez *`your-role-arn`* par l'ARN de rôle que vous avez noté lors d'une étape précédente. Utilisez `s3Import` comme valeur de l'option `--feature-name`.

  Example

  Pour Linux, macOS ou 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
```

  Pour 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
```

Utilisation d'informations d'identification de sécurité pour accéder à un compartiment Amazon S3

Si vous préférez, au lieu de donner à accès un compartiment Amazon S3 avec un rôle IAM, vous pouvez utiliser des informations d'identification de sécurité. Pour cela, utilisez le paramètre `credentials` dans l'appel de fonction aws_s3.table_import_from_s3 (p. 1401).

Le paramètre `credentials` est une structure de type `aws_commons._aws_credentials_1`, qui contient des informations d'identification AWS. Utilisez la fonction aws_commons.create_aws_credentials (p. 1404) pour définir la clé d'accès et la clé secrète dans une structure `aws_commons._aws_credentials_1`, comme indiqué ci-après.

```
psql=> SELECT aws_commons.create_aws_credentials(
   'sample_access_key', 'sample_secret_key', '')
AS creds \gset
```

Après avoir créé la structure `aws_commons._aws_credentials_1` , utilisez la fonction aws_s3.table_import_from_s3 (p. 1401) avec le paramètre `credentials` pour importer les données, comme indiqué ci-après.

```
psql=> SELECT aws_s3.table_import_from_s3(
   't', '', '(format csv)',
   :'s3_uri',
   :'creds'
);
```

Vous pouvez également inclure l'appel de fonction aws_commons.create_aws_credentials (p. 1404) en ligne au sein de l'appel de fonction `aws_s3.table_import_from_s3`.

```
psql=> SELECT aws_s3.table_import_from_s3(
   't', '', '(format csv)',
   :'s3_uri',
   aws_commons.create_aws_credentials('sample_access_key', 'sample_secret_key', '')
);
```

Résolution des problèmes d'accès à Amazon S3

Si vous rencontrez des problèmes de connexion lors de la tentative d'importation de données de fichier Amazon S3, reportez-vous aux recommandations suivantes :

- Résolution des problèmes liés à Identity and Access Amazon RDS (p. 1581)
- Résolutions des problèmes liés à Amazon S3
- Résolution des problèmes liés à Amazon S3 et IAM

Utilisation de la fonction aws_s3.table_import_from_s3 pour importer des données Amazon S3

Importez vos données Amazon S3 en appelant la fonction aws_s3.table_import_from_s3 (p. 1401).

> **Note**
>
> Les exemples suivants utilisent la méthode du rôle IAM pour donner accès au compartiment Amazon S3. Il n'y a donc pas de paramètres d'informations d'identification dans les appels de fonction `aws_s3.table_import_from_s3`.

Voici un exemple PostgreSQL type qui utilise psql.

```
psql=> SELECT aws_s3.table_import_from_s3(
   't1',
   '',
   '(format csv)',
   :'s3_uri'
);
```

Les paramètres sont les suivants :

- `t1` – Nom de la table de dans l'instance de base de données PostgreSQL dans laquelle copier les données.
- `''` – Liste facultative des colonnes de la table de base de données. Vous pouvez utiliser ce paramètre pour indiquer quelles colonnes des données S3 sont copiées dans quelles colonnes de table. Si aucune colonne n'est spécifiée, toutes les colonnes sont copiées dans la table. Pour obtenir un exemple d'utilisation d'une liste de colonnes, veuillez consulter Importation d'un fichier Amazon S3 qui utilise un délimiteur personnalisé (p. 1400).
- `(format csv)` – Arguments PostgreSQL COPY. Le processus de copie utilise les arguments et le format de la commande PostgreSQL COPY. Dans l'exemple précédent, la commande `COPY` utilise le format de fichier CSV (valeurs séparées par des virgules) pour copier les données.
- `s3_uri` – Structure contenant les informations d'identification du fichier Amazon S3. Pour obtenir un exemple d'utilisation de la fonction aws_commons.create_s3_uri (p. 1403) pour créer une structure `s3_uri`, consultez Présentation de l'importation de données Amazon S3 (p. 1393).

Pour obtenir des informations de référence complètes sur cette fonction, veuillez consulter aws_s3.table_import_from_s3 (p. 1401).

Les exemples suivants montrent comment spécifier différents types de fichiers lors de l'importation de données Amazon S3.

Rubriques

- Importation d'un fichier Amazon S3 qui utilise un délimiteur personnalisé (p. 1400)
- Importation d'un fichier compressé Amazon S3 (gzip) (p. 1400)
- Importation d'un fichier codé Amazon S3 (p. 1401)

Importation d'un fichier Amazon S3 qui utilise un délimiteur personnalisé

L'exemple suivant montre comment importer un fichier qui utilise un délimiteur personnalisé. Il montre également comment définir l'emplacement de destination des données dans la table de base de données à l'aide du paramètre `column_list` de la fonction aws_s3.table_import_from_s3 (p. 1401).

Pour cet exemple, supposons que les informations suivantes sont organisées en colonnes délimitées par une barre verticale dans le fichier Amazon S3.

```
1|foo1|bar1|elephant1
2|foo2|bar2|elephant2
3|foo3|bar3|elephant3
4|foo4|bar4|elephant4
...
```

Pour importer un fichier qui utilise un délimiteur personnalisé

1. Créez une table dans la base de données pour les données importées.

   ```
   psql=> CREATE TABLE test (a text, b text, c text, d text, e text);
   CREATE TABLE
   ```

2. Utilisez le format suivant de la fonction aws_s3.table_import_from_s3 (p. 1401) pour importer des données à partir du fichier Amazon S3.

   Vous pouvez inclure l'appel de fonction aws_commons.create_s3_uri (p. 1403) en ligne au sein de l'appel de fonction `aws_s3.table_import_from_s3` pour spécifier le fichier.

   ```
   psql=> SELECT aws_s3.table_import_from_s3(
      'test',
      'a,b,d,e',
      'DELIMITER ''|''',
      aws_commons.create_s3_uri('sampleBucket', 'pipeDelimitedSampleFile', 'us-east-2')
   );
   ```

Les données se retrouvent désormais dans la table dans les colonnes suivantes.

```
psql=> SELECT * FROM test;
a | b | c | d | e
---+------+---+---+------+-----------
1 | foo1 | | bar1 | elephant1
2 | foo2 | | bar2 | elephant2
3 | foo3 | | bar3 | elephant3
4 | foo4 | | bar4 | elephant4
```

Importation d'un fichier compressé Amazon S3 (gzip)

L'exemple suivant montre comment importer un fichier compressé avec gzip à partir d'Amazon S3.

Vérifiez que le fichier contient les métadonnées Amazon S3 suivantes :

- Clé : `Content-Encoding`
- Valeur : `gzip`

Pour de plus amples informations sur l'ajout de ces valeurs aux métadonnées Amazon S3, veuillez consulter Comment ajouter des métadonnées à un objet S3 ? dans le manuel Amazon Simple Storage Service Guide de l'utilisateur de la console.

Importez le fichier gzip dans l'instance de base de données RDS for PostgreSQL de votre comme décrit ci-après.

```
psql=> CREATE TABLE test_gzip(id int, a text, b text, c text, d text);
CREATE TABLE
psql=> SELECT aws_s3.table_import_from_s3(
 'test_gzip', '', '(format csv)',
 'myS3Bucket', 'test-data.gz', 'us-east-2'
);
```

Importation d'un fichier codé Amazon S3

L'exemple suivant montre comment importer un fichier codé en Windows-1252 à partir d'Amazon S3.

```
psql=> SELECT aws_s3.table_import_from_s3(
 'test_table', '', 'encoding ''WIN1252''',
 aws_commons.create_s3_uri('sampleBucket', 'SampleFile', 'us-east-2')
);
```

Guide de référence des fonctions

Fonctions

- aws_s3.table_import_from_s3 (p. 1401)
- aws_commons.create_s3_uri (p. 1403)
- aws_commons.create_aws_credentials (p. 1404)

aws_s3.table_import_from_s3

Importe les données Amazon S3 vers une table Amazon RDS. L'extension `aws_s3` fournit la fonction `aws_s3.table_import_from_s3`.

Syntaxe

Les trois paramètres obligatoires sont `table_name`, `column_list` et `options`. Ils identifient la table de base de données et spécifient la façon dont les données sont copiées dans la table.

Vous pouvez également utiliser les paramètres suivants :

- Le paramètre `s3_info` spécifie le fichier Amazon S3 à importer. Lorsque vous utilisez ce paramètre, l'accès à Amazon S3 est fourni par un rôle IAM pour l'instance du de base de données PostgreSQL.

```
aws_s3.table_import_from_s3 (
   table_name text,
   column_list text,
   options text,
   s3_info aws_commons._s3_uri_1
)
```

- Le paramètre `credentials` spécifie les informations d'identification permettant d'accéder à Amazon S3. Lorsque vous utilisez ce paramètre, vous n'utilisez pas de rôle IAM.

```
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
)
```

Paramètres

table_name

Chaîne de texte obligatoire contenant le nom de la table de base de données PostgreSQL dans laquelle importer les données.

column_list

Chaîne de texte obligatoire contenant la liste facultative des colonnes de la table de base de données PostgreSQL dans lesquelles copier les données. Si la chaîne est vide, toutes les colonnes de la table sont utilisées. Pour obtenir un exemple, veuillez consulter Importation d'un fichier Amazon S3 qui utilise un délimiteur personnalisé (p. 1400).

options

Chaîne de texte obligatoire contenant les arguments de la commande `COPY` de PostgreSQL. Ces arguments spécifient la façon dont les données sont copiées dans la table PostgreSQL. Pour de plus amples informations, veuillez consulter la documentation sur la commande COPY de PostgreSQL.

s3_info

Type composite `aws_commons._s3_uri_1` contenant les informations suivantes sur l'objet S3 :

- `bucket` – Nom du compartiment Amazon S3 contenant le fichier.
- `file_path` – Chemin d'accès Amazon S3 au fichier.
- `region` – Région AWS dans laquelle se trouve le fichier. Pour obtenir la liste des noms de régions AWS et les valeurs associées, consultez Régions, zones de disponibilité et zones locales (p. 39)

credentials

Type composite `aws_commons._aws_credentials_1` contenant les informations d'identification suivantes à utiliser pour l'opération d'importation :

- Clé d'accès
- Clé secrète
- Jeton de session

Pour de plus amples informations sur la création d'une structure composite `aws_commons._aws_credentials_1`, veuillez consulter aws_commons.create_aws_credentials (p. 1404).

Syntaxe alternative

Pour faciliter le test, vous pouvez utiliser un ensemble étendu de paramètres au lieu des paramètres `s3_info` et `credentials`. Plusieurs variations de syntaxe supplémentaires pour la fonction `aws_s3.table_import_from_s3` sont fournies ci-dessous.

- Au lieu d'utiliser le paramètre `s3_info` pour identifier un fichier Amazon S3, utilisez la combinaison des paramètres `bucket`, `file_path` et `region`. Sous cette forme, l'accès à Amazon S3 est fourni par un rôle IAM sur l'instance de base de données PostgreSQL.

```
aws_s3.table_import_from_s3 (
   table_name text,
   column_list text,
   options text,
   bucket text,
   file_path text,
   region text
)
```

- Au lieu d'utiliser le paramètre `credentials` pour spécifier l'accès à Amazon S3, utilisez la combinaison des paramètres `access_key`, `session_key` et `session_token`.

```
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
)
```

Autres paramètres

bucket

Chaîne de texte comportant le nom du compartiment Amazon S3 qui contient le fichier.

file_path

Chaîne de texte contenant le chemin d'accès Amazon S3 au fichier.

région

Chaîne de texte contenant la région AWS dans laquelle se trouve le fichier. Pour obtenir la liste des noms de régions AWS et les valeurs associées, consultez Régions, zones de disponibilité et zones locales (p. 39)

access_key

Chaîne de texte contenant la clé d'accès à utiliser pour l'opération d'importation. La valeur par défaut est NULL.

secret_key

Chaîne de texte contenant la clé secrète à utiliser pour l'opération d'importation. La valeur par défaut est NULL.

session_token

(Facultatif) Chaîne de texte contenant la clé de session à utiliser pour l'opération d'importation. La valeur par défaut est NULL.

aws_commons.create_s3_uri

Crée une structure `aws_commons._s3_uri_1` pour contenir les informations relatives au fichier Amazon S3. Utilisez les résultats de la fonction `aws_commons.create_s3_uri` dans le paramètre `s3_info` de la fonction aws_s3.table_import_from_s3 (p. 1401).

Syntaxe

```
aws_commons.create_s3_uri(
   bucket text,
   file_path text,
   region text
)
```

Paramètres

bucket

Chaîne de texte obligatoire contenant le nom du compartiment Amazon S3 pour le fichier.

file_path

Chaîne de texte obligatoire contenant le chemin d'accès Amazon S3 au fichier.

région

Chaîne de texte obligatoire contenant la région AWS dans laquelle se trouve le fichier. Pour obtenir la liste des noms de régions AWS et les valeurs associées, consultez Régions, zones de disponibilité et zones locales (p. 39)

aws_commons.create_aws_credentials

Définit une clé d'accès et une clé secrète dans une structure `aws_commons._aws_credentials_1`. Utilisez les résultats de la fonction `aws_commons.create_aws_credentials` dans le paramètre `credentials` de la fonction aws_s3.table_import_from_s3 (p. 1401).

Syntaxe

```
aws_commons.create_aws_credentials(
   access_key text,
   secret_key text,
   session_token text
)
```

Paramètres

access_key

Chaîne de texte obligatoire contenant la clé d'accès à utiliser pour l'importation d'un fichier Amazon S3. La valeur par défaut est NULL.

secret_key

Chaîne de texte obligatoire contenant la clé secrète à utiliser pour l'importation d'un fichier Amazon S3. La valeur par défaut est NULL.

session_token

Chaîne de texte facultative contenant le jeton de session à utiliser pour l'importation d'un fichier Amazon S3. La valeur par défaut est NULL. Si vous saisissez le paramètre `session_token` facultatif, vous pouvez utiliser les informations d'identification temporaires.

Transport de bases de données PostgreSQL entre des instances de base de données

Les bases de données transportables PostgreSQL pour Amazon RDS vous permettent de transporter une base de données PostgreSQL entre deux instances de base de données. Cette méthode permet de migrer très rapidement des bases de données volumineuses entre des instances de base de données distinctes. Pour que vous puissiez transporter des bases de données à l'aide de cette méthode, vos instances de base de données doivent toutes les deux exécuter la version majeure de PostgreSQL.

Pour utiliser des bases de données transportables, installez l'extension `pg_transport`. Cette extension offre un mécanisme physique de transport permettant de déplacer chaque base de données. En transmettant les fichiers de base de données avec un traitement minimal, le mécanisme de transport physique déplace les données bien plus rapidement qu'avec les processus traditionnels de vidage et de chargement, en provoquant une interruption minimale. Les bases de données transportables PostgreSQL utilisent un modèle d'extraction dans lequel l'instance de base de données de destination importe la base de données à partir de l'instance de base de données source.

> **Note**
>
> Les bases de données transportables PostgreSQL sont disponibles dans RDS pour les versions PostgreSQL 10.10 et ultérieures, et 11.5 et ultérieures.

Rubriques

- Limites à l'utilisation de bases de données transportables PostgreSQL (p. 1405)
- Configuration du transport de bases de données PostgreSQL (p. 1406)
- Transport d'une base de données PostgreSQL à l'aide de la fonction transport.import_from_server (p. 1406)
- Que se passe-t-il durant le transport d'une base de données ? (p. 1407)
- Fonction transport.import_from_server (p. 1407)
- Paramètre de configuration de l'extension pg_transport (p. 1408)

Limites à l'utilisation de bases de données transportables PostgreSQL

Les bases de données transportables présentent les limites suivantes :

- Réplicas en lecture – Vous ne pouvez pas utiliser les bases de données transportables sur les réplicas en lecture ou les instances parent de réplicas en lecture.
- Types de colonne non pris en charge – Vous ne pouvez pas utiliser les types de données `reg` dans les tables de bases de données que vous souhaitez transporter avec cette méthode. Ces types dépendent des ID d'objet de catalogue système (OID), qui varient souvent durant le transport.
- Espaces de tables – Tous les objets de base de données source doivent se trouver dans l'espace de table par défaut `pg_default`.
- Compatibilité – Les instances de base de données source et destination doivent exécuter la même version majeure de PostgreSQL.

  Avant que le transport ne débute, la fonction `transport.import_from_server` compare les instances de base de données source et de destination pour vérifier la compatibilité des bases de données. Elle vérifie en particulier la compatibilité avec la version majeure de PostgreSQL. La fonction vérifie aussi que l'instance de base de données de destination possède suffisamment d'espace pour recevoir la base de données source. Elle effectue plusieurs autres vérifications pour s'assurer que le transport est possible.

- Extensions – La seule extension que vous pouvez installer sur l'instance de base de données source durant le transport est `pg_transport`.
- Rôles et ACL – Les droits d'accès et les informations de propriété de la base de données source ne sont pas transportés vers la base de données de destination. Tous les objets de base de données sont créés par l'utilisateur de destination locale du transport et sont sa propriété.
- Transports simultanés – Vous pouvez effectuer jusqu'à 32 transports en même temps sur une instance de base de données, en incluant les importations et les exportations. Pour définit les processus de travail utilisés pour chaque transport, utilisez les paramètres `pg_transport.work_mem` et `pg_transport.num_workers`. Pour pouvoir effectuer des transports simultanés, il peut s'avérer nécessaire d'augmenter un peu la valeur du paramètre `max_worker_processes`. Pour de plus amples informations, veuillez consulter Paramètre de configuration de l'extension pg_transport (p. 1408).

Configuration du transport de bases de données PostgreSQL

Pour préparer le transport d'une base de données PostgreSQL d'une instance de base de données vers une autre, procédez comme indiqué ci-après.

Pour configurer le transport d'une base de données PostgreSQL

1. Veillez à ce que le groupe de sécurité de l'instance de base de données source autorise le trafic entrant depuis l'instance de base de données de destination. Cela est nécessaire, car l'instance de base de données de destination débute le transport de base de données par un appel d'importation en direction de l'instance de base de données source. Pour de plus amples informations sur l'utilisation des groupes de sécurité, veuillez consulter Contrôle d'accès par groupe de sécurité (p. 1590).
2. Ajoutez pour les instances de base de données source et de destination la valeur `pg_transport` au paramètre `shared_preload_libraries` dans chaque groupe de paramètres. Le paramètre `shared_preload_libraries` est statique et nécessite donc un redémarrage de la base de données pour prendre effet. Pour de plus amples informations sur les groupes de paramètres, veuillez consulter Utilisation de groupes de paramètres de base de données (p. 225).
3. Installez pour les instances de base de données source et de destination l'extension PostgreSQL `pg_transport` requise.

   Pour cela, démarrez psql en tant qu'utilisateur ayant le rôle `rds_superuser` pour chaque instance de base de données, puis exécutez la commande suivante :

   ```
   psql=> CREATE EXTENSION pg_transport;
   ```

Transport d'une base de données PostgreSQL à l'aide de la fonction transport.import_from_server

Une fois terminé le processus décrit dans Configuration du transport de bases de données PostgreSQL (p. 1406), vous pouvez démarrer le transport. Pour cela, exécutez la fonction transport.import_from_server (p. 1407) sur l'instance de base de données de destination.

> Note
>
> L'utilisateur de destination du transport et l'utilisateur source de la connexion doivent tous deux être membres du rôle `rds_superuser`.
> L'instance de base de données de destination ne doit pas déjà contenir une base de données portant le même nom que la base de données source à transporter. Si tel est le cas, le transport échoue.

L'illustration suivante présente un exemple de transport.

```
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);
```

Cette fonction nécessite que vous fournissiez les mots de passe utilisateur de la base de données. Nous vous recommandons donc de modifier les mots de passe des rôles utilisateur que vous avez utilisés une fois le transport terminé. Vous pouvez aussi utiliser des variables de liaison SQL pour créer des rôles utilisateur temporaires. Utilisez ces rôles temporaires pour le transport, puis supprimez-les une fois que vous n'en avez plus besoin.

Pour de plus amples informations sur la fonction `transport.import_from_server` et ses paramètres, veuillez consulter Fonction transport.import_from_server (p. 1407).

Que se passe-t-il durant le transport d'une base de données ?

La fonction `transport.import_from_server` crée la base de données en transit sur l'instance de base de données de destination. La base de données en transit est inaccessible sur l'instance de base de données de destination pendant toute la durée du transport.

Lorsque le transport commence, toutes les sessions en cours sur la base de données source cessent. Les bases de données autres que la base de données source sur l'instance de base de données source ne sont pas affectées par le transport.

La base de données source est placée dans un mode lecture seule spécial. Lorsqu'elle est dans ce mode, vous pouvez vous connecter à la base de données source et exécuter des requêtes de lecture seule. Par contre, les requêtes d'écriture et certains autres types de commandes sont bloqués. Seule la base de données source qui fait l'objet du transport est affectée par ces restrictions.

Durant le transport, vous ne pouvez pas restaurer l'instance de base de données de destination à un instant dans le passé. En effet, le transport n'est pas transactionnel et n'utilise pas le journal write-ahead (WAL) PostgreSQL pour enregistrer les modifications. Si les sauvegardes automatiques sont activées pour l'instance de base de données de destination, une sauvegarde est automatiquement effectuée une fois le transport terminé. Des restaurations à un instant dans le passé sont disponibles pour les périodes postérieures à la sauvegarde.

En cas d'échec du transport, l'extension `pg_transport` tente d'annuler toutes les modifications apportées aux instances de base de données source et de destination. Cela inclut la suppression de la base de données partiellement transportée sur la destination. Selon le type de défaillance, la base de données source peut continuer à rejeter les requêtes d'écriture. Si tel est le cas, utilisez la commande suivante pour autoriser les requêtes d'écriture.

```
ALTER DATABASE my-database SET default_transaction_read_only = false;
```

Fonction transport.import_from_server

La fonction `transport.import_from_server` transporte une base de données PostgreSQL en l'important d'une instance de base de données source vers une instance de base de données de destination. Elle effectue cette opération en utilisant un mécanisme de transport physique de connexion de base de données.

Syntaxe

```
transport.import_from_server(
   host text,
   port int,
   username text,
   password text,
   database text,
   local_password text,
   dry_run bool
)
```

Valeur renvoyée

Aucun.

Paramètres

Le tableau ci-dessous contient les descriptions des paramètres de la fonction `transport.import_from_server`.

Paramètre	Description
`host`	Point de terminaison de l'instance de base de données source.
`port`	Entier représentant le port de l'instance de base de données source. Les instances de base de données PostgreSQL utilisent souvent le port 5432.
`username`	Utilisateur de l'instance de base de données source. Cet utilisateur doit être membre du rôle `rds_superuser`.
`password`	Mot de passe utilisateur de l'instance de base de données source.
`database`	Nom de la base de données à transporter à partir de l'instance de base de données source.
`local_password`	Mot de passe local de l'utilisateur actuel pour l'instance de base de données de destination. Cet utilisateur doit être membre du rôle `rds_superuser`.
`dry_run`	Valeur booléenne facultative spécifiant si un essai est nécessaire. La valeur par défaut est `false`, ce qui signifie que le transport est effectué. Pour vérifier la compatibilité entre les instances de base de données source et de destination sans effectuer le transport réel, définissez `dry_run` sur `true`.

Exemple

Pour obtenir un exemple, consultez Transport d'une base de données PostgreSQL à l'aide de la fonction transport.import_from_server (p. 1406).

Paramètre de configuration de l'extension pg_transport

Utilisez les paramètres suivants pour configurer le comportement de l'extension `pg_transport`.

```
SET pg_transport.num_workers = integer;
SET pg_transport.work_mem = kilobytes;
SET pg_transport.timing = Boolean;
```

Le tableau ci-dessous contient les descriptions de ces paramètres.

Paramètre	Description
`pg_transport.num_workers`	Nombre d'unités de travail à utiliser pour un transport physique. La valeur par défaut est 3. Les valeurs valides vont de 1 à 32. Même les transports volumineux atteignent généralement leur débit maximal avec moins de 8 unités de travail. Durant le transport, la valeur de `pg_transport.num_workers` sur l'instance de base de données de destination est utilisée à la fois sur les instances de base de données source et de destination. Un paramètre associé est le paramètre PostgreSQL `max_worker_processes`. Le processus de transport crée plusieurs processus de travail en arrière-plan. La valeur du paramètre `pg_transport.num_workers` peut vous obliger à définir le paramètre `max_worker_processes` sur une valeur beaucoup plus élevée à la fois sur les instances de base de données source et de destination. Nous vous recommandons de définir `max_worker_processes` à la fois sur les instances de base de données source et de destination sur une valeur au moins trois fois supérieure à celle du paramètre `pg_transport.num_workers` sur l'instance de base de données de destination. Augmentez un peu la valeur pour pouvoir fournir des processus de travail autres que ceux du transport en arrière-plan. Pour de plus amples informations sur le paramètre `max_worker_processes`, veuillez consulter la documentation PostgreSQL sur le Comportement asynchrone.
`pg_transport.timing`	Valeur booléenne qui indique s'il est nécessaire de signaler des informations temporelles durant le transport. La valeur par défaut est `true`. Les valeurs valides sont `true` pour signaler des informations temporelles et `false` pour désactiver le signalement de ce type d'informations. Nous vous déconseillons de définir ce paramètre sur `false`. La désactivation de `pg_transport.timing` réduit considérablement votre capacité de suivi de la progression du transport.
`pg_transport.work_mem`	Quantité de mémoire maximale à allouer à chaque unité de travail. La valeur par défaut est de 131 072 kilo-octets (Ko). La valeur minimale est de 64 méga-octets (65 536 Ko). Les valeurs valides sont exprimées en kilo-octets (Ko) sous forme d'unités binaires de base 2, où 1 Ko = 1 024 octets. Le transport peut utiliser moins de mémoire que spécifié dans ce paramètre. Même les transports volumineux atteignent généralement leur débit maximal avec moins de 256 Mo (262 144 Ko) de mémoire par unité de travail.

Exportation de données à partir d'une instance de base de données RDS for PostgreSQL vers Amazon S3

Vous pouvez interroger des données à partir d'une instance de base de données RDS for PostgreSQL et les exporter directement dans des fichiers stockés dans un compartiment Amazon S3. Pour ce faire, utilisez l'extension PostgreSQL `aws_s3` fournie par Amazon RDS.

Pour plus d'informations sur le stockage de données avec Amazon S3, consultez Créer un compartiment dans le Amazon Simple Storage Service Guide de mise en route.

Rubriques

- Présentation de l'exportation de données vers Amazon S3 (p. 1410)
- Spécification du chemin d'accès au fichier Amazon S3 vers lequel effectuer l'exportation (p. 1411)
- Configuration de l'accès à un compartiment Amazon S3 (p. 1411)
- Exportation de données de requête à l'aide de la fonction aws_s3.query_export_to_s3 (p. 1414)
- Guide de référence des fonctions (p. 1416)

Présentation de l'exportation de données vers Amazon S3

Pour exporter des données stockées dans une base de données RDS PostgreSQL vers un compartiment Amazon S3, procédez comme suit.

Pour exporter des données Amazon RDS PostgreSQL vers S3

1. Installez les extensions PostgreSQL nécessaires. Il s'agit notamment des extensions `aws_s3` et `aws_commons`. Pour cela, démarrez psql et utilisez les commandes suivantes.

   ```
   CREATE EXTENSION IF NOT EXISTS aws_s3 CASCADE;
   ```

   L'extension `aws_s3` fournit la fonction aws_s3.query_export_to_s3 (p. 1416) que vous utilisez pour exporter des données vers Amazon S3. L'extension `aws_commons` est incluse pour fournir des fonctions d'assistance supplémentaires.
2. Identifiez un chemin d'accès de fichier Amazon S3 à utiliser pour exporter des données. Pour de plus amples informations sur ce processus, veuillez consulter Spécification du chemin d'accès au fichier Amazon S3 vers lequel effectuer l'exportation (p. 1411).
3. Fournissez une autorisation d'accès au compartiment Amazon S3.

   Pour exporter des données vers un fichier Amazon S3, vous devez accorder à l'instance de base de données RDS for PostgreSQL l'autorisation d'accéder au compartiment Amazon S3 que l'exportation utilisera pour le stockage. Cette opération comprend les étapes suivantes :

   1. Créez une stratégie IAM donnant accès à un compartiment Amazon S3 vers lequel vous souhaitez exporter.
   2. Créez un rôle IAM.
   3. Attachez la stratégie que vous avez créée au rôle que vous avez créé.
   4. Ajoutez ce rôle IAM à votre instance de base de données.

   Pour de plus amples informations sur ce processus, veuillez consulter Configuration de l'accès à un compartiment Amazon S3 (p. 1411).
4. Identifiez une requête de base de données pour obtenir les données. Exportez les données de requête en appelant la fonction `aws_s3.query_export_to_s3`.

   Après avoir terminé les tâches de préparation précédentes, utilisez la fonction aws_s3.query_export_to_s3 (p. 1416) pour exporter les résultats de requête vers Amazon S3. Pour de plus amples informations sur ce processus, veuillez consulter Exportation de données de requête à l'aide de la fonction aws_s3.query_export_to_s3 (p. 1414).

Spécification du chemin d'accès au fichier Amazon S3 vers lequel effectuer l'exportation

Spécifiez les informations suivantes pour identifier l'emplacement dans Amazon S3 vers lequel vous souhaitez exporter des données :

- Nom du compartiment – Un compartiment est un conteneur d'objets ou de fichiers Amazon S3.

  Pour de plus amples informations sur le stockage de données avec Amazon S3, veuillez consulter Créer un compartiment et Afficher un objet dans le Amazon Simple Storage Service Guide de mise en route.
- Chemin d'accès au fichier – Le chemin d'accès au fichier identifie l'emplacement de stockage de l'exportation dans le compartiment Amazon S3. Le chemin d'accès au fichier se compose des éléments suivants :
  - Préfixe de chemin facultatif qui identifie un chemin d'accès à un dossier virtuel.
  - Préfixe de fichier qui identifie un ou plusieurs fichiers à stocker. Les exportations les plus volumineuses sont stockées dans plusieurs fichiers, chacun ayant une taille maximale d'environ 6 Go. Les noms de fichiers supplémentaires ont le même préfixe de fichier mais en ajoutant `_partXX`. `XX` représente 2, puis 3, et ainsi de suite.

  Par exemple, un chemin d'accès de fichier avec un dossier `exports` et un préfixe de fichier `query-1-export` sera représenté par `/exports/query-1-export`.
- Région AWS (facultatif) – Région AWS où se trouve le compartiment Amazon S3. Si vous ne spécifiez pas de valeur de région AWS, Amazon RDS enregistre vos fichiers dans Amazon S3 dans la même région AWS que celle où se trouve l'instance de base de données.

  > **Note**
  >
  > Actuellement, la région AWS doit être la même que celle de l'instance de base de données à l'origine de l'exportation.

  Pour obtenir la liste des noms de régions AWS et les valeurs associées, consultez Régions, zones de disponibilité et zones locales (p. 39)

Pour conserver les informations de fichier Amazon S3 sur l'emplacement de stockage de l'exportation, vous pouvez utiliser la fonction aws_commons.create_s3_uri (p. 1419) pour créer une structure composite `aws_commons._s3_uri_1` comme suit.

```
psql=> SELECT aws_commons.create_s3_uri(
   'sample-bucket',
   'sample-filepath',
   'us-west-2'
) AS s3_uri_1 \gset
```

Vous fournissez ultérieurement cette valeur `s3_uri_1` en tant que paramètre dans l'appel à la fonction aws_s3.query_export_to_s3 (p. 1416). Pour obtenir des exemples, consultez Exportation de données de requête à l'aide de la fonction aws_s3.query_export_to_s3 (p. 1414).

Configuration de l'accès à un compartiment Amazon S3

Pour exporter des données vers Amazon S3, accordez à votre instance l'autorisation d'accéder au compartiment Amazon S3 dans lequel les fichiers doivent être stockés.

Pour cela, procédez comme suit :

Pour donner à une instance de base de données PostgreSQL l'accès à Amazon S3 via un rôle IAM

1. Créez une stratégie IAM.

   Cette stratégie fournit le compartiment et les autorisations d'objet permettant à votre instance de base de données PostgreSQL d'accéder à Amazon S3.

   Dans le cadre de la création de cette stratégie, procédez comme suit :

   a. Incluez dans la stratégie les actions obligatoires suivantes pour permettre le transfert de fichiers de votre instance de base de donnée PostgreSQL vers un compartiment Amazon S3 :

      - `s3:PutObject`
      - `s3:AbortMultipartUpload`

   b. Incluez l'Amazon Resource Name (ARN) qui identifie le compartiment Amazon S3 et les objets du compartiment. Le format ARN pour l'accès à Amazon S3 est le suivant : `arn:aws:s3:::your-s3-bucket/*`

   Pour plus d'informations sur la création d'une stratégie IAM pour Amazon RDS pour PostgreSQL, consultez Création et utilisation d'une stratégie IAM pour l'accès à une base de données IAM (p. 1558). Veuillez consulter également Didacticiel : Créer et attacher votre première stratégie gérée par le client dans le IAM Guide de l'utilisateur.

   La commande d'AWS CLI suivante crée une stratégie IAM nommée `rds-s3-export-policy` avec ces options. Elle accorde un accès à un compartiment nommé `your-s3-bucket`.

   > **Warning**
   >
   > Nous vous recommandons de configurer votre base de données dans un VPC privé dont les stratégies de point de terminaison sont configurées pour accéder à des compartiments spécifiques. Pour de plus amples informations, veuillez consulter Utilisation des stratégies de point de terminaison pour Amazon S3 dans le Amazon VPC Guide de l'utilisateur.
   > Nous vous recommandons vivement de ne pas créer de stratégie avec accès à toutes les ressources. Cet accès peut constituer une menace pour la sécurité des données. Si vous créez une stratégie qui accorde à `S3:PutObject` un accès à toutes les ressources à l'aide de `"Resource":"*"`, un utilisateur disposant de privilèges d'exportation peut exporter des données vers tous les compartiments de votre compte. En outre, l'utilisateur peut exporter des données vers n'importe quel compartiment accessible publiquement en écriture dans votre région AWS.

   Après avoir créé la stratégie, notez son ARN (Amazon Resource Name). Vous en aurez besoin par la suite pour attacher la stratégie à un rôle IAM.

```
aws iam create-policy  --policy-name rds-s3-export-policy  --policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Sid": "s3export",
         "Action": [
           "S3:PutObject"
         ],
         "Effect": "Allow",
         "Resource": [
           "arn:aws:s3:::your-s3-bucket/*"
         ]
       }
     ]
```

```
   }'
```

2. Créez un rôle IAM.

   L'objectif est ici de permettre à Amazon RDS d'endosser ce rôle IAM en votre nom pour accéder à vos compartiments Amazon S3. Pour de plus amples informations, veuillez consulter Création d'un rôle pour déléguer les autorisations à un utilisateur IAM dans le IAM Guide de l'utilisateur.

   L'exemple suivant montre comment utiliser la commande d'AWS CLI pour créer un rôle nommé `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": "rds.amazonaws.com"
          },
         "Action": "sts:AssumeRole"
       }
     ]
   }'
```

3. Attachez la stratégie IAM que vous avez créée au rôle IAM que vous venez de créer.

   La commande d'AWS CLI suivante attache la stratégie créée précédemment au rôle nommé `rds-s3-export-role.`. Remplacez *`your-policy-arn`* par l'ARN de la stratégie que vous avez noté à une étape précédente.

```
aws iam attach-role-policy  --policy-arn your-policy-arn  --role-name rds-s3-export-
role
```

4. Ajoutez le rôle IAM à l'instance de base de données. Pour ce faire, utilisez AWS Management Console ou AWS CLI, comme décrit à la suite.

Console

Pour ajouter un rôle IAM à l'instance du de base de données PostgreSQL à l'aide de la console

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Choisissez le nom de l'instance du de base de données PostgreSQL pour afficher ses détails.
3. Dans l'onglet Connectivity & security (Connexion & sécurité) de la section Manage IAM roles (Gérer les rôles IAM), choisissez le rôle à ajouter sous Add IAM roles to this instance (Ajouter les rôles IAM à cette instance).
4. Sous Feature (Fonctionnalité), choisissez s3Export.
5. Choisissez Add role (Ajouter un rôle).

AWS CLI

Pour ajouter un rôle IAM à une instance de base de données PostgreSQL à l'aide de l'interface de ligne de commande

- Utilisez la commande suivante pour ajouter le rôle à l'instance de base de données PostgreSQL nommée `my-db-instance`. Remplacez *`your-role-arn`* par l'ARN de rôle que vous avez noté lors d'une étape précédente. Utilisez `s3Export` comme valeur de l'option `--feature-name`.

Example

Pour Linux, macOS ou 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
```

Pour 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
```

Exportation de données de requête à l'aide de la fonction aws_s3.query_export_to_s3

Exportez vos données PostgreSQL vers Amazon S3 en appelant la fonction aws_s3.query_export_to_s3 (p. 1416).

Rubriques

- Conditions préalables requises (p. 1414)
- Appel de aws_s3.query_export_to_s3 (p. 1415)
- Exportation vers un fichier CSV qui utilise un délimiteur personnalisé (p. 1416)
- Exportation vers un fichier binaire avec encodage (p. 1416)
- Résolution des problèmes d'accès à Amazon S3 (p. 1416)

Conditions préalables requises

Avant d'utiliser la fonction `aws_s3.query_export_to_s3`, assurez-vous de remplir les conditions préalables suivantes :

- Installez les extensions PostgreSQL requises comme décrit dans Présentation de l'exportation de données vers Amazon S3 (p. 1410).
- Déterminez vers quel emplacement Amazon S3 exporter vos données comme décrit dans Spécification du chemin d'accès au fichier Amazon S3 vers lequel effectuer l'exportation (p. 1411).
- Assurez-vous que le cluster de base de données dispose d'un accès à Amazon S3 comme décrit dans Configuration de l'accès à un compartiment Amazon S3 (p. 1411).

Les exemples suivants utilisent une table de base de données appelée `sample_table`. Ces exemples exportent les données dans un compartiment appelé `sample-bucket`. Les exemples de table et de données sont créés avec les instructions SQL suivantes dans 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');
```

Appel de aws_s3.query_export_to_s3

Ce qui suit montre les techniques de base permettant d'appeler la fonction aws_s3.query_export_to_s3 (p. 1416).

Ces exemples utilisent la variable `s3_uri_1` pour identifier une structure contenant les informations identifiant le fichier Amazon S3. Utilisez la fonction aws_commons.create_s3_uri (p. 1419) pour créer la structure.

```
psql=> SELECT aws_commons.create_s3_uri(
   'sample-bucket',
   'sample-filepath',
   'us-west-2'
) AS s3_uri_1 \gset
```

Bien que les paramètres varient pour les deux appels de fonction `aws_s3.query_export_to_s3` suivants, les résultats sont les mêmes pour ces exemples. Toutes les lignes de la table `sample_table` sont exportées dans un compartiment appelé `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');
```

Les paramètres sont décrits comme suit :

- `'SELECT * FROM sample_table'` – Le premier paramètre est une chaîne de texte obligatoire contenant une requête SQL. Le moteur PostgreSQL exécute cette requête. Les résultats de la requête sont copiés dans le compartiment S3 identifié dans d'autres paramètres.
- `:'s3_uri_1'` – Ce paramètre est une structure qui identifie le fichier Amazon S3. Cet exemple utilise une variable pour identifier la structure créée précédemment. Vous pouvez plutôt créer la structure en incluant l'appel de fonction `aws_commons.create_s3_uri` en ligne dans l'appel de fonction `aws_s3.query_export_to_s3` comme suit.

  ```
  SELECT * from aws_s3.query_export_to_s3('select * from sample_table',
     aws_commons.create_s3_uri('sample-bucket', 'sample-filepath', 'us-west-2')
  );
  ```

- `options :='format text'` – Le paramètre `options` est une chaîne de texte facultative contenant des arguments `COPY` PostgreSQL. Le processus de copie utilise les arguments et le format de la commande PostgreSQL COPY.

Si le fichier spécifié n'existe pas dans le compartiment Amazon S3, il est créé. Si le fichier existe déjà, il est remplacé. La syntaxe d'accès aux données exportées dans Amazon S3 est la suivante.

```
s3-region://bucket-name[/path-prefix]/file-prefix
```

Les exportations les plus volumineuses sont stockées dans plusieurs fichiers, chacun ayant une taille maximale d'environ 6 Go. Les noms de fichiers supplémentaires ont le même préfixe de fichier mais en ajoutant `_partXX`. *XX* représente 2, puis 3, et ainsi de suite. Par exemple, supposons que vous spécifiiez le chemin d'accès où vous stockez les fichiers de données comme suit.

```
s3-us-west-2://my-bucket/my-prefix
```

Si l'exportation doit créer trois fichiers de données, le compartiment Amazon S3 contient les fichiers de données suivants.

```
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
```

Pour obtenir la référence complète de cette fonction et les moyens supplémentaires de l'appeler, veuillez consulter aws_s3.query_export_to_s3 (p. 1416). Pour de plus amples informations sur l'accès aux fichiers dans Amazon S3, veuillez consulter Afficher un objet dans le Amazon Simple Storage Service Guide de mise en route.

Exportation vers un fichier CSV qui utilise un délimiteur personnalisé

L'exemple suivant montre comment appeler la fonction aws_s3.query_export_to_s3 (p. 1416) pour exporter des données vers un fichier qui utilise un délimiteur personnalisé. L'exemple utilise les arguments de la commande PostgreSQL COPY pour spécifier le format CSV (valeur séparée par des virgules) et un délimiteur deux-points (:).

```
SELECT * from aws_s3.query_export_to_s3('select * from basic_test', :'s3_uri_1',
 options :='format csv, delimiter $$:$$');
```

Exportation vers un fichier binaire avec encodage

L'exemple suivant montre comment appeler la fonction aws_s3.query_export_to_s3 (p. 1416) pour exporter des données vers un fichier binaire ayant un encodage Windows-1253.

```
SELECT * from aws_s3.query_export_to_s3('select * from basic_test', :'s3_uri_1',
 options :='format binary, encoding WIN1253');
```

Résolution des problèmes d'accès à Amazon S3

Si vous rencontrez des problèmes de connexion lors de la tentative d'exportation de données vers Amazon S3, veuillez consulter les recommandations suivantes :

- Résolution des problèmes liés à Identity and Access Amazon RDS (p. 1581)
- Dépannage de Amazon S3 dans le Amazon Simple Storage Service Manuel du développeur.
- Résolution des problèmes liés à Amazon S3 et IAM dans le IAM Guide de l'utilisateur.

Guide de référence des fonctions

Fonctions

- aws_s3.query_export_to_s3 (p. 1416)
- aws_commons.create_s3_uri (p. 1419)

aws_s3.query_export_to_s3

Exporte un résultat de requête PostgreSQL vers un compartiment Amazon S3. L'extension `aws_s3` fournit la fonction `aws_s3.query_export_to_s3`.

Les deux paramètres requis sont `query` et `s3_info`. Ils définissent la requête à exporter et identifient le compartiment Amazon S3 vers lequel effectuer l'exportation. Un paramètre facultatif appelé `options`

permet de définir différents paramètres d'exportation. Pour obtenir des exemples d'utilisation de la fonction `aws_s3.query_export_to_s3`, veuillez consulter Exportation de données de requête à l'aide de la fonction aws_s3.query_export_to_s3 (p. 1414).

Syntaxe

```
aws_s3.query_export_to_s3(
    query text,
    s3_info aws_commons._s3_uri_1,
    options text
)
```

Paramètres d'entrée

query

Chaîne de texte obligatoire contenant une requête SQL exécutée par le moteur PostgreSQL. Les résultats de cette requête sont copiés dans un compartiment S3 identifié dans le paramètre `s3_info`.

s3_info

Type composite `aws_commons._s3_uri_1` contenant les informations suivantes sur l'objet S3 :

- `bucket` – Nom du compartiment Amazon S3 contenant le fichier.
- `file_path` – Chemin d'accès Amazon S3 au fichier.
- `region` – Région AWS dans laquelle se trouve le compartiment. Pour obtenir la liste des noms de régions AWS et les valeurs associées, consultez Régions, zones de disponibilité et zones locales (p. 39)

  Actuellement, cette valeur doit être la même région AWS que celle du cluster de base de données à l'origine de l'exportation. La valeur par défaut est la région AWS du cluster de base de données à l'origine de l'exportation.

Pour créer une structure composite `aws_commons._s3_uri_1`, veuillez consulter aws_commons.create_s3_uri (p. 1419) fonction.

options

Chaîne de texte facultative contenant les arguments de la commande `COPY` de PostgreSQL. Ces arguments spécifient la façon dont les données doivent être copiées lors de l'exportation. Pour de plus amples informations, veuillez consulter la documentation sur la commande COPY de PostgreSQL.

Autres paramètres d'entrée

Pour faciliter le test, vous pouvez utiliser un ensemble étendu de paramètres au lieu du paramètre `s3_info`. Plusieurs variations de syntaxe supplémentaires pour la fonction `aws_s3.query_export_to_s3` sont fournies ci-dessous.

Au lieu d'utiliser le paramètre `s3_info` pour identifier un fichier Amazon S3, utilisez la combinaison des paramètres `bucket`, `file_path` et `region`.

```
aws_s3.query_export_to_s3(
    query text,
    bucket text,
    file_path text,
    region text,
    options text
)
```

query

Chaîne de texte obligatoire contenant une requête SQL exécutée par le moteur PostgreSQL. Les résultats de cette requête sont copiés dans un compartiment S3 identifié dans le paramètre `s3_info`.

bucket

Chaîne de texte obligatoire comportant le nom du compartiment Amazon S3 qui contient le fichier.

file_path

Chaîne de texte obligatoire contenant le chemin d'accès Amazon S3 au fichier.

région

Chaîne de texte facultative contenant la région AWS dans laquelle se trouve le compartiment. Pour obtenir la liste des noms de régions AWS et les valeurs associées, consultez Régions, zones de disponibilité et zones locales (p. 39)

Actuellement, cette valeur doit être la même région AWS que celle du cluster de base de données à l'origine de l'exportation. La valeur par défaut est la région AWS du cluster de base de données à l'origine de l'exportation.

options

Chaîne de texte facultative contenant les arguments de la commande `COPY` de PostgreSQL. Ces arguments spécifient la façon dont les données doivent être copiées lors de l'exportation. Pour de plus amples informations, veuillez consulter la documentation sur la commande COPY de PostgreSQL.

Paramètres de sortie

```
aws_s3.query_export_to_s3(
    OUT rows_uploaded bigint,
    OUT files_uploaded bigint,
    OUT bytes_uploaded bigint
)
```

rows_uploaded

Nombre de lignes de table qui ont été téléchargées avec succès vers Amazon S3 pour la requête donnée.

files_uploaded

Nombre de fichiers téléchargés vers Amazon S3. Les fichiers sont créés avec des tailles d'environ 6 Go. Chaque fichier supplémentaire créé voit l'élément `_part`*`XX`* ajouté à son nom. *`XX`* représente 2, puis 3, et ainsi de suite.

bytes_uploaded

Nombre total d'octets téléchargés vers Amazon S3.

Exemples

```
psql=> SELECT * from aws_s3.query_export_to_s3('select * from sample_table', 'sample-
bucket', 'sample-filepath');
psql=> SELECT * from aws_s3.query_export_to_s3('select * from sample_table', 'sample-
bucket', 'sample-filepath','us-west-2');
psql=> SELECT * from aws_s3.query_export_to_s3('select * from sample_table', 'sample-
bucket', 'sample-filepath','us-west-2','format text');
```

aws_commons.create_s3_uri

Crée une structure `aws_commons._s3_uri_1` pour contenir les informations relatives au fichier Amazon S3. Vous utilisez les résultats de la fonction `aws_commons.create_s3_uri` dans le paramètre `s3_info` de la fonction aws_s3.query_export_to_s3 (p. 1416). Pour obtenir un exemple d'utilisation de la fonction `aws_commons.create_s3_uri`, veuillez consulter Spécification du chemin d'accès au fichier Amazon S3 vers lequel effectuer l'exportation (p. 1411).

Syntaxe

```
aws_commons.create_s3_uri(
   bucket text,
   file_path text,
   region text
)
```

Paramètres d'entrée

bucket

Chaîne de texte obligatoire contenant le nom du compartiment Amazon S3 pour le fichier.

file_path

Chaîne de texte obligatoire contenant le chemin d'accès Amazon S3 au fichier.

région

Chaîne de texte obligatoire contenant la région AWS dans laquelle se trouve le fichier. Pour obtenir la liste des noms de régions AWS et les valeurs associées, consultez Régions, zones de disponibilité et zones locales (p. 39)

Tâches DBA courantes pour PostgreSQL

Cette section décrit les implémentations de Amazon RDS de certaines tâches d'administration de base de données courantes pour les instances de bases de données exécutant le moteur de base de données PostgreSQL. Pour offrir une expérience de service géré, Amazon RDS ne fournit pas l'accès shell aux instances de base de données et limite l'accès à certaines tables et procédures système qui requièrent des privilèges avancés.

Pour plus d'informations sur l'utilisation de fichiers journaux PostgreSQL sur Amazon RDS, consultez Fichiers journaux de base de données PostgreSQL (p. 521).

Rubriques

- Création de rôles (p. 1420)
- Gestion d'un accès à la base de données PostgreSQL (p. 1420)
- Utilisation des paramètres PostgreSQL (p. 1421)
- Utilisation de la fonction autovacuum de PostgreSQL sur Amazon RDS (p. 1431)
- Journalisation d'audit pour une instance de base de données PostgreSQL (p. 1440)
- Utilisation de l'extension pgaudit (p. 1440)
- Utilisation de l'extension pg_repack (p. 1442)
- Utilisation de PostGIS (p. 1443)
- Utilisation de pgBadger pour l'analyse de journal serveur avec PostgreSQL (p. 1445)
- Affichage du contenu de pg_config (p. 1445)
- Utilisation de l'extension orafce (p. 1446)
- Accès aux données externes à l'aide de l'extension postgres_fdw (p. 1447)

- Utilisation d'un serveur DNS personnalisé pour l'accès réseau sortant. (p. 1448)
- Restriction de la gestion des mots de passe (p. 1449)

Création de rôles

Lorsque vous créez une instance de base de données, le rôle `rds_superuser` est affecté au compte du système de l'utilisateur principal que vous avez créé. Le rôle `rds_superuser` est un rôle Amazon RDS prédéfini semblable au rôle de superutilisateur PostgreSQL (habituellement désigné sous le nom de `postgres` dans les instances locales), mais limité par certaines restrictions. Tout comme le rôle de superutilisateur PostgreSQL, le rôle `rds_superuser` dispose du plus grand nombre de privilèges pour votre instance de base de données. Vous ne devriez pas attitrer ce rôle à des utilisateurs, sauf s'ils nécessitent l'accès le plus étendu à l'instance de base de données.

Le rôle `rds_superuser` permet d'effectuer les opérations suivantes :

- Ajoutez les extensions qu'il est possible d'utiliser avec Amazon RDS. Pour plus d'informations, consultez Fonctions PostgreSQL prises en charge (p. 1509) et la documentation sur PostgreSQL.
- Gérer les espaces de table, y compris en créer et les supprimer. Pour plus d'informations, consultez la section Tablespaces dans la documentation PostgreSQL.
- Répertorier tous les utilisateurs auxquels le rôle `rds_superuser` n'est pas attribué à l'aide de la commande `pg_stat_activity` et mettre fin à leur connexion à l'aide des commandes `pg_terminate_backend` et `pg_cancel_backend`.
- Accorder et révoquer le rôle `rds_replication` pour tous les rôles autres que le rôle `rds_superuser`. Pour plus d'informations, consultez la section GRANT (ACCORDER) dans la documentation PostgreSQL.

L'exemple suivant montre comment créer un utilisateur puis lui affecter le rôle `rds_superuser`. Les rôles définis par l'utilisateur, comme `rds_superuser`, doivent être accordés.

```
create role testuser with password 'testuser' login;
CREATE ROLE
grant rds_superuser to testuser;
GRANT ROLE
```

Gestion d'un accès à la base de données PostgreSQL

Dans Amazon RDS pour PostgreSQL, vous pouvez contrôler quels utilisateurs disposent des accès aux bases de données. Dans les environnements PostgreSQL, vous pouvez parfois effectuer ce type de contrôle en modifiant le fichier `pg_hba.conf`. Vous pouvez plutôt utiliser les autorisations de bases de données dans Amazon RDS.

Les nouvelles bases de données dans PostgreSQL sont toujours créées avec un ensemble de privilèges par défaut. Les privilèges par défaut permettent au `PUBLIC` (tous les utilisateurs) de se connecter à la base de données et de créer des tableaux temporaires lorsqu'ils sont connectés.

Afin de contrôler les utilisateurs disposant des accès à une base de données particulière dans Amazon RDS, révoquez d'abord les privilèges `PUBLIC` par défaut. Ensuite, accordez de nouveau les privilèges sur une base plus granulaire. L'exemple de code suivant illustre la marche à suivre.

```
psql> revoke all on database <database-name> from public;
psql> grant connect, temporary on database <database-name> to <user/role name>;
```

Pour plus d'informations sur les privilèges dans les bases de données PostgreSQL, consultez la commande `GRANT` dans la documentation PostgreSQL.

Utilisation des paramètres PostgreSQL

Les paramètres PostgreSQL définis pour une instance PostgreSQL locale dans le fichier postgresql.conf sont conservés dans le groupe de paramètres de base de données de votre instance de base de données. Si vous créez une instance de base de données à l'aide du groupe de paramètres par défaut, les paramètres figurent dans un groupe de paramètres appelé default.postgres9.6.

Lorsque vous créez une instance de base de données, les paramètres du groupe de paramètres DB associé sont chargés. Vous ne pouvez pas modifier de valeurs des paramètres en modifiant des valeurs dans le groupe de paramètres. Vous pouvez également modifier des valeurs de paramètres, si vous disposez des privilèges de sécurité nécessaires, en utilisant les commandes ALTER DATABASE, ALTER ROLE et SET. Vous ne pouvez pas utiliser la commande de ligne de commande `postgres` ou la commande `env PGOPTIONS`, car vous n'aurez pas accès à l'hôte.

Il peut parfois s'avérer difficile de suivre les paramètres PostgreSQL. Utilisez les commandes suivantes pour répertorier les paramètres actuels et leur valeur par défaut.

```
select name, setting, boot_val, reset_val, unit
from pg_settings
order by name;
```

Pour savoir ce que signifient les valeurs de sortie, veuillez consulter la rubrique `pg_settings` dans la documentation PostgreSQL.

Si les paramètres de mémoire sont définis de manière trop large pour `max_connections` ou `shared_buffers`, l'instance PostgreSQL ne pourra pas démarrer. Certains paramètres utilisent des unités que vous pouvez ne pas bien connaître. Par exemple, `shared_buffers` définit le nombre de tampons de mémoire partagée de 8 Ko utilisés par le serveur.

L'erreur suivante est écrite dans le fichier postgres.log lorsque l'instance tente de démarrer, mais des paramètres mal définis empêchent le démarrage.

```
2013-09-18 21:13:15 UTC::@:[8097]:FATAL:  could not map anonymous shared
memory: Cannot allocate memory
2013-09-18 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.
```

Il existe deux types de paramètres PostgreSQL : les paramètres statiques et les paramètres dynamiques. Les paramètres statiques nécessitent le redémarrage de l'instance de base de données avant d'être appliqués. Les paramètres dynamiques peuvent être appliqués immédiatement. Le tableau suivant illustre les paramètres que vous pouvez modifier pour une instance de base de données PostgreSQL, ainsi que tous les types de paramètres.

Nom du paramètre	Type d'application	Description
`application_name`	Dynamique	Définit le nom de l'application à indiquer dans les statistiques et les journaux.
`array_nulls`	Dynamique	Autorise l'entrée d'éléments NULL dans les tableaux.
`authentication_timeout`	Dynamique	Définit le délai maximum autorisé pour procéder à l'authentification du client.
`autovacuum`	Dynamique	Démarre le sous-processus autovacuum.

Nom du paramètre	Type d'application	Description
autovacuum_analyze_scale_factor	Dynamique	Nombre de tuples insérés, mis à jour ou supprimés avant analyse en tant que partie de reltuples.
autovacuum_analyze_threshold	Dynamique	Nombre minimum de tuples insérés, mis à jour ou supprimés avant analyse.
autovacuum_naptime	Dynamique	Temps de repos entre les exécutions autovacuum.
autovacuum_vacuum_cost_delay	Dynamique	Valeur du coût de retard du processus vacuum en millisecondes, pour le processus autovacuum.
autovacuum_vacuum_cost_limit	Dynamique	Coût cumulé qui provoque l'endormissement du processus vacuum, pour le processus autovacuum.
autovacuum_vacuum_scale_factor	Dynamique	Nombre de tuples mis à jour ou supprimés avant le processus vacuum en tant que partie de reltuples.
autovacuum_vacuum_threshold	Dynamique	Nombre de tuples mis à jour ou supprimés avant le processus vacuum.
backslash_quote	Dynamique	Définit si une barre oblique inverse (\) peut être utilisée dans les littéraux de chaîne.
bgwriter_delay	Dynamique	Délai d'inactivité entre les tours d'activité du processus d'écriture en arrière-plan.
bgwriter_lru_maxpages	Dynamique	Nombre maximum de pages récemment utilisées qui peuvent être vidées à chaque tour par le processus d'écriture en tâche de fond.
bgwriter_lru_multiplier	Dynamique	Multiple de l'utilisation moyenne de tampons à libérer par tour.
bytea_output	Dynamique	Configure le format de sortie pour les valeurs de type octets.
check_function_bodies	Dynamique	Vérifie les corps des fonctions pendant la fonction CREATE FUNCTION.
checkpoint_completion_target	Dynamique	Temps nécessaire pour vider les tampons sales au moment de la vérification, sous la forme d'une fraction de temps entre deux points de vérification.
checkpoint_segments	Dynamique	Définit la distance maximale dans les segments de journaux entre deux points de vérification automatique de journal WAL.
checkpoint_timeout	Dynamique	Définit le temps maximum entre deux points de vérification automatique des WAL.
checkpoint_warning	Dynamique	Active les avertissements si des segments de points de vérification sont remplis à une fréquence supérieure à ce paramètre.
client_encoding	Dynamique	Définit l'encodage du jeu de caractères du client.
client_min_messages	Dynamique	Définit les niveaux des messages envoyés au client.

Nom du paramètre	Type d'application	Description
`commit_delay`	Dynamique	Définit la durée, en micro-secondes, entre le déclenchement de la sonde transaction-commit et le vidage de WAL vers le disque.
`commit_siblings`	Dynamique	Définit le nombre minimum de transactions ouvertes simultanément avant d'atteindre le délai commit_delay.
`constraint_exclusion`	Dynamique	Autorise le planificateur à utiliser des contraintes pour optimiser les requêtes.
`cpu_index_tuple_cost`	Dynamique	Définit l'estimation faite par le planificateur du coût de traitement de chaque entrée d'index pendant la vérification d'un index.
`cpu_operator_cost`	Dynamique	Définit l'estimation faite par le planificateur du coût de traitement de chaque opérateur ou appel de fonction.
`cpu_tuple_cost`	Dynamique	Définit l'estimation faite par le planificateur du coût de traitement de chaque ligne.
`cursor_tuple_fraction`	Dynamique	Définit l'estimation faite par le planificateur de la fraction des lignes d'un curseur qui sera récupérée.
`datestyle`	Dynamique	Définit le format d'affichage des valeurs de type date et heure.
`deadlock_timeout`	Dynamique	Définit le délai d'attente au niveau d'un verrou avant blocage.
`debug_pretty_print`	Dynamique	Indente les affichages des arborescence d'analyse et de planification.
`debug_print_parse`	Dynamique	Enregistre l'arborescence d'analyse de chaque requête.
`debug_print_plan`	Dynamique	Enregistre le plan d'exécution de chaque requête.
`debug_print_rewritten`	Dynamique	Enregistre l'arbre d'interprétation réécrit de chaque requête.
`default_statistics_target`	Dynamique	Définit la cible des statistiques par défaut.
`default_tablespace`	Dynamique	Définit l'espace de table par défaut dans lequel créer des tables et des index.
`default_transaction_deferrable`	Dynamique	Définit le statut reportable des nouvelles transactions.
`default_transaction_isolation`	Dynamique	Définit le niveau d'isolation de transaction de chaque nouvelle transaction.
`default_transaction_read_only`	Dynamique	Définit le statut en lecture seule des nouvelles transactions.
`default_with_oids`	Dynamique	Crée des tables avec des OID par défaut.
`effective_cache_size`	Dynamique	Définit l'estimation faite par le planificateur de la taille du cache du disque.

Nom du paramètre	Type d'application	Description
effective_io_concurrency	Dynamique	Nombre de demandes simultanées pouvant être traitées de manière efficace par le sous-système du disque.
enable_bitmapscan	Dynamique	Autorise l'utilisation de plans de parcours de bitmap par le planificateur.
enable_hashagg	Dynamique	Autorise l'utilisation de plans d'agrégation hachée par le planificateur.
enable_hashjoin	Dynamique	Autorise l'utilisation de plans de jointures de hachage par le planificateur.
enable_indexscan	Dynamique	Autorise l'utilisation de plans de parcours d'index par le planificateur.
enable_material	Dynamique	Autorise l'utilisation de la matérialisation par le planificateur.
enable_mergejoin	Dynamique	Autorise l'utilisation de plans de jointures de fusion par le planificateur.
enable_nestloop	Dynamique	Autorise l'utilisation de plans de jointures de boucles imbriquées par le planificateur.
enable_seqscan	Dynamique	Autorise l'utilisation de plans de parcours séquentiels par le planificateur.
enable_sort	Dynamique	Autorise l'utilisation des étapes de tri explicite par le planificateur.
enable_tidscan	Dynamique	Autorise l'utilisation de plans de parcours de TID par le planificateur.
escape_string_warning	Dynamique	Avertit sur l'utilisation des barres obliques inverses (\) dans des littéraux de chaîne ordinaires.
extra_float_digits	Dynamique	Définit le nombre de chiffres affichés pour les valeurs à virgule flottante.
from_collapse_limit	Dynamique	Définit la taille FROM-list au-delà de laquelle les sous-requêtes ne sont pas regroupées.
fsync	Dynamique	Force la synchronisation des mises à jour sur le disque.
full_page_writes	Dynamique	Ecrit les pages complètes dans les WAL lors de la première modification après un point de vérification.
geqo	Dynamique	Active l'optimisation génétique des requêtes.
geqo_effort	Dynamique	geqo_effort est utilisé pour définir la valeur par défaut pour les autres paramètres GEQO.
geqo_generations	Dynamique	GEQO : nombre d'itérations de l'algorithme.
geqo_pool_size	Dynamique	GEQO : nombre d'individus au sein d'une population.

Nom du paramètre	Type d'application	Description
geqo_seed	Dynamique	GEQO : valeur initiale pour la sélection des chemins au hasard.
geqo_selection_bias	Dynamique	GEQO : pression de sélectivité au sein de la population.
geqo_threshold	Dynamique	Définit le seuil d'éléments FROM au-delà duquel GEQO est utilisé.
gin_fuzzy_search_limit	Dynamique	Définit le résultat maximum autorisé pour la recherche exacte par GIN.
hot_standby_feedback	Dynamique	Détermine si une instance de secours envoie des messages de commentaire aux instances principales ou de veille en amont.
intervalstyle	Dynamique	Définit le format d'affichage des valeurs de type intervalle.
join_collapse_limit	Dynamique	Définit la taille FROM-list au-delà de laquelle les constructions JOIN ne sont pas mises à plat.
lc_messages	Dynamique	Définit la langue d'affichage des messages.
lc_monetary	Dynamique	Définit la locale à utiliser pour le formatage des montants monétaires.
lc_numeric	Dynamique	Définit la locale à utiliser pour le formatage des nombres.
lc_time	Dynamique	Définit la locale à utiliser pour le formatage des valeurs de date et d'heure.
log_autovacuum_min_duration	Dynamique	Définit la durée minimum d'exécution au-delà de laquelle les actions autovacuum seront enregistrées.
log_checkpoints	Dynamique	Enregistre les points de vérification.
log_connections	Dynamique	Enregistre toutes les connexions réussies.
log_disconnections	Dynamique	Enregistre la fin d'une session, y compris sa durée.
log_duration	Dynamique	Enregistre la durée de chaque instruction SQL terminée.
log_error_verbosity	Dynamique	Définit la quantité de détails dans les messages enregistrés.
log_executor_stats	Dynamique	Ecrit les statistiques de performance de l'exécuteur dans le journal du serveur.
log_filename	Dynamique	Définit le modèle de nom de fichier pour les fichiers journaux.
log_hostname	Dynamique	Enregistre le nom de l'hôte dans les journaux de connexion.

Nom du paramètre	Type d'application	Description
`log_lock_waits`	Dynamique	Enregistre les longs temps d'attente pour l'acquisition d'un verrou.
`log_min_duration_statement`	Dynamique	Définit la durée minimum d'exécution au-delà de laquelle les instructions seront enregistrées.
`log_min_error_statement`	Dynamique	Déclenche l'enregistrement de toutes les instructions générant une erreur à ce niveau ou à un niveau supérieur.
`log_min_messages`	Dynamique	Définit les niveaux des messages qui sont enregistrés.
`log_parser_stats`	Dynamique	Ecrit les statistiques de performance de l'analyseur dans le journal du serveur.
`log_planner_stats`	Dynamique	Ecrit les statistiques de performance du planificateur dans le journal du serveur.
`log_rotation_age`	Dynamique	Déclenchement de la rotation de fichier journal automatique au-delà d'un délai de N minutes.
`log_rotation_size`	Dynamique	Déclenchement de la rotation de fichier journal automatique au-delà de N kilo-octets.
`log_statement`	Dynamique	Définit le type d'instructions enregistrées.
`log_statement_stats`	Dynamique	Ecrit les statistiques de performance cumulées dans le journal du serveur.
`log_temp_files`	Dynamique	Enregistre l'utilisation des fichiers temporaires dont la taille est supérieure à cette taille en kilo-octets.
`maintenance_work_mem`	Dynamique	Définit la quantité maximum de mémoire que peuvent utiliser les opérations de maintenance.
`max_stack_depth`	Dynamique	Définit la profondeur maximum de la pile, en kilo-octets.
`max_standby_archive_delay`	Dynamique	Définit le délai maximum avant l'annulation des requêtes lorsqu'un serveur hot standby traite des données WAL archivées.
`max_standby_streaming_delay`	Dynamique	Définit le délai maximum avant l'annulation des requêtes lorsqu'un serveur hot standby traite des données WAL diffusées.
`max_wal_size`	Statique	Définit la taille de journal WAL qui déclenche le point de vérification. Pour PostgreSQL version 9.6 ou antérieure, la taille `max_wal_size` est exprimée en unités de 16 Mo. Pour PostgreSQL version 10 ou supérieure, la taille `max_wal_size` est exprimée en unités de 1 Mo.

Nom du paramètre	Type d'application	Description
`min_wal_size`	Statique	Définit la taille minimale à laquelle réduire le journal WAL. Pour PostgreSQL version 9.6 ou antérieure, la taille `min_wal_size` est exprimée en unités de 16 Mo. Pour PostgreSQL version 10 ou supérieure, la taille `min_wal_size` est exprimée en unités de 1 Mo.
`quote_all_identifiers`	Dynamique	Ajoute des guillemets (") à tous les identificateurs lors de la génération de fragments SQL.
`random_page_cost`	Dynamique	Définit l'estimation faite par le planificateur du coût d'une page de disque extraite de façon non séquentielle.
`rds.adaptive_autovacuum`	Dynamique	Règle automatiquement les paramètres d'autovacuum chaque fois que les seuils d'ID de transaction sont dépassés.
`rds.log_retention_period`	Dynamique	Définit la rétention des journaux de telle manière qu'Amazon RDS supprime les journaux PostgreSQL antérieurs à N minutes.
`rds.restrict_password_commands`	Statique	Limite la gestion des mots de passe aux utilisateurs auxquels le rôle `rds_password` a été affecté. Pour la restriction par mot de passe, définissez ce paramètre sur 1. La valeur par défaut est 0.
`search_path`	Dynamique	Définit l'ordre de recherche des schémas pour les noms pour lesquels le schéma n'est pas précisé.
`seq_page_cost`	Dynamique	Définit l'estimation faite par le planificateur du coût d'une page de disque extraite de façon séquentielle.
`session_replication_role`	Dynamique	Définit le comportement des sessions concernant les déclencheurs et les règles de réécriture.
`sql_inheritance`	Dynamique	Entraîne l'ajout par défaut de sous-tables dans plusieurs commandes.
`ssl_renegotiation_limit`	Dynamique	Définit la quantité de trafic à envoyer et recevoir avant de renégocier les clés de chiffrement.
`standard_conforming_strings`	Dynamique	Entraîne les chaînes ... à traiter littéralement les barres obliques inverses.
`statement_timeout`	Dynamique	Définit la durée maximum de toute instruction.
`synchronize_seqscans`	Dynamique	Active les analyses séquentielles synchronisées.
`synchronous_commit`	Dynamique	Définit le niveau de synchronisation des transactions actuelles.
`tcp_keepalives_count`	Dynamique	Nombre maximum de paquets TCP keepalive.
`tcp_keepalives_idle`	Dynamique	Délai entre les émissions de paquets TCP keepalive.
`tcp_keepalives_interval`	Dynamique	Délai entre les envois de paquets TCP keepalive.

Nom du paramètre	Type d'application	Description
`temp_buffers`	Dynamique	Définit le nombre maximum de tampons temporaires utilisés par chaque session.
`temp_tablespaces`	Dynamique	Définit l'espace de table à utiliser pour les tables et fichiers de tri temporaires.
`timezone`	Dynamique	Définit le fuseau horaire pour l'affichage et l'interprétation de la date et de l'heure.
`track_activities`	Dynamique	Collecte des informations sur les commandes en cours d'exécution.
`track_counts`	Dynamique	Active la collecte de statistiques sur l'activité de la base de données.
`track_functions`	Dynamique	Active la collecte de statistiques au niveau de la fonction sur l'activité de la base de données.
`track_io_timing`	Dynamique	Active la collecte de statistiques de durée sur l'activité I/O de la base de données.
`transaction_deferrable`	Dynamique	Indique si une transaction sérialisable en lecture seule doit être différée jusqu'à ce qu'elle puisse être démarrée sans échec de sérialisation possible.
`transaction_isolation`	Dynamique	Définit le niveau d'isolation des transactions actuelles.
`transaction_read_only`	Dynamique	Définit le statut en lecture seule des transactions actuelles.
`transform_null_equals`	Dynamique	Traite l'expression =NULL en tant que IS NULL.
`update_process_title`	Dynamique	Met à jour le titre du processus pour indiquer la commande SQL active.
`vacuum_cost_delay`	Dynamique	Valeur du coût de délai du processus vacuum en millisecondes.
`vacuum_cost_limit`	Dynamique	Coût cumulé qui provoque l'endormissement du processus vacuum.
`vacuum_cost_page_dirty`	Dynamique	Coût du processus vacuum pour une page salie par le processus vacuum.
`vacuum_cost_page_hit`	Dynamique	Coût du processus vacuum pour une page trouvée dans le cache des tampons.
`vacuum_cost_page_miss`	Dynamique	Coût du processus vacuum pour une page non trouvée dans le cache des tampons.
`vacuum_defer_cleanup_age`	Dynamique	Nombre de transactions pendant lesquelles le processus vacuum et le nettoyage hot seront reportés à plus tard, le cas échéant.
`vacuum_freeze_min_age`	Dynamique	Âge limite auquel le processus vacuum doit figer une ligne de tableau.

Nom du paramètre	Type d'application	Description
`vacuum_freeze_table_age`	Dynamique	Âge auquel le processus vacuum effectue une analyse complète de la table pour figer des lignes.
`wal_writer_delay`	Dynamique	Délai d'inactivité de l'enregistreur des WAL entre les actions de vidage WAL.
`work_mem`	Dynamique	Définit la quantité maximum de mémoire que peuvent utiliser les espaces de travail des requêtes.
`xmlbinary`	Dynamique	Définit la façon dont les valeurs binaires doivent être codées en XML.
`xmloption`	Dynamique	Définit si des données XML dans des opérations d'analyse ou de sérialisation implicites doivent être considérées comme des documents ou des fragments de contenu.
`autovacuum_freeze_max_age`	Statique	Âge auquel lancer le processus autovacuum sur une table pour empêcher le renvoi à la ligne de l'ID de transaction.
`autovacuum_max_workers`	Statique	Définit le nombre maximum de processus autovacuum qui peuvent être exécutés simultanément.
`max_connections`	Statique	Définit le nombre maximum de connexions simultanées.
`max_files_per_process`	Statique	Définit le nombre maximum de fichiers ouverts simultanément pour chaque processus serveur.
`max_locks_per_transaction`	Statique	Définit le nombre maximum de verrous par transaction.
`max_pred_locks_per_transaction`	Statique	Définit le nombre maximum de verrous de prédicat par transaction.
`max_prepared_transactions`	Statique	Définit le nombre maximum de transactions préparées simultanément.
`shared_buffers`	Statique	Définit le nombre de tampons de mémoire partagée utilisés par le serveur.
`ssl`	Statique	Active les connexions SSL.
`temp_file_limit`	Statique	Définit la taille maximale en Ko que peuvent atteindre les fichiers temporaires.
`track_activity_query_size`	Statique	Définit la taille réservée pour pg_stat_activity.current_query, en octets.
`wal_buffers`	Statique	Définit le nombre de tampons de page de disque dans la mémoire partagée pour les WAL.

Amazon RDS utilise les unités PostgreSQL par défaut pour tous les paramètres. Le tableau suivant indique l'unité et la valeur PostgreSQL par défaut de chaque paramètre.

Nom du paramètre	Unité
effective_cache_size	8 Ko
segment_size	8 Ko
shared_buffers	8 Ko
temp_buffers	8 Ko
wal_buffers	8 Ko
wal_segment_size	8 Ko
log_rotation_size	Ko
log_temp_files	Ko
maintenance_work_mem	Ko
max_stack_depth	Ko
ssl_renegotiation_limit	Ko
temp_file_limit	Ko
work_mem	Ko
log_rotation_age	minutes
autovacuum_vacuum_cost_delay	ms
bgwriter_delay	ms
deadlock_timeout	ms
lock_timeout	ms
log_autovacuum_min_duration	ms
log_min_duration_statement	ms
max_standby_archive_delay	ms
max_standby_streaming_delay	ms
statement_timeout	ms
vacuum_cost_delay	ms
wal_receiver_timeout	ms
wal_sender_timeout	ms
wal_writer_delay	ms
archive_timeout	s
authentication_timeout	s
autovacuum_naptime	s
checkpoint_timeout	s

Nom du paramètre	Unité
checkpoint_warning	s
post_auth_delay	s
pre_auth_delay	s
tcp_keepalives_idle	s
tcp_keepalives_interval	s
wal_receiver_status_interval	s

Utilisation de la fonction autovacuum de PostgreSQL sur Amazon RDS

Nous vous conseillons vivement d'utiliser la fonction autovacuum pour les bases de données PostgreSQL afin de maintenir l'intégrité de votre instance de base de données PostgreSQL. La fonction autovacuum automatise le lancement des commandes VACUUM et ANALYZE. Elle recherche les tables ayant eu un grand nombre de tuples insérés, mis à jour ou supprimés. Elle récupère alors le stockage en supprimant les données et les tuples obsolètes de la base de données PostgreSQL.

La fonction autovacuum est activée par défaut pour toutes les nouvelles instances de base de données Amazon RDS PostgreSQL, et les paramètres de configuration associés sont configurés par défaut de manière appropriée. Comme nos valeurs par défaut sont relativement génériques, vous pouvez bénéficier du réglage des paramètres en fonction de votre charge de travail spécifique. La section suivante peut vous aider à effectuer l'ajustement nécessaire d'autovacuum.

Rubriques

- Allocation de mémoire pour la fonction autovacuum (p. 1431)
- Réduction de la probabilité de renvoi à la ligne de l'ID de transaction (p. 1432)
- Déterminer si les tables de votre base de données ont besoin d'une opération VACUUM (p. 1433)
- Déterminer les tables actuellement éligibles pour autovacuum (p. 1434)
- Déterminer si autovacuum est en cours d'exécution et pour combien de temps (p. 1435)
- Réalisation d'un gel manuel du processus vacuum (p. 1436)
- Réindexation d'une table pendant l'exécution du processus autovacuum (p. 1438)
- Autres paramètres qui affectent la fonction d'autovacuum (p. 1438)
- Définition des paramètres d'autovacuum au niveau de la table (p. 1439)
- Journalisation d'autovacuum (p. 1439)

Allocation de mémoire pour la fonction autovacuum

L'un des paramètres les plus importants qui influencent les performances d'autovacuum est `maintenance_work_mem`. Ce paramètre détermine la quantité de mémoire que vous allouez à autovacuum pour analyser une table de base de données et conserver tous les ID des lignes qui vont faire l'objet d'une opération VACUUM. Si vous définissez une valeur trop basse du paramètre `maintenance_work_mem`, le processus vacuum pourrait avoir à analyser la table plusieurs fois pour effectuer son travail. Ces nombreuses analyses peuvent avoir un impact négatif sur les performances.

Lorsque vous faites des calculs pour déterminer la valeur du paramètre `maintenance_work_mem`, gardez les deux choses suivantes à l'esprit :

- L'unité par défaut est le kilo-octet (Ko) pour ce paramètre.
- Le paramètre `maintenance_work_mem` fonctionne conjointement avec le paramètre `autovacuum_max_workers`. Si vous disposez de plusieurs petites tables, allouez plus de `autovacuum_max_workers` et moins de `maintenance_work_mem`. Si vous avez de grandes tables (par exemple, d'une taille supérieure à 100 Go), allouez plus de mémoire et moins de processus de travail. Vous devez avoir alloué suffisamment de mémoire pour pouvoir prendre en charge votre plus grande table. Chaque `autovacuum_max_workers` peut utiliser la mémoire que vous allouez. Ainsi, vous devez vous assurer que la combinaison des processus de travail et de la mémoire est égale à la mémoire totale que vous souhaitez allouer.

De manière générale, pour les hôtes volumineux, affectez au paramètre `maintenance_work_mem` une valeur comprise entre un et deux gigaoctets (entre 1 048 576 et 2 097 152 Ko). Pour les hôtes extrêmement volumineux, affectez à ce paramètre une valeur comprise entre deux et quatre gigaoctets (entre 2 097 152 et 4 194 304 Ko). La valeur que vous définissez pour ce paramètre doit dépendre de la charge de travail. Amazon RDS a mis à jour sa valeur par défaut pour ce paramètre en un nombre de kilo-octets calculé comme suit :

```
GREATEST({DBInstanceClassMemory/63963136*1024},65536).
```

Réduction de la probabilité de renvoi à la ligne de l'ID de transaction

Dans certains cas, les valeurs du groupe de paramètres associées à la fonction autovacuum peuvent ne pas être suffisamment agressives pour empêcher le renvoi à la ligne de l'ID de transaction. Pour résoudre ce problème, Amazon RDS pour PostgreSQL fournit un mécanisme qui adapte automatiquement les valeurs des paramètres de la fonction autovacuum. Le réglage adaptatif des paramètres d'autovacuum est une fonction pour RDS for PostgreSQL. Une explication détaillée du renvoi à la ligne de l'ID de transaction figure dans la documentation PostgreSQL.

Le réglage adaptatif des paramètres d'autovacuum est activé par défaut pour les instances RDS PostgreSQL avec le paramètre dynamique `rds.adaptive_autovacuum` défini sur ON. Nous vous recommandons vivement de garder cette option activée. Toutefois, pour désactiver le réglage adaptatif des paramètres d'autovacuum, définissez le paramètre `rds.adaptive_autovacuum` sur 0 ou OFF.

Le renvoi à la ligne de l'ID de transaction est encore possible même lorsque RDS règle les paramètres d'autovacuum. Nous vous encourageons à implémenter une alarme Amazon CloudWatch pour le renvoi à la ligne de l'ID de transaction. Pour de plus amples informations, veuillez consulter le billet de blog Implement an Early Warning System for Transaction ID Wraparound in Amazon RDS for PostgreSQL.

Lorsque le réglage adaptatif des paramètres d'autovacuum est activé, RDS commence à ajuster les paramètres d'autovacuum lorsque la métrique CloudWatch `MaximumUsedTransactionIDs` atteint la valeur du paramètre `autovacuum_freeze_max_age` ou 500 000 000, quelle que soit la valeur la plus élevée.

RDS continue à ajuster les paramètres pour la fonction d'autovacuum si une table continue à s'orienter vers le renvoi à la ligne de l'ID de transaction. Chacun de ces ajustements dédie plus de ressources à la fonction d'autovacuum pour éviter le renvoi à la ligne. RDS met à jour les paramètres suivants associés à la fonction d'autovacuum :

- autovacuum_vacuum_cost_delay
- autovacuum_vacuum_cost_limit
- autovacuum_work_mem
- autovacuum_naptime

RDS modifie ces paramètres seulement si la nouvelle valeur rend la fonction d'autovacuum plus agressive. Ces paramètres sont modifiés dans la mémoire sur l'instance de base de données. Les valeurs figurant

dans le groupe de paramètres ne sont pas modifiées. Pour afficher les paramètres en mémoire actuels, utilisez la commande SQL SHOW de PostgreSQL.

Chaque fois que RDS modifie certains de ces paramètres d'autovacuum, il génère un événement pour l'instance de base de données affectée qui est visible sur la AWS Management Console (https://console.aws.amazon.com/rds/) et via l'API RDS. Une fois que la métrique CloudWatch `MaximumUsedTransactionIDs` est repassée sous le seuil, RDS réinitialise les paramètres associés à la fonction d'autovacuum en mémoire en rétablissant les valeurs spécifiées dans le groupe de paramètres, et génère un autre événement correspondant à ce changement.

Déterminer si les tables de votre base de données ont besoin d'une opération VACUUM

Vous pouvez utiliser la requête suivante pour afficher le nombre de transactions non vidées dans une base de données. La colonne `datfrozenxid` de la ligne `pg_database` d'une base de données est une limite inférieure appliquée aux ID de transaction normaux qui apparaissent dans cette base de données. Cette colonne représente le minimum des valeurs `relfrozenxid` par table au sein de la base de données.

```
SELECT datname, age(datfrozenxid) FROM pg_database ORDER BY age(datfrozenxid) desc limit
 20;
```

Par exemple, les résultats de l'exécution de la requête précédente pourraient être les suivants.

```
datname    | age
mydb       | 1771757888
template0  | 1721757888
template1  | 1721757888
rdsadmin   | 1694008527
postgres   | 1693881061
(5 rows)
```

Lorsque l'âge d'une base de données atteint 2 milliards d'ID de transactions, un renvoi à la ligne de l'ID de transaction (XID) se produit et la base de données passe en lecture seule. Cette requête peut servir à produire une métrique et être exécutée plusieurs fois par jour. Par défaut, autovacuum est défini pour conserver un âge de transactions inférieur à 200 000 000 (`autovacuum_freeze_max_age`).

Un exemple de stratégie de surveillance peut ressembler à ceci :

- Définissez la valeur `autovacuum_freeze_max_age` sur 200 millions de transactions.
- Si une table atteint les 500 millions de transactions non vidées, elle déclenche une alarme de faible gravité. Ce n'est pas une valeur déraisonnable, mais elle peut indiquer que la fonction d'autovacuum ne suit pas.
- Si l'âge d'une table atteint 1 milliard, cela doit être considéré comme une alarme exigeant une action. En général, il est conseillé de conserver des âges plus proches de `autovacuum_freeze_max_age` pour des raisons de performances. Nous vous recommandons d'enquêter en appliquant les recommandations suivantes.
- Si une table atteint les 1,5 million de transactions non vidées, elle déclenche une alarme de haute gravité. En fonction de la vitesse à laquelle votre base de données utilise les ID de transaction, cette alarme peut indiquer que le système n'a presque plus de temps pour exécuter le processus d'autovacuum. Dans ce cas, nous vous recommandons de résoudre cela immédiatement.

Si une table enfreint constamment ces seuils, vous devez continuer à modifier vos paramètres d'autovacuum. Par défaut, l'utilisation manuelle de VACUUM (pour lequel les retards basés sur les coûts sont désactivés) est plus agressive que le processus d'autovacuum par défaut, mais elle est également plus intrusive pour le système dans son ensemble.

Nous vous recommandons la procédure suivante :

- Gardez tout cela à l'esprit et activez un mécanisme de surveillance afin de connaître l'âge de vos transactions les plus anciennes.

  Pour de plus amples informations sur la création d'un processus qui vous avertisse d'un renvoi à la ligne de l'ID de transaction, veuillez consulter le billet de blog AWS consacré aux bases de données Implement an Early Warning System for Transaction ID Wraparound in Amazon RDS for PostgreSQL.
- Pour les tables plus occupées, procédez régulièrement au gel manuel du processus de vacuum pendant une fenêtre de maintenance, en plus de compter sur la fonction d'autovacuum. Pour de plus amples informations sur le gel manuel du processus vacuum, veuillez consulter Réalisation d'un gel manuel du processus vacuum (p. 1436).

Déterminer les tables actuellement éligibles pour autovacuum

Souvent, une ou deux tables ont besoin d'une opération VACUUM. Les tables dont la valeur `relfrozenxid` est supérieure au nombre de transactions dans `autovacuum_freeze_max_age` sont toujours ciblées par la fonction d'autovacuum. Sinon, si le nombre de tuples rendus obsolètes depuis la dernière opération VACUUM dépasse le « seuil de vacuum », la table est vidée.

Le seuil d'autovacuum est défini comme suit :

```
Vacuum-threshold = vacuum-base-threshold + vacuum-scale-factor * number-of-tuples
```

Pendant que vous êtes connecté à votre base de données, exécutez la requête suivante pour afficher la liste des tables qu'autovacuum considère comme éligibles pour une action « vacuum » :

```
  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 cvsf on cvsf.param = 'autovacuum_vacuum_scale_factor' and
c.oid = cvsf.opt_oid
left join sto cfma on cfma.param = 'autovacuum_freeze_max_age' and
c.oid = cfma.opt_oid
WHERE c.relkind = 'r' and 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(cvsf.value::float,autovacuum_vacuum_scale_factor::float) *
c.reltuples <= n_dead_tup
   -- or 1 = 1
)
ORDER BY age(relfrozenxid) DESC LIMIT 50;
```

Déterminer si autovacuum est en cours d'exécution et pour combien de temps

Si vous avez besoin de vider manuellement une table, vous devez déterminer si autovacuum est en cours d'exécution. Si c'est le cas, vous devrez peut-être ajuster les paramètres pour le faire fonctionner plus efficacement, ou mettre fin à autovacuum afin de pouvoir exécuter manuellement VACUUM.

Utilisez la requête suivante pour déterminer si autovacuum est en cours d'exécution, pendant combien de temps il a été en cours d'exécution et s'il est en attente sur une autre session.

Si vous utilisez Amazon RDS PostgreSQL 9.6+ ou versions ultérieures, utilisez la requête suivante :

```
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;
```

Après l'exécution de la requête, vous devez obtenir un résultat similaire à ce qui suit.

```
 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
       +
         |          |       |        |            |                         | WHERE query
 like '%VACUUM%'
 +
         |          |       |        |            |                         | ORDER BY
 xact_start;
   +
```

Si vous utilisez une version Amazon RDS for PostgreSQL antérieure à la version 9.6, utilisez la requête suivante.

```
SELECT datname, usename, pid, waiting, current_timestamp - xact_start AS xact_runtime,
 query
FROM pg_stat_activity
```

```
WHERE upper(query) LIKE '%VACUUM%'
ORDER BY xact_start;
```

Après l'exécution de la requête, vous devez obtenir un résultat similaire à ce qui suit.

```
 datname | usename  |  pid  | waiting |       xact_runtime      | query
 --------+----------+-------+---------+-------------------------
+-----------------------------------------------------------------------------------------------
 mydb    | rdsadmin | 16473 | f       | 33 days 16:32:11.600656 | autovacuum: VACUUM
 ANALYZE public.mytable1 (to prevent wraparound)
 mydb    | rdsadmin | 22553 | f       | 14 days 09:15:34.073141 | autovacuum: VACUUM
 ANALYZE public.mytable2 (to prevent wraparound)
 mydb    | rdsadmin | 41909 | f       | 3 days 02:43:54.203349  | autovacuum: VACUUM
 ANALYZE public.mytable3
 mydb    | rdsadmin |   618 | f       | 00:00:00                | SELECT datname, usename,
 pid, waiting, current_timestamp - xact_start AS xact_runtime, query+
         |          |       |         |                         | FROM pg_stat_activity
                                                                   +
         |          |       |         |                         | WHERE query like '%VACUUM
%'                                                                 +
         |          |       |         |                         | ORDER BY xact_start;
                                                                   +
```

Plusieurs problèmes peuvent occasionner des longueurs d'exécution (plusieurs jours) d'une session autovacuum. Le problème le plus courant est que la valeur de votre paramètre `maintenance_work_mem` est trop basse pour la taille de la table ou pour la fréquence des mises à jour.

Nous vous recommandons d'utiliser la formule suivante pour définir la valeur du paramètre `maintenance_work_mem`.

```
GREATEST({DBInstanceClassMemory/63963136*1024},65536)
```

De courtes sessions autovacuum peuvent également indiquer des problèmes :

- Cela peut indiquer un nombre `autovacuum_max_workers` insuffisant pour votre charge de travail. Dans ce cas, vous devez indiquer le nombre d'exécutants.
- Cela peut indiquer une corruption d'index (la fonction d'autovacuum se bloque et redémarre sur la même relation, mais ne progresse pas). Dans ce cas, exécutez un gel manuel du processus vacuum en mode détaillé sur ___table___ pour voir la cause exacte.

Réalisation d'un gel manuel du processus vacuum

Vous pouvez effectuer un gel manuel sur une table pour laquelle un processus vacuum est déjà en cours. C'est utile si vous avez identifié une table avec un âge proche de 2 milliards de transactions (ou supérieur à tous les seuils que vous surveillez).

Les étapes suivantes sont fournies à titre informatif et il existe plusieurs variantes de ce processus. Par exemple, pendant le test, supposons que vous trouviez que la valeur du paramètre `maintenance_work_mem` a été définie trop bas et que vous devez agir immédiatement sur une table. Toutefois, vous ne voulez pas renvoyer l'instance à l'expéditeur pour le moment. À l'aide des requêtes des sections précédentes, vous déterminez quelle table pose problème et remarquez une session autovacuum en cours d'exécution depuis longtemps. Vous savez que vous devez modifier le paramètre `maintenance_work_mem`, mais vous devez également agir immédiatement et effectuer un processus vacuum sur la table concernée. La procédure suivante montre ce que vous devez faire dans cette situation :

Pour procéder manuellement au gel du processus vacuum

1. Ouvrez les deux sessions de la base de données contenant la table sur laquelle vous voulez effectuer le processus vacuum. Pour la seconde session, utilisez « écran » ou un autre utilitaire qui gère la session si votre connexion est abandonnée.
2. Dans la première session, obtenez le PID de la session autovacuum en cours d'exécution sur la table.

   Exécutez la requête suivante pour obtenir le PID de la session autovacuum.

```
SELECT datname, usename, pid, current_timestamp - xact_start
AS xact_runtime, query
FROM pg_stat_activity WHERE upper(query) LIKE '%VACUUM%' ORDER BY
xact_start;
```

3. Dans la deuxième session, calculez la quantité de mémoire dont vous avez besoin pour cette opération. Dans cet exemple, nous déterminons que nous pouvons nous permettre d'utiliser jusqu'à 2 Go de mémoire pour cette opération. Nous affectons donc 2 Go à `maintenance_work_mem` pour la session en cours.

```
set maintenance_work_mem='2 GB';
SET
```

4. Dans la deuxième session, émettez une commande `vacuum freeze verbose` pour la table. Le paramètre de mode détaillé est utile, car il vous permet de voir l'activité bien qu'il n'existe actuellement aucun rapport d'avancement de cette opération dans PostgreSQL.

```
\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. Dans la première session, si autovacuum provoquait un blocage, vous voyez dans `pg_stat_activity` que l'attente a la valeur « T » pour votre session vacuum. Dans ce cas, vous devez mettre fin au processus autovacuum comme suit.

```
SELECT pg_terminate_backend('the_pid');
```

6. À ce stade, votre session commence. Il est important de noter que la fonction d'autovacuum redémarre immédiatement parce que cette table figure probablement tout en haut de sa liste de tâches. Lancez votre commande `vacuum freeze verbose` dans la session 2, puis terminez le processus autovacuum de la session 1.

Réindexation d'une table pendant l'exécution du processus autovacuum

Si un index a été corrompu, la fonction d'autovacuum continue à traiter la table et échoue. Si vous essayez d'effectuer un processus vacuum manuel dans cette situation, vous recevez un message d'erreur similaire à ce qui suit :

```
mydb=# vacuum freeze pgbench_branches;
ERROR: index "pgbench_branches_test_index" contains unexpected
   zero page at block 30521
HINT: Please REINDEX it.
```

Lorsque l'index est corrompu et que la fonction d'autovacuum tente de s'exécuter sur la table, vous vous heurtez à une session autovacuum déjà en cours d'exécution. Lorsque vous émettez une commande « REINDEX », vous retirez un verrou exclusif sur la table. Les opérations d'écriture sont bloquées, ainsi que les opérations de lecture qui utilisent cet index spécifique.

Pour réindexer une table lorsque la fonction d'autovacuum est en cours d'exécution sur la table

1. Ouvrez les deux sessions de la base de données contenant la table sur laquelle vous voulez effectuer le processus vacuum. Pour la seconde session, utilisez « écran » ou un autre utilitaire qui gère la session si votre connexion est abandonnée.
2. Dans la première session, obtenez le PID de la session autovacuum en cours d'exécution sur la table.

   Exécutez la requête suivante pour obtenir le PID de la session autovacuum.

   ```
   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. Dans la deuxième session, émettez la commande reindex.

   ```
   \timing on
   Timing is on.
   reindex index pgbench_branches_test_index;
   REINDEX
   Time: 9.966 ms
   ```
4. Dans la première session, si autovacuum provoquait un blocage, vous voyez dans `pg_stat_activity` que l'attente a la valeur « T » pour votre session vacuum. Dans ce cas, vous devez mettre fin au processus autovacuum.

   ```
   select pg_terminate_backend('the_pid');
   ```
5. À ce stade, votre session commence. Il est important de noter que la fonction d'autovacuum redémarre immédiatement parce que cette table figure probablement tout en haut de sa liste de tâches. Lancez votre commande dans la session 2, puis terminez le processus autovacuum dans la session 1.

Autres paramètres qui affectent la fonction d'autovacuum

Cette requête affiche les valeurs de certains des paramètres qui ont un impact direct sur la fonction d'autovacuum et son comportement. Les paramètres d'autovacuum sont décrits en détails dans la documentation PostgreSQL.

```
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');
```

Tous ces paramètres affectent la fonction d'autovacuum, mais les plus importants sont :

- maintenance_work_mem
- autovacuum_freeze_max_age
- autovacuum_max_workers
- autovacuum_vacuum_cost_delay
- autovacuum_vacuum_cost_limit

Définition des paramètres d'autovacuum au niveau de la table

Les paramètres de stockage liés à la fonction d'autovacuum peuvent être définis au niveau de la table, ce qui peut être plus judicieux que de modifier le comportement de toute la base de données. Pour les grandes tables, vous devrez peut-être définir des paramètres agressifs et il est déconseillé de faire en sorte que la fonction d'autovacuum se comporte de cette manière pour toutes les tables.

La requête suivante affiche les tables qui ont actuellement des options en place au niveau de la table.

```
SELECT relname, reloptions
FROM pg_class
WHERE reloptions IS NOT null;
```

Par exemple, cela peut être utile sur les tables qui sont beaucoup plus grandes que le reste de vos tables. Supposez que vous avez une table de 300 Go et 30 autres tables de moins de 1 Go. Dans ce cas, vous pouvez définir des paramètres spécifiques pour votre grande table afin de ne pas modifier le comportement de l'intégralité de votre système.

```
ALTER TABLE mytable set (autovacuum_vacuum_cost_delay=0);
```

Cela permet de désactiver le retard d'autovacuum basé sur les coûts pour cette table au détriment d'une plus grande utilisation des ressources sur votre système. Normalement, autovacuum s'arrête pour autovacuum_vacuum_cost_delay chaque fois qu'autovacuum_cost_limit est atteint. Pour plus d'informations, consultez la documentation PostgreSQL concernant le processus de vacuum basé sur les coûts.

Journalisation d'autovacuum

Par défaut, postgresql.log ne contient pas d'informations sur le processus autovacuum. Vous pouvez voir la sortie dans le journal des erreurs PostgreSQL à partir des opérations de l'exécutant autovacuum en définissant le paramètre `rds.force_autovacuum_logging_level`. Les valeurs autorisées sont

`disabled`, `debug5`, `debug4`, `debug3`, `debug2`, `debug1`, `info`, `notice`, `warning`, `error`, `log`, `fatal`, et `panic`. La valeur par défaut est `disabled` parce que les autres valeurs autorisées peuvent ajouter une quantité importante d'informations à vos journaux.

Nous vous recommandons de définir la valeur du paramètre `rds.force_autovacuum_logging_level` sur `log` et d'affecter au paramètre `log_autovacuum_min_duration` une valeur comprise entre 1 000 et 5 000 millisecondes. Si vous définissez cette valeur sur 5 000, Amazon RDS écrit toute activité de plus de cinq secondes dans le journal. Il affiche également des messages « action vacuum ignorée » lorsque des tables sont intentionnellement ignorées en raison du verrouillage de l'application. Si vous voulez résoudre un problème et que vous avez besoin de plus de détails, vous pouvez utiliser une autre valeur de niveau de journalisation, telle que `debug1` ou `debug3`. Utilisez ces paramètres de débogage pendant une courte période de temps, car ils produisent un contenu extrêmement détaillé écrit dans le fichier journal des erreurs. Pour plus d'informations sur ces paramètres de débogage, consultez la documentation PostgreSQL.

> **Note**
>
> PostgreSQL permet au compte `rds_superuser` d'afficher les sessions autovacuum dans `pg_stat_activity`. Par exemple, vous pouvez identifier et mettre fin à la session qui bloque l'exécution d'une commande ou empêche la commande de s'exécuter plus lentement qu'une commande vacuum exécutée manuellement.

Journalisation d'audit pour une instance de base de données PostgreSQL

Plusieurs paramètres vous permettent de définir la consignation de l'activité qui se produit sur votre instance de base de données PostgreSQL. Ces paramètres sont les suivants :

- Le paramètre`log_statement` peut être utilisé pour consigner l'activité utilisateur dans votre base de données PostgreSQL. Pour plus d'informations, consultez Fichiers journaux de base de données PostgreSQL (p. 521).
- Le paramètre `rds.force_admin_logging_level` consigne les actions effectuées par l'utilisateur interne RDS (rdsadmin) dans les bases de données sur l'instance de base de données, et écrit la sortie dans le journal des erreurs PostgreSQL. Les valeurs autorisées sont disabled, debug5, debug4, debug3, debug2, debug1, info, notice, warning, error, log, fatal et panic. La valeur par défaut est disabled.
- Le paramètre `rds.force_autovacuum_logging_level` consigne les opérations de l'exécutant autovacuum dans toutes les bases de données sur l'instance de base de données et écrit la sortie dans le journal des erreurs PostgreSQL. Les valeurs autorisées sont disabled, debug5, debug4, debug3, debug2, debug1, info, notice, warning, error, log, fatal et panic. La valeur par défaut est disabled. Le paramètre recommandé par Amazon RDS pour rds.force_autovacuum_logging_level est LOG. Affectez à log_autovacuum_min_duration une valeur comprise entre 1 000 et 5 000. L'affectation de la valeur 5 000 entraîne l'écriture dans le journal des activités de plus de 5 secondes et l'affichage de messages « action vacuum ignorée ». Pour de plus amples informations sur ce paramètre, veuillez consulter Bonnes pratiques pour utiliser les moteurs de stockage PostgreSQL (p. 142).

Utilisation de l'extension pgaudit

L'extension `pgaudit` fournit une journalisation détaillée des audits de session et d'objet pour Amazon RDS for PostgreSQL version 9.6.3 ou ultérieure, ainsi que version 9.5.7 ou ultérieure. Vous pouvez activer des audits de session ou des audits d'objet à l'aide de cette extension.

Avec les audits de session, vous pouvez journaliser des événements d'audit de différentes sources et inclure le texte de commande complet lorsqu'il est disponible. Par exemple, vous pouvez utiliser des audits de session pour journaliser toutes les instructions READ qui se connectent à une base de données en définissant pgaudit.log sur « READ ».

Avec les audits d'objet, vous pouvez affiner la journalisation d'audit pour que celle-ci fonctionne avec des commandes spécifiques. Par exemple, vous pouvez spécifier que vous souhaitez une journalisation d'audit pour les opérations READ sur un nombre spécifique de tables.

Pour utiliser la journalisation basée sur des objets avec l'extension **`pgaudit`**

1. Créez un rôle de base de données spécifique appelé `rds_pgaudit`. Utilisez la commande suivante pour créer le rôle.

```
CREATE ROLE rds_pgaudit;
CREATE ROLE
```

2. Modifiez le groupe de paramètres qui est associé à votre instance de base de données pour utiliser les bibliothèques de préchargement partagées contenant `pgaudit` et définissez le paramètre `pgaudit.role`. `pgaudit.role` doit être défini sur le rôle `rds_pgaudit`.

   La commande suivante modifie un groupe de paramètres personnalisé.

```
aws rds modify-db-parameter-group
   --db-parameter-group-name rds-parameter-group-96
   --parameters
 "ParameterName=pgaudit.role,ParameterValue=rds_pgaudit,ApplyMethod=pending-reboot"
   --parameters
 "ParameterName=shared_preload_libraries,ParameterValue=pgaudit,ApplyMethod=pending-
reboot"
   --region us-west-2
```

3. Redémarrez l'instance de base de données pour qu'elle récupère les modifications apportées au groupe de paramètres. La commande suivante redémarre une instance de base de données.

```
aws rds reboot-db-instance --db-instance-identifier rds-test-instance --region us-
west-2
```

4. Exécutez la commande suivante pour confirmer que `pgaudit` a été initialisé.

```
show shared_preload_libraries;
shared_preload_libraries
--------------------------
rdsutils,pgaudit
(1 row)
```

5. Exécutez la commande suivante pour créer l'extension `pgaudit`.

```
CREATE EXTENSION pgaudit;
CREATE EXTENSION
```

6. Exécutez la commande suivante pour confirmer que `pgaudit.role` est défini sur rds_pgaudit.

```
show pgaudit.role;
```

```
pgaudit.role
------------------
rds_pgaudit
```

Pour tester la journalisation d'audit, exécutez plusieurs commandes que vous avez choisies d'auditer. Par exemple, vous pouvez exécuter les commandes suivantes.

```
CREATE TABLE t1 (id int);
CREATE TABLE
GRANT SELECT ON t1 TO rds_pgaudit;
GRANT
select * from t1;
id
----
(0 rows)
```

Les journaux de base de données doivent contenir une entrée similaire à ce qui suit.

```
...
2017-06-12 19:09:49 UTC:...:rds_test@postgres:[11701]:LOG: AUDIT:
OBJECT,1,1,READ,SELECT,TABLE,public.t1,select * from t1;
...
```

Pour obtenir des informations sur l'affichage des journaux, veuillez consulter Amazon RDS Fichiers journaux de base de données (p. 490).

Utilisation de l'extension pg_repack

Vous pouvez utiliser l'extension `pg_repack` pour éliminer la distension des tables et des index. Cette extension est prise en charge sur Amazon RDS pour PostgreSQL versions 9.6.3 et versions ultérieures. Pour plus d'informations sur l'extension `pg_repack`, consultez la documentation de projet Github.

Pour utiliser l'extension pg_repack

1. Installez l'extension `pg_repack` sur votre Amazon RDS pour instance de base de données PostgreSQL en exécutant la commande suivante.

   ```
   CREATE EXTENSION pg_repack;
   ```

2. Utilisez l'utilitaire client pg_repack pour vous connecter à une base de données. Utilisez un rôle de base de données disposant des privilèges rds_superuser pour vous connecter à la base de données. Dans l'exemple de connexion suivant, le rôle rds_test dispose des privilèges rds_superuser, et le point de terminaison de base de données utilisé est rds-test-instance.cw7jjfgdr4on8.us-west-2.rds.amazonaws.com.

   ```
   pg_repack -h rds-test-instance.cw7jjfgdr4on8.us-west-2.rds.amazonaws.com -U rds_test -k
    postgres
   ```

Connectez-vous à l'aide de l'option -k. L'option -a n'est pas prise en charge.

3. La réponse du client pg_repack fournit des informations sur les tables sur l'instance de base de données qui sont reconditionnées.

```
INFO: repacking table "pgbench_tellers"
INFO: repacking table "pgbench_accounts"
INFO: repacking table "pgbench_branches"
```

Utilisation de PostGIS

PostGIS est une extension de PostgreSQL pour le stockage et la gestion des informations spatiales. Si vous n'êtes pas familier avec PostGIS, veuillez consulter PostGIS.net.

Vous devez procéder à certaines configurations avant de pouvoir utiliser l'extension PostGIS. La liste suivante présente ce que vous devez faire. Chaque étape est décrite de façon plus détaillée plus loin dans cette section.

- Connectez-vous à l'instance de base de données à l'aide du nom d'utilisateur principal utilisé pour créer l'instance de base de données.
- Chargez les extensions PostGIS.
- Transférez la propriété des extensions au rôle `rds_superuser`.
- Transférez la propriété des objets au rôle `rds_superuser`.
- Testez les extensions.

Étape 1 : Connexion à l'instance de base de données à l'aide de l'identifiant principal utilisé pour créer l'instance de base de données

Connectez-vous d'abord à l'instance de base de données à l'aide du nom d'utilisateur principal utilisé pour créer l'instance de base de données. Le rôle `rds_superuser` est automatiquement affecté au nom. Vous avez besoin du rôle `rds_superuser` qui est nécessaire pour les étapes restantes.

L'exemple suivant utilise SELECT pour vous montrer l'utilisateur actuel. Dans le cas présent, l'utilisateur doit être l'utilisateur principal choisi lors de la création de l'instance de base de données.

```
select current_user;
 current_user
 -------------
  myawsuser
 (1 row)
```

Étape 2 : Chargez les extensions PostGIS

Utilisez les instructions CREATE EXTENSION pour charger les extensions PostGIS. Vous devez également charger l'extension . Vous pouvez ensuite utiliser la commande `\dn` psql pour répertorier les propriétaires des schémas PostGIS.

```
create extension postgis;
CREATE EXTENSION
```

```
create extension fuzzystrmatch;
CREATE EXTENSION
create extension postgis_tiger_geocoder;
CREATE EXTENSION
create extension postgis_topology;
CREATE EXTENSION
\dn
     List of schemas
     Name      |   Owner
--------------+-----------
 public       | myawsuser
 tiger        | rdsadmin
 tiger_data   | rdsadmin
 topology     | rdsadmin
(4 rows)
```

Étape 3 : Transférez la propriété des extensions au rôle rds_superuser

Utilisez les instructions ALTER SCHEMA pour transférer la propriété des schémas au rôle `rds_superuser`.

```
alter schema tiger owner to rds_superuser;
ALTER SCHEMA
alter schema tiger_data owner to rds_superuser;
ALTER SCHEMA
alter schema topology owner to rds_superuser;
ALTER SCHEMA
\dn
       List of schemas
     Name      |      Owner
--------------+---------------
 public       | myawsuser
 tiger        | rds_superuser
tiger_data    | rds_superuser
 topology     | rds_superuser
(4 rows)
```

Étape 4 : Transférez la propriété des objets au rôle rds_superuser

Utilisez la fonction suivante pour transférer la propriété des objets PostGIS au rôle `rds_superuser`. Exécutez l'instruction suivante à partir de l'invite psql pour créer la fonction.

```
CREATE FUNCTION exec(text) returns text language plpgsql volatile AS $f$ BEGIN EXECUTE $1;
 RETURN $1; END; $f$;
```

Ensuite, exécutez cette requête pour exécuter la fonction exec qui à son tour exécute les instructions et modifie les autorisations.

```
SELECT exec('ALTER TABLE ' || quote_ident(s.nspname) || '.' || quote_ident(s.relname) || '
 OWNER TO rds_superuser;')
  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;
```

Étape 5 : Testez les extensions

Ajoutez `tiger` à votre chemin de recherche à l'aide de la commande suivante.

```
SET search_path=public,tiger;
```

Testez `tiger` à l'aide de l'instruction SELECT suivante.

```
select na.address, na.streetname, na.streettypeabbrev, na.zip
from normalize_address('1 Devonshire Place, Boston, MA 02109') as na;
 address | streetname | streettypeabbrev |  zip
---------+------------+------------------+-------
       1 | Devonshire | Pl               | 02109
(1 row)
```

Testez `topology` à l'aide de l'instruction SELECT suivante.

```
select topology.createtopology('my_new_topo',26986,0.5);
 createtopology
----------------
              1
(1 row)
```

Utilisation de pgBadger pour l'analyse de journal serveur avec PostgreSQL

Vous pouvez utiliser un analyseur de journaux tel que pgbadger pour analyser les journaux PostgreSQL. La documentation pgbadger indique que le motif %l (ligne de journal pour la session/le processus) doit faire partie du préfixe. Cependant, si vous fournissez le préfixe rds log_line_prefix en tant que paramètre pour pgbadger, il doit tout de même produire un rapport.

Par exemple, la commande suivante formate correctement un fichier journal PostgreSQL Amazon RDS daté du 04/02/2014 à l'aide de pgbadger.

```
./pgbadger -p '%t:%r:%u@%d:[%p]:' postgresql.log.2014-02-04-00
```

Affichage du contenu de pg_config

Dans PostgreSQL version 9.6.1, vous pouvez voir les paramètres de configuration du temps compilation de la version actuellement installée de PostgreSQL à l'aide de la nouvelle vue pg_config. Vous pouvez utiliser la vue en appelant la fonction pg_config, comme illustré dans l'exemple suivant.

```
select * from pg_config();
       name        |             setting

-------------------
+-----------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------
```

```
 BINDIR            | /rdsdbbin/postgres-9.6.1.R1/bin
 DOCDIR            | /rdsdbbin/postgres-9.6.1.R1/share/doc
 HTMLDIR           | /rdsdbbin/postgres-9.6.1.R1/share/doc
 INCLUDEDIR        | /rdsdbbin/postgres-9.6.1.R1/include
 PKGINCLUDEDIR     | /rdsdbbin/postgres-9.6.1.R1/include
 INCLUDEDIR-SERVER | /rdsdbbin/postgres-9.6.1.R1/include/server
 LIBDIR            | /rdsdbbin/postgres-9.6.1.R1/lib
 PKGLIBDIR         | /rdsdbbin/postgres-9.6.1.R1/lib
 LOCALEDIR         | /rdsdbbin/postgres-9.6.1.R1/share/locale
 MANDIR            | /rdsdbbin/postgres-9.6.1.R1/share/man
 SHAREDIR          | /rdsdbbin/postgres-9.6.1.R1/share
 SYSCONFDIR        | /rdsdbbin/postgres-9.6.1.R1/etc
 PGXS              | /rdsdbbin/postgres-9.6.1.R1/lib/pgxs/src/makefiles/pgxs.mk
 CONFIGURE         | '--prefix=/rdsdbbin/postgres-9.6.1.R1' '--with-openssl' '--with-perl'
 '--with-tcl' '--with-ossp-uuid' '--with-libxml' '--with-libraries=/rdsdbbin
/postgres-9.6.1.R1/lib' '--with-includes=/rdsdbbin/postgres-9.6.1.R1/include' '--enable-
debug'
 CC                | gcc
 CPPFLAGS          | -D_GNU_SOURCE -I/usr/include/libxml2 -I/rdsdbbin/postgres-9.6.1.R1/
include
 CFLAGS            | -Wall -Wmissing-prototypes -Wpointer-arith -Wdeclaration-after-
statement
 -Wendif-labels -Wmissing-format-attribute -Wformat-security -fno-strict-
aliasing -fwrapv -fexcess-precision=standard -g -O2
 CFLAGS_SL         | -fpic
 LDFLAGS           | -L../../src/common -L/rdsdbbin/postgres-9.6.1.R1/lib -Wl,--as-needed -
Wl,
 -rpath,'/rdsdbbin/postgres-9.6.1.R1/lib',--enable-new-dtags
 LDFLAGS_EX        |
 LDFLAGS_SL        |
 LIBS              | -lpgcommon -lpgport -lxml2 -lssl -lcrypto -lz -lreadline -lrt -lcrypt
 -ldl -lm
 VERSION           | PostgreSQL 9.6.1
(23 rows)
```

Si vous essayez d'accéder directement à la vue, la demande échoue.

```
select * from pg_config;
ERROR:  permission denied for relation pg_config
```

Utilisation de l'extension orafce

L'extension `orafce` propose des fonctions courantes de bases de données commerciales et facilite le portage d'une base de données commerciale vers PostgreSQL. Amazon RDS pour les versions 9.6.6 et ultérieures de PostgreSQL prend en charge cette extension. Pour plus d'informations sur `orafce`, consultez le projet orafce sur GitHub.

> **Note**
>
> Amazon RDS pour PostgreSQL ne prend pas en charge le package `utl_file` qui fait partie de l'extension `orafce`. La raison en est que les fonctions du schéma `utl_file` fournissent des opérations de lecture et d'écriture sur les fichiers de texte des systèmes d'exploitation, ce qui nécessite un accès de super-utilisateur à l'hôte sous-jacent.

Pour utiliser l'extension orafce

1. Connectez-vous à l'instance de base de données avec le nom d'utilisateur principal utilisé pour créer l'instance de base de données.

Note

Si vous souhaitez activer `orafce` sur une base de données différente dans la même instance, utilisez la commande psql `/c dbname` pour changer de la base de données principale après avoir lancé la connexion.

2. Activez l'extension orafce avec l'extension `CREATE EXTENSION`.

```
CREATE EXTENSION orafce;
```

3. Transférez la propriété du schéma oracle au rôle rds_superuser avec la déclaration `ALTER SCHEMA`.

```
ALTER SCHEMA oracle OWNER TO rds_superuser;
```

Note

Si vous souhaitez voir la liste des propriétaires du schéma oracle, utilisez la commande psql `\dn`.

Accès aux données externes à l'aide de l'extension postgres_fdw

Vous pouvez accéder aux données d'un tableau sur un serveur de bases de données distant à l'aide de l'extension postgres_fdw. Si vous configurez une connexion distante à partir de votre instance de base de données PostgreSQL, l'accès à votre réplica en lecture est également disponible.

Pour utiliser postgres_fdw pour accéder à un serveur de bases de données distant

1. Installez l'extension postgres_fdw.

```
CREATE EXTENSION postgres_fdw;
```

2. Créez un serveur de données externes à l'aide de CREATE SERVER.

```
CREATE SERVER foreign_server
FOREIGN DATA WRAPPER postgres_fdw
OPTIONS (host 'xxx.xx.xxx.xx', port '5432', dbname 'foreign_db');
```

3. Créez un mappage utilisateur pour identifier le rôle à utiliser sur le serveur distant.

```
CREATE USER MAPPING FOR local_user
SERVER foreign_server
OPTIONS (user 'foreign_user', password 'password');
```

4. Créez une table mappée à la table sur le serveur distant.

```
CREATE FOREIGN TABLE foreign_table (
        id integer NOT NULL,
        data text)
```

```
SERVER foreign_server
OPTIONS (schema_name 'some_schema', table_name 'some_table');
```

Utilisation d'un serveur DNS personnalisé pour l'accès réseau sortant.

Amazon RDS pour PostgreSQL prend en charge l'accès réseau sortant sur les instances de base de données. Il permet également la résolution DNS depuis un serveur DNS appartenant au client. Vous pouvez résoudre uniquement les deux noms de domaine complets à partir de votre instance de base de données Amazon RDS via votre serveur DNS personnalisé.

Rubriques

- Activation de la résolution DNS personnalisée (p. 1448)
- Désactivation de la résolution DNS personnalisée (p. 1448)
- Configuration d'un serveur DNS personnalisé (p. 1448)

Activation de la résolution DNS personnalisée

Pour activer la résolution DNS dans le VPC de votre client, associez un groupe personnalisé de paramètres de base de données à votre instance RDS PostgreSQL, définissez le paramètre `rds.custom_dns_resolution` sur 1 pour l'activer, puis redémarrez l'instance de base de données pour que les modifications soient prises en compte.

Désactivation de la résolution DNS personnalisée

Pour désactiver la résolution DNS dans le VPC de votre client, désactivez le paramètre `rds.custom_dns_resolution` de votre groupe personnalisé de paramètres de base de données en le définissant sur 0, puis redémarrez l'instance de base de données pour que les modifications soient prises en compte.

Configuration d'un serveur DNS personnalisé

Une fois que votre serveur de nom DNS personnalisé est configuré, la propagation des modifications dans votre instance de base de données peut prendre jusqu'à 30 minutes. Une fois que les modifications sont propagées dans votre instance de base de données, l'ensemble du trafic réseau sortant nécessitant une recherche DNS interroge votre serveur DNS via le port 53.

> **Note**
>
> Si vous ne configurez pas de serveur DNS personnalisé et que le paramètre `rds.custom_dns_resolution` est défini sur 1, les hôtes sont résolus à l'aide d'une zone privée Route 53. Pour de plus amples informations, veuillez onsulter Utilisation des zones hébergées privées.

Pour configurer un serveur DNS personnalisé pour votre instance de base de données Amazon RDS PostgreSQL

1. A partir du jeu d'options DHCP liées à votre VPC, définissez l'option `domain-name-servers` sur l'adresse IP de votre serveur de noms DNS. Pour de plus amples informations, veuillez consulter Jeux d'options DHCP.

Note

L'option `domain-name-servers` autorise jusqu'à quatre valeurs, mais votre instance de base de données Amazon RDS utilise uniquement la première valeur.

2. Assurez-vous que votre serveur DNS peut résoudre toutes les requêtes de recherche, notamment les noms DNS publics, les noms DNS privés Amazon EC2 et les noms DNS spécifiés par le client. Si le trafic réseau sortant contient une recherche DNS que votre serveur DNS ne peut pas gérer, votre serveur DNS doit avoir des fournisseurs DNS en amont appropriés, configurés.
3. Configurez votre serveur DNS pour produire des réponses UDP (User Datagram Protocol) de 512 octets ou moins.
4. Configurez votre serveur DNS pour produire des réponses TCP (Transmission Control Protocol) de 1024 octets ou moins.
5. Configurez votre serveur DNS pour permettre le trafic entrant à partir de vos instances de bases de données Amazon RDS sur le port 53. Si votre serveur DNS est dans un Amazon VPC, le VPC doit avoir un groupe de sécurité qui contient des règles entrantes qui permettent le trafic UDP et TCP sur le port 53. Si votre serveur DNS n'est pas dans un Amazon VPC, il doit avoir des paramètres de pare-feux appropriés pour permettre le trafic UDP et TCP sur le port 53.

   Pour de plus amples informations, veuillez consulter Groupes de sécurité pour votre VPC et Ajout et suppression de règles.
6. Configurez le VPC de votre instance de base de données Amazon RDS pour permettre le trafic sortant via le port 53. Votre serveur VPC doit avoir un groupe de sécurité qui contient des règles sortantes permettant le trafic UDP et TCP sur le port 53.

   Pour de plus amples informations, veuillez consulter Groupes de sécurité pour votre VPC et Ajout et suppression de règles.
7. Le chemin d'acheminement entre l'instance de base de données Amazon RDS et le serveur DNS doit être configuré correctement pour permettre un trafic DNS.

   Si l'instance de base de données Amazon RDS et le serveur DNS ne sont pas dans le même VPC, une connexion d'appairage doit être configurée entre les deux. Pour de plus amples informations, veuillez consulter Qu'est-ce que l'appairage de VPC ?

Restriction de la gestion des mots de passe

Vous pouvez définir qui peut gérer les mots de passe des utilisateurs de base de données en affectant un rôle spécifique aux personnes concernées. Cette technique vous permet d'avoir plus de contrôle sur la gestion des mots de passe du côté du client.

Pour activer la gestion restreinte des mots de passe, utilisez le paramètre statique `rds.restrict_password_commands` et le rôle `rds_password`. Lorsque le paramètre `rds.restrict_password_commands` est défini sur 1, seuls les utilisateurs associés au rôle `rds_password` peuvent exécuter certaines commandes SQL. Ces commandes SQL restreintes permettent de modifier les mots de passe des utilisateurs de base de données, ainsi que le délai d'expiration des mots de passe.

Pour utiliser la gestion restreinte des mots de passe, l'instance de base de données doit exécuter Amazon RDS pour PostgreSQL 10.6 ou version ultérieure. Comme le paramètre `rds.restrict_password_commands` est statique, vous devez redémarrer la base de données pour le modifier.

Lorsque la gestion restreinte des mots de passe est activée au niveau d'une base de données, si vous essayez d'exécuter des commandes SQL restreintes, l'erreur suivante est générée : ERROR: must be a member of rds_password to alter passwords (ERREUR : la modification des mots de passe nécessite que vous ayez le rôle rds_password).

Vous trouverez ci-dessous des exemples de commandes SQL dont l'utilisation est contrôlée lorsque la gestion restreinte des mots de passe est activée.

```
postgres=> CREATE ROLE myrole WITH PASSWORD 'mypassword';
postgres=> CREATE ROLE myrole WITH PASSWORD 'mypassword' VALID UNTIL '2020-01-01';
postgres=> ALTER ROLE myrole WITH PASSWORD 'mypassword' VALID UNTIL '2020-01-01';
postgres=> ALTER ROLE myrole WITH PASSWORD 'mypassword';
postgres=> ALTER ROLE myrole VALID UNTIL '2020-01-01';
postgres=> ALTER ROLE myrole RENAME TO myrole2;
```

Certaines commandes `ALTER ROLE` qui incluent `RENAME TO` peuvent également être restreintes. Elles peuvent être restreintes, car la modification du nom d'un rôle PostgreSQL associé à un mot de passe MD5 supprime le mot de passe.

Par défaut, le rôle `rds_password` est toujours affecté au rôle `rds_superuser`. Cette configuration n'est pas modifiable. Vous pouvez affecter le rôle `rds_password` à d'autres rôles à l'aide de la commande SQL `GRANT`. Nous vous conseillons de n'affecter le rôle `rds_password` qu'à quelques rôles utilisés exclusivement pour la gestion des mots de passe. Ces rôles nécessitent l'attribut `CREATEROLE` pour pouvoir modifier d'autres rôles.

Assurez-vous de vérifier les exigences de mot de passe telles que la date d'expiration et le niveau de complexité requis du côté du client. Nous vous recommandons d'employer votre propre utilitaire côté client pour limiter les modifications liées aux mots de passe. Cette utilitaire doit être membre du rôle `rds_password` et posséder l'attribut de rôle `CREATEROLE`.

Utilisation de l'authentification Kerberos avec Amazon RDS pour PostgreSQL

Vous pouvez désormais utiliser l'authentification Kerberos pour authentifier les utilisateurs lorsqu'ils se connectent à votre instance de base de données qui exécute PostgreSQL. Dans ce cas, votre instance de base de données utilise AWS Directory Service for Microsoft Active Directory (Enterprise Edition) pour activer l'authentification Windows. AWS Directory Service for Microsoft Active Directory (Enterprise Edition) est également appelé AWS Managed Microsoft AD.

Vous créez un annuaire AWS Managed Microsoft AD pour stocker les informations d'identification utilisateur. Vous fournissez ensuite à votre instance de de bases de données PostgreSQL le domaine d'Active Directory ainsi que d'autres informations. Lorsque les utilisateurs s'authentifient auprès de l'instance de de bases de données PostgreSQL, les demandes d'authentification sont transférées vers l'annuaire AWS Managed Microsoft AD.

Vous pouvez gagner du temps et de l'argent en conservant toutes les informations d'identification dans le même annuaire. Vous avez un endroit centralisé de stockage et de gestion des informations d'identification pour plusieurs instances de base de données. L'utilisation d'un annuaire peut également améliorer votre profil de sécurité global.

Kerberos fournit une méthode d'authentification différente d'AWS Identity and Access Management (IAM). Une base de données peut utiliser l'authentification Kerberos ou IAM, mais pas les deux. Pour de plus amples informations sur l'authentification IAM, veuillez consulter Authentification de base de données IAM pour MySQL et PostgreSQL (p. 1554).

Amazon RDS prend en charge l'authentification Kerberos pour les instances de base de données PostgreSQL dans les régions AWS suivantes :

- USA Est (Ohio)

- USA Est (Virginie du Nord)
- USA Ouest (Californie du Nord)
- USA Ouest (Oregon)
- Asie-Pacifique (Mumbai)
- Asie-Pacifique (Séoul)
- Asie-Pacifique (Singapour)
- Asie-Pacifique (Sydney)
- Asie-Pacifique (Tokyo)
- Canada (Centre)
- Europe (Francfort)
- Europe (Irlande)
- Europe (Londres)
- Europe (Stockholm)
- Amérique du Sud (São Paulo)
- Chine (Pékin)
- Chine (Ningxia)

Rubriques

- Présentation de l'authentification Kerberos pour les instances de base de données PostgreSQL (p. 1451)
- Configuration de l'authentification Kerberos pour les instances de base de données PostgreSQL (p. 1452)
- Gestion d'une instance de base de données dans un domaine (p. 1462)
- Connexion à PostgreSQL avec l'authentification Kerberos (p. 1463)

Présentation de l'authentification Kerberos pour les instances de base de données PostgreSQL

Pour configurer l'authentification Kerberos pour une instance de base de données PostgreSQL, exécutez les étapes suivantes, décrites plus en détails par la suite :

1. Utilisez AWS Managed Microsoft AD pour créer un annuaire AWS Managed Microsoft AD. Vous pouvez utiliser AWS Management Console, AWS CLI ou l'API AWS Directory Service pour créer l'annuaire.
2. Créez un rôle fournissant l'accès à Amazon RDS pour effectuer des appels vers votre annuaire AWS Managed Microsoft AD. Pour cela, créez un rôle AWS Identity and Access Management (IAM) qui utilise la stratégie IAM gérée `AmazonRDSDirectoryServiceAccess`.

   Pour que le rôle IAM autorise l'accès, le point de terminaison AWS Security Token Service (AWS STS) doit être activé dans la région AWS correcte pour votre compte AWS. Les points de terminaison AWS STS sont actifs par défaut dans toutes les régions AWS et vous pouvez les utiliser sans qu'aucune autre action soit nécessaire. Pour de plus amples informations, veuillez consulter Activation et désactivation d'AWS STS dans une région AWS dans le Guide de l'utilisateur IAM.
3. Créez et configurez les utilisateurs dans l'annuaire AWS Managed Microsoft AD à l'aide des outils Microsoft Active Directory. Pour de plus amples informations sur la création d'utilisateurs dans votre annuaire Active Directory, veuillez consulter Gérer les utilisateurs et les groupes dans Microsoft AD géré par AWS dans le Guide d'administration AWS Directory Service.

4. Si vous avez l'intention de rechercher l'annuaire et l'instance de base de données dans des comptes AWS ou des VPC (Virtual Private Cloud) différents, configurez l'appairage des VPC. Pour de plus amples informations, veuillez consulter Qu'est-ce que l'appairage de VPC ? dans le Amazon VPC Peering Guide.
5. Créez ou modifiez une instance de base de données PostgreSQL depuis la console, l'interface de ligne de commande ou l'API RDS à l'aide de l'une des méthodes suivantes :
   - Création d'une instance de base de données Amazon RDS (p. 146)
   - Modification d'une instance de base de données Amazon RDS (p. 243)
   - Restauration à partir d'un instantané de base de données (p. 329)
   - Restauration d'une instance de base de données à une date spécifiée (p. 365)

   Lorsque vous créez ou modifiez l'instance de base de données, fournissez l'identifiant de domaine (identifiant `d-*`) qui a été généré lors de la création de votre annuaire. Fournissez également le nom du rôle IAM que vous avez créé. Vous pouvez rechercher l'instance de base de données dans le même VPC que l'annuaire ou dans un autre compte AWS ou VPC.
6. Utilisez les informations d'identification de l'utilisateur principal RDS pour vous connecter à l'instance de base de données PostgreSQL. Créez l'utilisateur dans PostgreSQL en vue de son identification externe. Les utilisateurs identifiés en externe peuvent se connecter à l'instance de base de données PostgreSQL à l'aide de l'authentification Kerberos.

Configuration de l'authentification Kerberos pour les instances de base de données PostgreSQL

Vous utilisez AWS Directory Service for Microsoft Active Directory (Enterprise Edition) (AWS Managed Microsoft AD) pour configurer l'authentification Kerberos pour une instance de base de données PostgreSQL. Pour configurer l'authentification Kerberos, procédez comme suit :

Rubriques

- Étape 1 : Créer un annuaire à l'aide d'AWS Managed Microsoft AD (p. 1452)
- Étape 2 : (Facultatif) Créer une approbation pour un Active Directory sur site (p. 1456)
- Étape 3 : Créer un rôle IAM pour qu'Amazon RDS accède à AWS Directory Service (p. 1457)
- Étape 4 : Créer et configurer des utilisateurs (p. 1458)
- Étape 5 : Activer le trafic entre VPC entre le répertoire et l'instance de base de données (p. 1458)
- Étape 6 : Créer ou modifier une instance de base de données PostgreSQL (p. 1459)
- Étape 7 : Créer les connexions PostgreSQL d'authentification Kerberos (p. 1461)
- Étape 8 : Configurer un client PostgreSQL (p. 1461)

Étape 1 : Créer un annuaire à l'aide d'AWS Managed Microsoft AD

AWS Directory Service crée un annuaire Active Directory totalement géré dans le Cloud AWS. Lorsque vous créez un annuaire AWS Managed Microsoft AD, AWS Directory Service crée deux contrôleurs de domaine et serveurs DNS pour vous. Les serveurs de répertoire sont créés dans des sous-réseaux différents d'un VPC. Cette redondance permet de s'assurer que votre annuaire reste accessible, y compris en cas de défaillance.

Lorsque vous créez un annuaire AWS Managed Microsoft AD, AWS Directory Service effectue les tâches suivantes en votre nom :

- Configuration d'un annuaire Active Directory dans votre VPC.

- Création d'un compte d'administrateur d'annuaire avec le nom d'utilisateur `Admin` et le mot de passe spécifié. Ce compte est utilisé pour gérer votre annuaire.

  Important

  Veillez à enregistrer ce mot de passe. AWS Directory Service ne stocke pas ce mot de passe et il ne peut pas être récupéré ni réinitialisé.
- Création d'un groupe de sécurité pour les contrôleurs de l'annuaire.

Lorsque vous lancez AWS Directory Service for Microsoft Active Directory (Enterprise Edition), AWS crée une unité d'organisation (UO) qui contient tous les objets de votre annuaire. Cette unité d'organisation, qui porte le nom NetBIOS que vous avez entré lorsque vous avez créé votre annuaire, est située dans la racine du domaine. La racine du domaine appartient à AWS, qui la gère.

Le compte `Admin` qui a été créé avec votre annuaire AWS Managed Microsoft AD dispose des autorisations pour les activités d'administration les plus courantes pour votre unité d'organisation :

- Création, mise à jour et suppression des utilisateurs
- Ajouter des ressources à votre domaine, comme des serveurs de fichiers ou d'impression, puis attribuer des autorisations pour ces ressources aux utilisateurs dans votre unité d'organisation
- Créer des unités d'organisation et des conteneurs supplémentaires
- Déléguer des autorités
- Restaurer des objets supprimés de la corbeille Active Directory
- Exécuter des modules Active Directory et DNS (Domain Name Service) pour Windows PowerShell sur le service web Active Directory

Le compte `Admin` dispose également de droits pour exécuter les activités suivantes au niveau du domaine :

- Gérer les configurations DNS (ajouter, supprimer ou mettre à jour des enregistrements, des zones et des redirecteurs)
- Afficher les journaux d'événements DNS
- Afficher les journaux d'événements de sécurité

Pour créer un annuaire avec AWS Managed Microsoft AD

1. Dans le volet de navigation de la console AWS Directory Service, choisissez Annuaires, puis Configurer l'annuaire.
2. Choisissez AWS Managed Microsoft AD. AWS Managed Microsoft AD est la seule option actuellement prise en charge pour être utilisée avec Amazon RDS.
3. Choisissez Suivant.
4. Sur la page Enter directory information (Saisir les détails de l'annuaire), renseignez les informations suivantes :

   Edition

   Choisissez l'édition qui correspond à vos besoins.

   Nom de DNS de l'annuaire

   Nom complet de l'annuaire, par exemple **`corp.example.com`**.

   Nom NetBIOS de l'annuaire

   Nom court facultatif pour l'annuaire, par exemple `CORP`.

Description de l'annuaire

Description facultative de l'annuaire.

Mot de passe administrateur

Mot de passe de l'administrateur de l'annuaire. Le processus de création d'un annuaire crée un compte d'administrateur avec le nom utilisateur `Admin` et ce mot de passe.

Le mot de passe de l'administrateur de l'annuaire ne peut pas contenir le terme « admin ». Le mot de passe est sensible à la casse et doit comporter entre 8 et 64 caractères. Il doit également contenir au moins un caractère de trois des quatre catégories suivantes :

- Lettres minuscules (a–z)
- Lettres majuscules (A–Z)
- Chiffres (0–9)
- Caractères non alphanumériques (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)

Confirmer le mot de passe

Saisissez à nouveau le mot de passe de l'administrateur.

> **Important**
>
> Veillez à enregistrer ce mot de passe. AWS Directory Service ne stocke pas ce mot de passe et il ne peut pas être récupéré ni réinitialisé.

5. Choisissez Suivant.
6. Sur la page Choose VPC and subnets (Choisir un VPC et des sous-réseaux), indiquez les informations suivantes :

   VPC

   Sélectionnez le VPC pour l'annuaire. Vous pouvez créer l'instance de base de données PostgreSQL dans ce même VPC ou dans un autre VPC.

   Sous-réseaux

   Choisissez les sous-réseaux pour les serveurs d'annuaires. Les deux sous-réseaux doivent être dans des zones de disponibilité différentes.
7. Choisissez Suivant.
8. Vérifiez les informations de l’annuaire. Si vous devez apporter des modifications, choisissez Previous (Précédent) et entrez ces modifications. Lorsque les informations sont correctes, choisissez Create directory (Créer l'annuaire).

La création de l'annuaire prend plusieurs minutes. Lorsqu'il est créé, la valeur du champ Statut devient Actif.

Pour consulter les informations relatives à votre annuaire, choisissez l'ID de l’annuaire dans la liste. Notez la valeur de ID de l'annuaire. Vous en aurez besoin pour créer ou modifier votre instance de base de données PostgreSQL.

Étape 2 : (Facultatif) Créer une approbation pour un Active Directory sur site

Si vous ne prévoyez pas d'utiliser votre propre Microsoft Active Directory sur site, passez à Étape 3 : Créer un rôle IAM pour qu'Amazon RDS accède à AWS Directory Service (p. 1457).

Pour obtenir l'authentification Kerberos à l'aide de votre Active Directory sur site, vous devez créer une relation de domaine d'approbation à l'aide d'une forêt d'approbation entre votre Microsoft Active Directory sur site et l'annuaire AWS Managed Microsoft AD (créé dans Étape 1 : Créer un annuaire à l'aide d'AWS Managed Microsoft AD (p. 1452)). L'approbation peut être unidirectionnelle. Dans ce cas, l'annuaire AWS Managed Microsoft AD approuve Microsoft Active Directory sur site. L'approbation peut également être bidirectionnelle. Dans ce cas, les deux Active Directory s'approuvent mutuellement. Pour de plus amples informations sur la configuration d'approbations à l'aide d'AWS Directory Service, veuillez consulter Quand créer une relation d'approbation dans le AWS Directory Service Administration Guide.

> **Note**
>
> Si vous utilisez un Microsoft Active Directory sur site, les points de terminaison du cluster de base de données Les points de terminaison d'instance de base de données ne peuvent pas être utilisés par les clients Windows.

Assurez-vous que le nom de domaine de votre Microsoft Active Directory sur site inclut un routage de suffixe DNS correspondant à la relation d'approbation nouvellement créée. La capture d'écran suivante présente un exemple.

Étape 3 : Créer un rôle IAM pour qu'Amazon RDS accède à AWS Directory Service

Pour qu'Amazon RDS puisse appeler AWS Directory Service pour vous, un rôle IAM utilisant la stratégie IAM gérée `AmazonRDSDirectoryServiceAccess` est requis. Ce rôle permet à Amazon RDS d'effectuer des appels vers AWS Directory Service.

Lorsqu'une instance de base de données est créée à l'aide de l'AWS Management Console et que l'utilisateur de la console dispose de l'autorisation `iam:CreateRole`, la console crée ce rôle automatiquement. Dans ce cas, le nom du rôle est `rds-directoryservice-kerberos-access-role`. Sinon, créez le rôle IAM manuellement. Lorsque vous créez ce rôle IAM, choisissez `Directory Service` et attachez-lui la stratégie gérée AWS `AmazonRDSDirectoryServiceAccess`.

Pour de plus amples informations sur la création de rôles IAM pour un service, veuillez consulter Création d'un rôle pour déléguer des autorisations à un service AWS dans le IAM Guide de l'utilisateur.

> **Note**
>
> Le rôle IAM utilisé pour l'authentification Windows pour RDS for Microsoft SQL Server ne peut pas être utilisé pour Amazon RDS for PostgreSQL.

Vous pouvez également créer des stratégies avec les autorisations obligatoires au lieu d'utiliser la stratégie gérée IAM `AmazonRDSDirectoryServiceAccess`. Dans ce cas, le rôle IAM doit avoir la stratégie d'approbation IAM suivante :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
```

```
      "Principal": {
        "Service": [
          "directoryservice.rds.amazonaws.com",
          "rds.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Le rôle doit également avoir la stratégie de rôle IAM suivante.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
    "Effect": "Allow",
    "Resource": "*"
    }
  ]
}
```

Étape 4 : Créer et configurer des utilisateurs

Vous pouvez créer des utilisateurs à l'aide de l'outil Active Directory Users and Computers, qui fait partie des outils Active Directory Domain Services et Active Directory Lightweight Directory Services. Dans ce cas, les utilisateurs sont des personnes ou des entités qui ont accès à votre annuaire.

Pour créer des utilisateurs dans un annuaire AWS Directory Service, vous devez être connecté à une instance Amazon EC2 Windows. Cette instance EC2 doit également être membre de l'annuaire AWS Directory Service. Parallèlement, vous devez être connecté en tant qu'utilisateur disposant de privilèges pour créer des utilisateurs. Pour de plus amples informations, veuillez consulter Créer un utilisateur dans le Guide d'administration AWS Directory Service.

Étape 5 : Activer le trafic entre VPC entre le répertoire et l'instance de base de données

Si vous avez l'intention de rechercher l'annuaire et l'instance de base de données dans le même VPC, ignorez cette étape et passez à Étape 6 : Créer ou modifier une instance de base de données PostgreSQL (p. 1459).

Si vous avez l'intention de rechercher l'annuaire et l'instance de base de données dans des VPC différents, configurez le trafic entre VPC à l'aide de l'appairage de VPC ou à l'aide de AWS Transit Gateway.

La procédure suivante active le trafic entre les VPC à l'aide de l'appairage de VPC. Suivez les instructions de Qu'est-ce que l'appairage de VPC ? dans le Guide de l'appairage Amazon Virtual Private Cloud.

Pour activer le trafic entre VPC à l'aide de l'appairage de VPC

1. Configurez les règles de routage de VPC appropriées afin de veiller à ce que le trafic réseau puisse être acheminé dans les deux sens.

2. Assurez-vous que le groupe de sécurité de l'instance de base de données puisse recevoir le trafic entrant depuis le groupe de sécurité de cet annuaire.
3. Assurez-vous qu'il n'existe aucune règle de liste de contrôle d'accès (ACL) pour bloquer le trafic.

Si un autre compte AWS possède l'annuaire, vous devez le partager.

Pour partager l'annuaire entre des comptes AWS

1. Commencez le partage de l'annuaire avec le compte AWS dans lequel l'instance de base de données sera créée en suivant les instructions du Didacticiel : Partage de votre annuaire AWS Managed Microsoft AD pour la jonction de domaines EC2 en toute transparence dans le Guide d'administration AWS Directory Service.
2. Connectez-vous à la console AWS Directory Service à l'aide du compte pour l'instance de base de données et assurez-vous que l'état du domaine est `SHARED` avant de poursuivre.
3. Lorsque vous êtes connecté à la console AWS Directory Service avec le compte de l'instance de base de données, notez la valeur de ID de l'annuaire. Vous utilisez cet ID pour joindre l'instance de base de données au domaine.

Étape 6 : Créer ou modifier une instance de base de données PostgreSQL

Créez ou modifiez une instance de base de données PostgreSQL en vue de son utilisation avec votre annuaire. Vous pouvez utiliser la console, l'interface de ligne de commande ou l'API RDS pour associer une instance de base de données à un annuaire. Vous pouvez effectuer cette opération de différentes manières :

- Créez une instance de base de données PostgreSQL à l'aide de la console, de la commande de l'interface de ligne de commande create-db-instance ou de l'opération d'API RDS CreateDBInstance. Pour obtenir des instructions, consultez Création d'une instance de base de données Amazon RDS (p. 146).
- Modifiez une instance de base de données PostgreSQL existante à l'aide de la console, de l'interface de ligne de commande modify-db-instance ou de l'opération d'API RDS ModifyDBInstance. Pour obtenir des instructions, consultez Modification d'une instance de base de données Amazon RDS (p. 243).
- Restaurez une instance de base de données PostgreSQL à partir d'un instantané de bases de données à l'aide de la console, de la commande d'interface de ligne de commande restore-db-instance-from-db-snapshot ou de l'opération d'API RDS RestoreDBInstanceFromDBSnapshot. Pour obtenir des instructions, consultez Restauration à partir d'un instantané de base de données (p. 329).
- Restaurez une instance de base de données PostgreSQL à un moment donné en utilisant la console, la commande d'interface de ligne de commande restore-db-instance-to-point-in-time ou l'opération d'API RDS RestoreDBInstanceToPointInTime. Pour obtenir des instructions, consultez Restauration d'une instance de base de données à une date spécifiée (p. 365).

L'authentification Kerberos est uniquement prise en charge pour les instances de base de données PostgreSQL dans un VPC. L'instance de base de données peut se trouver dans le même VPC que l'annuaire ou dans un autre VPC. L'instance de base de données doit utiliser un groupe de sécurité qui accepte les sorties du VPC de l'annuaire, afin que l'instance de base de données puisse communiquer avec l'annuaire.

Lorsque vous utilisez la console pour créer une instance de base de données, choisissez Mot de passe et authentification Kerberos dans la section Authentification de base de données. Choisissez Parcourir les annuaires, puis sélectionnez l'annuaire, ou choisissez Créer un nouvel annuaire.

Lorsque vous utilisez la console pour modifier ou restaurer une instance de base de données, choisissez l'annuaire dans la section Authentification Kerberos ou choisissez Créer un nouvel annuaire.

Lorsque vous utilisez l'AWS CLI, les paramètres suivants sont obligatoires pour que l'instance de base de données puisse utiliser l'annuaire que vous avez créé :

- Pour le paramètre `--domain`, vous devez indiquer l'identifiant du domaine (identifiant « d-* ») généré lors de la création de l'annuaire.
- Pour le paramètre `--domain-iam-role-name`, utilisez le rôle que vous avez créé qui utilise la stratégie IAM gérée `AmazonRDSDirectoryServiceAccess`.

Par exemple, la commande d'interface de ligne de commande suivante modifie une instance de base de données de façon à utiliser un annuaire.

```
aws rds modify-db-instance --db-instance-identifier mydbinstance --domain d-Directory-ID --
domain-iam-role-name role-name
```

> **Important**
>
> Si vous modifiez une instance de base de données de façon à activer l'authentification Kerberos, redémarrez l'instance de base de données après avoir effectué la modification.

Étape 7 : Créer les connexions PostgreSQL d'authentification Kerberos

Utilisez ensuite les informations d'identification de l'utilisateur principal RDS pour vous connecter à l'instance de base de données PostgreSQL de la même manière qu'avec n'importe quelle instance de base de données. L'instance de base de données est jointe au domaine AWS Managed Microsoft AD. Vous pouvez ainsi mettre en service les connexions et utilisateurs PostgreSQL depuis les utilisateurs et groupes Microsoft Active Directory de votre domaine. Pour gérer les autorisations de base de données, vous pouvez octroyer et annuler les autorisations PostgreSQL standard pour ces connexions.

Pour autoriser un utilisateur Active Directory à s'authentifier avec PostgreSQL, utilisez les informations d'identification de l'utilisateur principal RDS. Vous utilisez ces informations d'identification pour vous connecter à l'instance de base de données PostgreSQL de la même manière que pour n'importe quelle instance de base de données. Après vous être connecté, créez un utilisateur authentifié en externe dans PostgreSQL et accordez-lui le rôle `rds_ad`.

```
CREATE USER "username@CORP.EXAMPLE.COM" WITH LOGIN;
GRANT rds_ad TO "username@CORP.EXAMPLE.COM";
```

Remplacez *`username`* par le nom de l'utilisateur et incluez le nom de domaine en majuscules. Les utilisateurs (personnes et applications) de votre domaine peuvent désormais se connecter à l'instance PostgreSQL RDS à partir d'un ordinateur client joint au domaine à l'aide de l'authentification Kerberos.

Étape 8 : Configurer un client PostgreSQL

Pour configurer un client PostgreSQL, procédez comme suit :

- Créez un fichier krb5.conf (ou équivalent) pointant vers le domaine.
- Vérifiez que le trafic peut circuler entre l'hôte du client et AWS Directory Service. Utilisez un utilitaire réseau tel que Netcat pour les opérations suivantes :
  - Vérifiez le trafic via DNS pour le port 53.
  - Vérifiez le trafic via TCP/UDP pour le port 53 et pour Kerberos, cela incluant les ports 88 et 464 pour AWS Directory Service.
- Vérifiez que le trafic peut circuler entre l'hôte du client et l'instance de base de données via le port de la base de données. Par exemple, utilisez psql pour vous connecter à la base de données et y accéder.

Vous trouverez ci-après un exemple de contenu krb5.conf pour AWS Managed Microsoft AD.

```
[libdefaults]
 default_realm = EXAMPLE.COM
 default_ccache_name = /tmp/kerbcache
[realms]
 EXAMPLE.COM = {
  kdc = example.com
  admin_server = example.com
 }
[domain_realm]
 .example.com = EXAMPLE.COM
 example.com = EXAMPLE.COM
```

Vous trouverez ci-après un exemple de contenu krb5.conf pour un Microsoft Active Directory sur site.

```
[libdefaults]
 default_realm = EXAMPLE.COM
 default_ccache_name = /tmp/kerbcache
```

```
[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
```

Gestion d'une instance de base de données dans un domaine

Vous pouvez utiliser la console, l'interface de ligne de commande ou l'API RDS pour gérer votre instance de base de données et sa relation avec votre annuaire Microsoft Active Directory. Par exemple, vous pouvez associer un annuaire Active Directory de façon à activer l'authentification Kerberos. Vous pouvez également supprimer l'association d'un annuaire Active Directory pour désactiver l'authentification Kerberos. Vous pouvez également transférer une instance de base de données vers un autre élément de même type afin de subir une authentification en externe par un annuaire Microsoft Active Directory.

Par exemple, l'interface de ligne de commande vous permet d'effectuer les actions suivantes :

- Pour retenter l'activation de l'authentification Kerberos en cas d'échec d'appartenance, utilisez la commande d'interface de ligne de commande modify-db-instance . Spécifiez l'ID d'annuaire du membre actuel pour l'option `--domain`.
- Pour désactiver l'authentification Kerberos sur une instance de base de données, utilisez la commande d'interface de ligne de commande modify-db-instance . Spécifiez `none` pour l'option `--domain`.
- Pour transférer une instance de base de données d'un domaine vers un autre, utilisez la commande d'interface de ligne de commande modify-db-instance . Spécifiez l'identifiant du nouveau domaine pour l'option `--domain`.

Présentation de l'appartenance au domaine

Une fois que vous avez créé ou modifié votre instance de base de données, elle devient membre du domaine. Vous pouvez consulter le statut de l'appartenance au domaine pour l'instance de base de données dans la console ou en exécutant la commande d'interface de ligne de commande describe-db-instances. Le statut de l'instance de base de données peut avoir les valeurs suivantes :

- `kerberos-enabled` – L'instance de base de données a l'authentification Kerberos activée.
- `enabling-kerberos` – AWS est en train d'activer l'authentification Kerberos sur cette instance de base de données.
- `pending-enable-kerberos` – L'activation de l'authentification Kerberos est en attente sur cette instance de base de données.
- `pending-maintenance-enable-kerberos` – AWS tentera d'activer l'authentification Kerberos sur cette instance de base de données lors de la prochaine fenêtre de maintenance planifiée.
- `pending-disable-kerberos` – La désactivation de l'authentification Kerberos est en attente sur cette instance de base de données.

- `pending-maintenance-disable-kerberos` – AWS tentera de désactiver l'authentification Kerberos sur cette instance de base de données lors de la prochaine fenêtre de maintenance planifiée.
- `enable-kerberos-failed` – Un problème de configuration a empêché AWS d'activer l'authentification Kerberos sur l'instance de base de données. Corrigez le problème de configuration avant de réémettre la commande de modification de l'instance de base de données.
- `disabling-kerberos` – AWS est en train de désactiver l'authentification Kerberos sur cette instance de base de données.

Une demande d'activation de l'authentification Kerberos peut échouer à cause d'un problème de connectivité réseau ou d'un rôle IAM incorrect. Dans certains cas, la tentative d'activation de l'authentification Kerberos peut échouer lorsque vous créez ou modifiez une instance de base de données. Si tel est le cas, vérifiez que vous utilisez le rôle IAM correct, puis modifiez l'instance de base de données afin d'effectuer son rattachement au domaine.

> **Note**
>
> Seule l'authentification Kerberos avec RDS for PostgreSQL envoie le trafic aux serveurs DNS du domaine. Toutes les autres demandes DNS sont traitées comme un accès réseau sortant sur vos instances de bases de données exécutant PostgreSQL. Pour de plus amples informations sur l'accès réseau sortant avec RDS for PostgreSQL, veuillez consulter Utilisation d'un serveur DNS personnalisé pour l'accès réseau sortant. (p. 1448).

Connexion à PostgreSQL avec l'authentification Kerberos

Vous pouvez vous connecter à PostgreSQL via l'authentification Kerberos avec l'interface pgAdmin ou avec une interface de ligne de commande telle que psql. Pour de plus amples informations sur la connexion,veuillez consulter Connexion à une instance de base de données exécutant le moteur de base de données PostgreSQL (p. 1364) .

pgAdmin

Pour vous connecter à PostgreSQL avec l'authentification Kerberos en utilisant pgAdmin, procédez comme suit :

1. Lancez l'application pgAdmin sur votre ordinateur client.
2. Dans l'onglet Tableau de bord, choisissez Add New Server (Ajouter un nouveau serveur).
3. Dans la boîte de dialogue Create - Server (Créer - Serveur), entrez un nom sur l'onglet General (Général) pour identifier le serveur dans pgAdmin.
4. Dans l'onglet Connection (Connexion), entrez les informations suivantes à partir de votre base de données RDS for PostgreSQL :
   - Pour Host (Hôte), entrez le point de terminaison. Utilisez un format tel que *`PostgreSQL-endpoint`*`.`*`AWS-Region`*`.rds.amazonaws.com`.

     Si vous utilisez un Microsoft Active Directory sur site à partir d'un client Windows, vous devez vous connecter à l'aide d'un point de terminaison spécial. Au lieu d'utiliser le domaine Amazon `rds.amazonaws.com` dans le point de terminaison hôte, utilisez le nom de domaine d'AWS Managed Active Directory.

     Par exemple, supposons que le nom de domaine pour AWS Managed Active Directory soit `corp.example.com`. Alors, pour Host (Hôte), utilisez le format *`PostgreSQL-endpoint`*`.`*`AWS-Region`*`.corp.example.com`.
   - Pour Port, entrez le port attribué.

- Pour Maintenance database (Base de données de maintenance), entrez le nom de la base de données initiale à laquelle le client se connectera.
- Pour Username (Nom d'utilisateur), tapez le nom d'utilisateur que vous avez entré pour l'authentification Kerberos dans Étape 7 : Créer les connexions PostgreSQL d'authentification Kerberos (p. 1461).

5. Choisissez Enregistrer.

Psql

Pour vous connecter à PostgreSQL avec l'authentification Kerberos en utilisant psql, procédez comme suit :

1. A partir d'une invite de commande, exécutez la commande suivante.

```
kinit username
```

   Remplacez *username* par le nom de l'utilisateur. À l'invite, entrez le mot de passe stocké dans le Microsoft Active Directory pour l'utilisateur.

2. Si l'instance de base de données PostgreSQL utilise un VPC accessible au public, insérez une adresse IP privée pour le point de terminaison de votre instance de base de données dans votre fichier `/etc/hosts` sur le client EC2. Par exemple, les commandes suivantes permettent d'obtenir l'adresse IP privée et de la placer dans le fichier `/etc/hosts`.

```
% 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
```

   Si vous utilisez un Microsoft Active Directory sur site à partir d'un client Windows, vous devez vous connecter à l'aide d'un point de terminaison spécial. Au lieu d'utiliser le domaine Amazon `rds.amazonaws.com` dans le point de terminaison hôte, utilisez le nom de domaine d'AWS Managed Active Directory.

   Par exemple, supposons que le nom de domaine de votre AWS Managed Active Directory soit `corp.example.com`. Alors, utilisez le format *PostgreSQL-endpoint.AWS-Region.corp.example.com* pour le point de terminaison et placez-le dans le fichier `/etc/hosts`.

```
% echo " 34.210.197.118  PostgreSQL-endpoint.AWS-Region.corp.example.com" >> /etc/hosts
```

3. Utilisez la commande psql suivante pour vous connecter à une instance de base de données PostgreSQL intégré à Active Directory.

```
psql -U username@CORP.EXAMPLE.COM -p 5432 -h PostgreSQL-endpoint.AWS-
Region.rds.amazonaws.com postgres
```

   Pour vous connecter au cluster de base de données PostgreSQL à partir d'un client Windows à l'aide d'un Active Directory sur site, utilisez la commande psql suivante avec le nom de domaine de l'étape précédente (`corp.example.com`) :

```
psql -U username@CORP.EXAMPLE.COM -p 5432 -h PostgreSQL-endpoint.AWS-
Region.corp.example.com postgres
```

Utilisation de l'environnement en préversion de base de données

Lorsque vous créez une instance de base de données dans Amazon RDS, vous savez que la version de PostgreSQL sur laquelle elle est basée a été testée et est totalement prise en charge par Amazon. La communauté PostgreSQL publie continuellement de nouvelles versions et de nouvelles extensions. Vous pouvez tester les nouvelles versions et extensions de PostgreSQL avant qu'elles ne soient totalement prises en charge. Pour cela, vous pouvez créer une nouvelle instance de base de données dans l'environnement en préversion de base de données.

Les instances de base de données de l'environnement en préversion de base de données sont similaires à celles de l'environnement de production. Toutefois, gardez à l'esprit certains éléments importants :

- Toutes les instances de base de données sont supprimées 60 jours après leur création, en même temps que leurs sauvegardes et leurs instantanés.
- Vous ne pouvez créer une instance de base de données que dans un VPC (Virtual Private Cloud) basé sur un service Amazon VPC.
- Vous ne pouvez créer que des types d'instances M5, T3 et R5. Pour plus d'informations sur les classes d'instances RDS, consultez Classes d'instances de base de données (p. 6).
- Vous ne pouvez utiliser que les stockages SSD à usage général et les stockages SSD IOPS provisionnés.
- Vous ne pouvez pas obtenir de l'aide sur les instances de bases de données auprès d'AWS Support. Vous pouvez cependant publier vos questions sur le forum de l'environnement en préversion de base de données RDS.
- Vous ne pouvez pas copier un instantané d'instance de base de données dans un environnement de production.
- Vous pouvez utiliser à la fois des déploiements mono-AZ et multi-AZ.
- Vous pouvez utiliser les fonctions de vidage et de chargement PostgreSQL standard pour exporter des bases de données depuis ou importer des bases de données vers l'environnement ne préversion de la base de données.

Rubriques

- Fonctions non prises en charge dans l'environnement en préversion (p. 1465)
- Extensions PostgreSQL prises en charge dans l'environnement en préversion (p. 1466)
- Création d'une nouvelle instance de base de données dans l'environnement en préversion (p. 1467)

Fonctions non prises en charge dans l'environnement en préversion

Les fonctions suivantes ne sont pas disponibles dans l'environnement en préversion :

- Copie d'instantanés entre régions
- Réplicas en lecture entre régions
- Extensions ne figurant pas dans le tableau suivant des extensions prises en charge

Extensions PostgreSQL prises en charge dans l'environnement en préversion

Les extensions PostgreSQL prises en charge dans l'environnement en préversion de base de données sont listées dans le tableau suivant.

Extension	Version
amcheck	1.2
aws_commons	1.0
aws_s3	1.0
bloom	1.0
btree_gin	1.3
btree_gist	1.5
citext	1.6
cube	1.4
dblink	1.2
dict_int	1.0
dict_xsyn	1.0
earthdistance	1.1
fuzzystrmatch	1.1
hstore	1,7
hstore_plper	1.0
intagg	1.1
intarray	1.3
ip4r	2,4
isn	1.2
jsonb_plperl	1.0
ltree	1.2
pageinspect	1.8
pg_buffercache	1.3
pg_freespacemap	1.2
pg_prewarm	1.2
pg_similarity	1.0
pg_stat_statements	1.8

Extension	Version
pg_transport	1.0
pg_trgm	1.5
pg_visibility	1.2
pgcrypto	1.3
pgrouting	3.0.0
pgrowlocks	1.2
pgstattuple	1.5
pgtap	1.1.0
plperl	1.0
plpgsql	1.0
plprofiler	4.1
pltcl	1.0
postgres_fdw	1.0
prefix	1.2.0
sslinfo	1.2
tablefunc	1.0
test_parser	1.0
tsm_system_rows	1.0
tsm_system_time	1.0
unaccent	1.1
uuid_ossp	1.1

Création d'une nouvelle instance de base de données dans l'environnement en préversion

Utilisez la procédure suivante pour créer une instance de base de données dans l'environnement en préversion.

Pour créer une instance de base de données dans l'environnement en préversion

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Choisissez Dashboard (Tableau de bord) dans le panneau de navigation.
3. Choisissez Switch to database preview environment (Basculer vers l'environnement en préversion de base de données).

Vous pouvez également accéder directement à l'environnement en préversion de base de données.

> **Note**
>
> Si vous souhaitez créer une instance dans l'environnement en préversion de base de données via l'API ou l'interface de ligne de commande, le point de terminaison est `rds-preview.us-east-2.amazonaws.com`.

4. Passez ensuite à la procédure décrite dans Console (p. 146).

Versions et extensions Amazon RDS pour PostgreSQL

Amazon RDS prend en charge les instances de bases de données qui exécutent plusieurs éditions de PostgreSQL. Reportez-vous à cette section pour savoir comment utiliser PostgreSQL sur Amazon RDS. Vous devez également être conscient des limites des instances de bases de données PostgreSQL.

Vous pouvez spécifier n'importe quelle version PostgreSQL actuellement prise en charge lorsque vous créez une instance de base de données. Vous pouvez spécifier la version majeure (par exemple PostgreSQL 10), puis toute version mineure prise en charge pour la version majeure spécifiée. Si aucune version n'est spécifiée, Amazon RDS utilise par défaut une version prise en charge, généralement la plus récente. Si une version majeure est spécifiée, mais qu'une version mineure ne l'est pas, Amazon RDS utilise par défaut une version récente de la version majeure que vous avez spécifiée. Pour afficher la liste des versions prises en charge, ainsi que celles par défaut des instances de base de données nouvellement créées, utilisez la commande `describe-db-engine-versions` de l'AWS CLI.

Pour plus d'informations sur l'importation des données PostgreSQL dans une instance de base de données, consultez Importation de données dans PostgreSQL sur Amazon RDS (p. 1388).

Rubriques

- Versions de base de données PostgreSQL prises en charge (p. 1468)
- Fonctions et extensions PostgreSQL prises en charge (p. 1488)

Versions de base de données PostgreSQL prises en charge

Amazon RDS prend en charge les versions suivantes de PostgreSQL.

Rubriques

- Versions de PostgreSQL 13 (p. 1469)
- Versions de PostgreSQL 12 (p. 1470)
- Versions de PostgreSQL 11 (p. 1471)
- Versions de PostgreSQL 10 (p. 1474)
- Versions de PostgreSQL 9.6 (p. 1478)
- Versions de PostgreSQL 9.5 (p. 1483)

Versions de PostgreSQL 13

Versions mineures

- PostgreSQL version 13 bêta 3 sur Amazon RDS dans l'environnement en préversion de base de données (p. 1469)
- PostgreSQL version 13 bêta 1 sur Amazon RDS dans l'environnement en préversion de base de données (p. 1470)

PostgreSQL version 13 bêta 3 sur Amazon RDS dans l'environnement en préversion de base de données

PostgreSQL version 13 Bêta 3 contient plusieurs améliorations qui sont décrites dans PostgreSQL 12.4, 11.9, 10.14, 9.6.19, 9.5.23 et 13 bêta 3 Released !.

Pour plus d'informations sur l'environnement en préversion de base de données, consultez the section called “Utilisation de l'environnement en préversion de base de données” (p. 1465). Pour accéder à l'environnement en préversion à partir de la console, sélectionnez https://console.aws.amazon.com/rds-preview/.

Cette version ajoute également les extensions suivantes :

- address_standardizer
- address_standardizer_data_us
- log_fdw
- pgaudit
- plcoffee
- plls
- plv8
- PostGIS
- postgis_raster
- postgis_tiger_geocoder
- postgis_topology
- postgresql-hll
- rdkit

Pour de plus amples informations sur les extensions et les modules, veuillez consulter Extensions et modules PostgreSQL version 13 pris en charge sur Amazon RDS (p. 1489).

PostgreSQL version 13 bêta 1 sur Amazon RDS dans l'environnement en préversion de base de données

PostgreSQL version 13 Bêta 1 contient plusieurs améliorations qui sont décrites dans PostgreSQL 13 Bêta 1 Released.

Pour plus d'informations sur l'environnement en préversion de base de données, consultez the section called “Utilisation de l'environnement en préversion de base de données” (p. 1465). Pour accéder à l'environnement en préversion à partir de la console, sélectionnez https://console.aws.amazon.com/rds-preview/.

Versions de PostgreSQL 12

Versions mineures

- PostgreSQL version 12.4 sur Amazon RDS (p. 1470)
- PostgreSQL version 12.3 sur Amazon RDS (p. 1470)
- PostgreSQL version 12.2 sur Amazon RDS (p. 1470)

PostgreSQL version 12.4 sur Amazon RDS

PostgreSQL version 12.4 est désormais disponible sur Amazon RDS. PostgreSQL version 12.4 contient plusieurs améliorations annoncées pour la version 12.4 de PostgreSQL.

Cette version inclut également les modifications suivantes :

1. Ajout de l'extension `pg_proctab` version 0.0.9.
2. Ajout de l'extension `rdkit` version 3.8.
3. Mise à niveau de l'extension `aws_s3` vers la version 1.1.
4. Mise à niveau de l'extension `pglogical` vers la version 2.3.2.
5. Mise à niveau du module `wal2json` vers la version 2.3

Pour de plus amples informations sur les extensions et les modules, veuillez consulter Extensions et modules PostgreSQL version 12 pris en charge sur Amazon RDS (p. 1491).

PostgreSQL version 12.3 sur Amazon RDS

PostgreSQL version 12.3 est maintenant disponible sur Amazon RDS. PostgreSQL version 12.3 contient plusieurs améliorations annoncées pour la version 12.3 de PostgreSQL.

Cette version inclut également les modifications suivantes :

1. Mise à jour de l'extension `pg_hint_plan` vers la version 1.3.5.
2. Mise à jour de l'extension `pglogical` vers la version 2.3.1.

Pour de plus amples informations sur les extensions et les modules, veuillez consulter Extensions et modules PostgreSQL version 12 pris en charge sur Amazon RDS (p. 1491).

PostgreSQL version 12.2 sur Amazon RDS

PostgreSQL version 12.2 est maintenant disponible sur Amazon RDS. PostgreSQL version 12.2 contient plusieurs améliorations annoncées pour les versions 12.0, 12.1 et 12.2 de PostgreSQL.

Pour de plus amples informations sur les extensions et les modules, veuillez consulter Extensions et modules PostgreSQL version 12 pris en charge sur Amazon RDS (p. 1491).

Versions de PostgreSQL 11

Versions mineures

- PostgreSQL version 11.9 sur Amazon RDS (p. 1471)
- PostgreSQL version 11.8 sur Amazon RDS (p. 1471)
- PostgreSQL version 11.7 sur Amazon RDS (p. 1471)
- PostgreSQL version 11.6 sur Amazon RDS (p. 1472)
- PostgreSQL version 11.5 sur Amazon RDS (p. 1472)
- PostgreSQL version 11.4 sur Amazon RDS (p. 1472)
- PostgreSQL version 11.2 sur Amazon RDS (p. 1472)
- PostgreSQL version 11.1 sur Amazon RDS (p. 1473)
- PostgreSQL version 11 sur Amazon RDS dans l'environnement en préversion de base de données (p. 1474)

PostgreSQL version 11.9 sur Amazon RDS

PostgreSQL version 11.9 est désormais disponible sur Amazon RDS. PostgreSQL version 11.9 contient plusieurs améliorations annoncées pour la version 11.9 de PostgreSQL.

Cette version inclut également les modifications suivantes :

1. Ajout de l'extension `aws_s3` version 1.1.
2. Ajout de l'extension `pg_proctab` version 0.0.9.
3. Mise à niveau de l'extension `pgaudit` vers la version 1.3.1.
4. Mise à niveau de l'extension `pglogical` vers la version 2.2.2.
5. Ajout de l'extension `rdkit` version 3.8.

Pour de plus amples informations sur les extensions et les modules, veuillez consulter Extensions et modules PostgreSQL version 11.x pris en charge sur Amazon RDS (p. 1494).

PostgreSQL version 11.8 sur Amazon RDS

PostgreSQL version 11.8 contient plusieurs correctifs de bogues pour palier aux problèmes de la version 11.7. Pour de plus amples informations sur les correctifs de PostgreSQL 11.8, veuillez consulter la documentation PostgreSQL 11.8.

Cette version inclut également la modification suivante :

1. Mise à jour de l'extension `pg_hint_plan` vers la version 1.3.5.

Pour de plus amples informations sur les extensions et les modules, veuillez consulter Extensions et modules PostgreSQL version 11.x pris en charge sur Amazon RDS (p. 1494).

PostgreSQL version 11.7 sur Amazon RDS

PostgreSQL version 11.7 contient plusieurs correctifs de bogues pour palier aux problèmes de la version 11.6. Pour de plus amples informations sur les correctifs de PostgreSQL 11.7, veuillez consulter la documentation PostgreSQL 11.7.

PostgreSQL version 11.6 sur Amazon RDS

PostgreSQL version 11.6 contient plusieurs correctifs de bogues pour les problèmes de la version 11.5. Pour de plus amples informations sur les correctifs de PostgreSQL 11.6, veuillez consulter la documentation PostgreSQL.

Cette version inclut également les modifications suivantes :

1. Mise à jour de l'extension `pgTAP` vers la version 1.1.0.
2. Ajout de l'extension `plprofiler`.
3. Ajout à `shared_preload_libraries` de la prise en charge en `pg_prewarm` pour autoriser un démarrage automatique

PostgreSQL version 11.5 sur Amazon RDS

PostgreSQL version 11.5 contient plusieurs correctifs de bogues pour les problèmes de la version 11.4. Pour de plus amples informations sur les correctifs de PostgreSQL 11.5, veuillez consulter la documentation PostgreSQL.

Cette version inclut également les modifications suivantes :

- Une nouvelle extension `pg_transport` a été ajoutée.
- L'extension `aws_s3` a été mise à jour pour prendre en charge les demandes virtuelles de type hébergé. Pour de plus amples informations, veuillez consulter Amazon S3 Path Deprecation Plan – The Rest of the Story.
- L'extension `PostGIS` a été mise à jour vers la version 2.5.2.

PostgreSQL version 11.4 sur Amazon RDS

Cette version contient un correctif de sécurité important, ainsi que des correctifs de bogue et des améliorations mises au point par la communauté PostgreSQL. Pour de plus amples informations sur le correctif de sécurité, veuillez consulter l'annonce de la communauté PostgreSQL et le correctif de sécurité CVE-2019-10164.

Avec cette version, l'extension `pg_hint_plan` a été mise à jour vers la version 1.3.4.

Pour plus d'informations sur les correctifs de PostgreSQL 11.4, consultez la documentation sur PostgreSQL.

PostgreSQL version 11.2 sur Amazon RDS

PostgreSQL version 11.2 contient plusieurs correctifs de bogues pour les problèmes de la version 11.1. Pour plus d'informations sur les correctifs de PostgreSQL 11.2, consultez la documentation sur PostgreSQL.

Cette version inclut également les modifications suivantes :

- Une nouvelle extension pgTAP version 1.0.
- Prise en charge de l'importation Amazon S3 Pour de plus amples informations, veuillez consulter Importation de données Amazon S3 dans une instance de base de données RDS for PostgreSQL d'un (p. 1393).
- La mise à niveau de plusieurs versions majeures est disponible vers PostgreSQL 11.2 à partir de certaines versions PostgreSQL précédentes. Pour plus d'informations, consultez Choix d'une mise à niveau de version majeure pour PostgreSQL (p. 1375).

Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

Pour obtenir la liste complète des extensions désormais prises en charge par Amazon RDS pour PostgreSQL, consultez Fonctions et extensions PostgreSQL prises en charge (p. 1488).

PostgreSQL version 11.1 sur Amazon RDS

PostgreSQL version 11.1 contient plusieurs améliorations qui sont annoncées dans PostgreSQL 11.1 Released! Cette version comprend des procédures SQL stockées qui autorisent les transactions intégrées au sein d'une procédure. Cette version inclut également des améliorations majeures pour le partitionnement et le parallélisme, ainsi que de nombreuses améliorations des performances. Par exemple, en utilisant une constante non-null pour une valeur par défaut de colonne, vous pouvez désormais utiliser une commande ALTER TABLE pour ajouter une colonne sans entraîner la réécriture d'une table.

PostgreSQL version 11.1 contient plusieurs correctifs de bogues pour les problèmes de la version 11. Pour des détails complets, veuillez consulter la documentation de PostgreSQL version 11.1. Certaines modifications importantes apportées dans cette version incluent les points suivants :

- Partitionnement – Les améliorations du partitionnement comprennent la prise en charge du partitionnement par hachage, ce qui permet la création d'une partition par défaut, et le déplacement de ligne dynamique vers une autre partition en fonction de la mise à jour de la colonne de clé.
- Performances – Les améliorations des performances comprennent le parallélisme lors de la création d'index, les vues matérialisées, les jointures par hachage et les analyses séquentielles pour améliorer les performances des opérations.
- Procédures stockées – Les procédures stockées SQL prennent désormais en charge les transactions intégrées.
- Prise en charge de la fonctionnalité JIT (juste-à-temps) – Les instances RDS PostgreSQL 11 sont créées avec la fonctionnalité JIT, ce qui accélère l'évaluation d'expressions. Pour activer la fonctionnalité JIT, définissez le paramètre `jit` sur 1 dans le groupe de paramètres PostgreSQL de la base de données.
- Taille de segment – La taille de segment WAL (Write-Ahead Logging) est passée de 16 Mo à 64 Mo.
- Améliorations d'autovacuum – Pour fournir une journalisation plus utile, le paramètre `rds.force_autovacuum_logging` a la valeur ON par défaut conjointement avec le paramètre `log_autovacuum_min_duration` défini sur 10 secondes. Pour améliorer l'efficacité d'autovacuum, les valeurs des paramètres `autovacuum_max_workers` et `autovacuum_vacuum_cost_limit` sont calculées selon la capacité de la mémoire hôte pour fournir des valeurs par défaut plus élevées.
- Délai de transaction amélioré – Le paramètre `idle_in_transaction_session_timeout` est défini sur 12 heures. Toute session inactive depuis plus de 12 heures est arrêtée.
- Métriques de performance – Le module `pg_stat_statements` est inclus dans `shared_preload_libraries` par défaut. Cela évite de devoir redémarrer l'instance immédiatement après sa création. Cependant, cette fonctionnalité vous oblige encore d'exécuter l'instruction `CREATE EXTENSION pg_stat_statements;`. De plus, `track_io_timing` est activé par défaut pour ajouter des données plus précises à `pg_stat_statements`.
- Le module tsearch2 n'est plus pris en charge – Si votre application utilise des fonctions `tsearch2`, mettez-la à jour pour utiliser les fonctions équivalentes fournies par le moteur PostgreSQL de base. Pour de plus amples informations sur le module tsearch2, veuillez consulter PostgreSQL tsearch2.
- Le module chkpass n'est plus pris en charge – Pour de plus amples informations sur le module `chkpass`, veuillez consulter PostgreSQL chkpass.
- Les mises à jour d'extension pour RDS PostgreSQL 11.1 sont notamment les suivantes :
  - Mise à jour de `pgaudit` vers la version 1.3.0
  - Mise à jour de `pg_hint_plan` vers la version 1.3.2
  - Mise à jour de `pglogical` vers la version 2.2.1
  - Mise à jour de `plcoffee` vers la version 2.3.8
  - Mise à jour de `plv8` vers la version 2.3.8

- Mise à jour de `PostGIS` vers la version 2.5.1
- Mise à jour de `prefix` vers la version 1.2.8
- Mise à jour de `wal2json` vers le hachage 9e962bad.

Pour obtenir la liste complète des extensions désormais prises en charge par Amazon RDS pour PostgreSQL, consultez Fonctions et extensions PostgreSQL prises en charge (p. 1488).

PostgreSQL version 11 sur Amazon RDS dans l'environnement en préversion de base de données

> Note
>
> PostgreSQL version 11 sur Amazon RDS a été lancé dans l'environnement de production. Il n'est plus pris en charge dans l'environnement en préversion de base de données.

PostgreSQL version 11 contient plusieurs améliorations qui sont décrites dans PostgreSQL 11 Released!

Pour plus d'informations sur l'environnement en préversion de base de données, consultez the section called “Utilisation de l'environnement en préversion de base de données” (p. 1465). Pour accéder à l'environnement en préversion à partir de la console, sélectionnez https://console.aws.amazon.com/rds-preview/.

Versions de PostgreSQL 10

Versions mineures

- PostgreSQL version 10.14 sur Amazon RDS (p. 1474)
- PostgreSQL version 10.13 sur Amazon RDS (p. 1475)
- PostgreSQL version 10.12 sur Amazon RDS (p. 1475)
- PostgreSQL version 10.11 sur Amazon RDS (p. 1475)
- PostgreSQL version 10.10 sur Amazon RDS (p. 1475)
- PostgreSQL version 10.9 sur Amazon RDS (p. 1475)
- PostgreSQL version 10.7 sur Amazon RDS (p. 1475)
- PostgreSQL version 10.6 sur Amazon RDS (p. 1476)
- PostgreSQL version 10.5 sur Amazon RDS (p. 1476)
- PostgreSQL version 10.4 sur Amazon RDS (p. 1477)
- PostgreSQL version 10.3 sur Amazon RDS (p. 1477)
- PostgreSQL version 10.1 sur Amazon RDS (p. 1478)

PostgreSQL version 10.14 sur Amazon RDS

PostgreSQL version 10.14 est désormais disponible sur Amazon RDS. PostgreSQL version 10.14 contient plusieurs améliorations annoncées pour la version 10.14 de PostgreSQL.

Cette version inclut également les modifications suivantes :

1. Ajout de l'extension `aws_s3` version 1.1. Pour de plus amples informations, veuillez consulter Exportation de données à partir d'une instance de base de données RDS for PostgreSQL vers Amazon S3 (p. 1409).
2. Mise à jour de l'extension `pgaudit` vers la version 1.2.1.
3. Mise à niveau de l'extension `pglogical` vers la version 2.2.2.
4. Mise à niveau du module `wal2json` vers la version 2.3

Pour de plus amples informations sur les extensions et les modules, veuillez consulter Extensions et modules PostgreSQL version 10.x pris en charge sur Amazon RDS (p. 1496).

PostgreSQL version 10.13 sur Amazon RDS

PostgreSQL version 10.13 contient plusieurs correctifs de bogues pour palier aux problèmes de la version 10.12. Pour de plus amples informations sur les correctifs de PostgreSQL 10.13, veuillez consulter la documentation PostgreSQL 10.13.

Cette version inclut également la modification suivante :

1. Mise à jour de l'extension `pg_hint_plan` vers la version 1.3.5.

Pour de plus amples informations sur les extensions et les modules, veuillez consulter Extensions et modules PostgreSQL version 10.x pris en charge sur Amazon RDS (p. 1496).

PostgreSQL version 10.12 sur Amazon RDS

PostgreSQL version 10.12 contient plusieurs correctifs de bogues pour palier aux problèmes de la version 10.11. Pour de plus amples informations sur les correctifs de PostgreSQL 10.12, veuillez consulter la documentation PostgreSQL 10.12.

PostgreSQL version 10.11 sur Amazon RDS

PostgreSQL version 10.11 contient plusieurs correctifs de bogues pour les problèmes de la version 10.10. Pour de plus amples informations sur les correctifs de PostgreSQL 10.11, veuillez consulter la documentation PostgreSQL. Les modifications apportées dans cette version incluent les points suivants :

1. Ajout de l'extension `plprofiler`.

PostgreSQL version 10.10 sur Amazon RDS

PostgreSQL version 10.10 contient plusieurs correctifs de bogues pour les problèmes de la version 10.9. Pour de plus amples informations sur les correctifs de PostgreSQL 10.10, veuillez consulter la documentation PostgreSQL. Les modifications apportées dans cette version incluent les points suivants :

1. L'extension `aws_s3` a été mise à jour pour prendre en charge les demandes virtuelles de type hébergé. Pour de plus amples informations, veuillez consulter Amazon S3 Path Deprecation Plan – The Rest of the Story.
2. L'extension `PostGIS` a été mise à jour vers la version 2.5.2.

PostgreSQL version 10.9 sur Amazon RDS

Cette version contient un correctif de sécurité important, ainsi que des correctifs de bogue et des améliorations mises au point par la communauté PostgreSQL. Pour de plus amples informations sur le correctif de sécurité, veuillez consulter l'annonce de la communauté PostgreSQL et le correctif de sécurité CVE-2019-10164.

Avec cette version, l'extension `pg_hint_plan` a été mise à jour vers la version 1.3.3.

Pour plus d'informations sur les correctifs de PostgreSQL 10.9, consultez la documentation sur PostgreSQL.

PostgreSQL version 10.7 sur Amazon RDS

PostgreSQL version 10.7 contient plusieurs correctifs de bogues pour les problèmes de la version 10.6. Pour de plus amples informations sur les correctifs de la version 10.7, veuillez consulter la documentation de PostgreSQL.

Cette version inclut également les modifications suivantes :

- Prise en charge de l'importation Amazon S3 Pour de plus amples informations, veuillez consulter Importation de données Amazon S3 dans une instance de base de données RDS for PostgreSQL d'un (p. 1393).
- La mise à niveau de plusieurs versions majeures est disponible vers PostgreSQL 10.7 à partir de certaines versions PostgreSQL précédentes. Pour plus d'informations, consultez Choix d'une mise à niveau de version majeure pour PostgreSQL (p. 1375).

Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

PostgreSQL version 10.6 sur Amazon RDS

PostgreSQL version 10.6 contient plusieurs correctifs de bogues pour les problèmes de la version 10.5. Pour plus d'informations sur les correctifs de PostgreSQL 10.6, consultez la documentation sur PostgreSQL.

Cette version inclut également les modifications suivantes :

- Un nouveau paramètre `rds.restrict_password_commands` et un nouveau rôle `rds_password` ont été introduits. Lorsque le paramètre `rds.restrict_password_commands` est activé, seuls les utilisateurs dotés du rôle `rds_password` peuvent apporter des modifications aux mots de passe utilisateur et à leur date d'expiration. En limitant les opérations liées aux mots de passe à des rôles spécifiques, vous pouvez mettre en œuvre des stratégies telles que des exigences de complexité des mots de passe du côté client. Le paramètre `rds.restrict_password_commands` est statique. Un redémarrage de la base de données est donc nécessaire pour le modifier. Pour plus d'informations, consultez Restriction de la gestion des mots de passe (p. 1449).
- Le plug-in de décodage logique `wal2json` a été mis à jour pour prendre en charge commit `9e962ba`.

Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

Pour obtenir la liste complète des extensions désormais prises en charge par Amazon RDS pour PostgreSQL, consultez Fonctions et extensions PostgreSQL prises en charge (p. 1488).

> **Note**
>
> Amazon RDS pour PostgreSQL a annoncé la suppression de l'extension `tsearch2` dans la prochaine version majeure. Nous encourageons les clients qui utilisent toujours la recherche de texte dans une version antérieure à 8.3 à migrer vers les fonctionnalités intégrées équivalentes. Pour plus d'informations sur la migration, consultez la documentation PostgreSQL.

PostgreSQL version 10.5 sur Amazon RDS

PostgreSQL version 10.5 contient plusieurs correctifs de bogues pour les problèmes de la version 10.4. Pour plus d'informations sur les correctifs de la version 10.5, consultez la documentation sur PostgreSQL.

Cette version inclut également les modifications suivantes :

- Prise en charge de l'extension `pglogical` version 2.2.0. Les prérequis pour pouvoir utiliser cette extension sont les mêmes que ceux nécessaires pour utiliser la réplication logique pour PostgreSQL, comme décrit dans Réplication logique pour PostgreSQL sur Amazon RDS (p. 1510).
- Prise en charge de l'extension `pg_similarity` version 1.0.
- Prise en charge de l'extension `pageinspect` version 1.6.
- Prise en charge de l'extension `libprotobuf` version 1.3.0 pour le composant PostGIS.
- Une mise à jour de l'extension `pg_hint_plan` à la version 1.3.1.

- Mise à jour de l'extension `wal2json` vers la version 01c5c1e.

Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

Pour obtenir la liste complète des extensions désormais prises en charge par Amazon RDS pour PostgreSQL, consultez Fonctions et extensions PostgreSQL prises en charge (p. 1488).

PostgreSQL version 10.4 sur Amazon RDS

PostgreSQL version 10.4 contient plusieurs correctifs de bogues pour les problèmes de la version 10.3. Pour plus d'informations sur les correctifs de la version 10.4, consultez la documentation sur PostgreSQL.

Cette version inclut également les modifications suivantes :

- Prise en charge de la réplication logique PostgreSQL 10 grâce à la publication native et à l'infrastructure d'abonnement. Les bases de données RDS PostgreSQL peuvent fonctionner à la fois en tant qu'éditeur et qu'abonné. Vous pouvez préciser la réplication dans d'autres bases de données PostgreSQL au niveau de la base de données ou de la table. Avec la réplication logique, les bases de données éditeur et abonné n'ont pas besoin d'être identiques physiquement (bloc pour bloc). Cela permet des cas d'utilisation tels que la consolidation de données, la distribution de données et la réplication de données sur différentes versions de bases de données pour les versions 10.4 et ultérieures. Pour plus d'informations, consultez Réplication logique pour PostgreSQL sur Amazon RDS (p. 1510).
- La limite de taille du fichier temporaire peut être configurée par l'utilisateur. Vous devez disposer du rôle rds_superuser pour pouvoir modifier le paramètre `temp_file_limit`.
- Mettez à jour la bibliothèque `GDAL`, qui est utilisée par l'extension PostGIS. Voir Utilisation de PostGIS (p. 1443).
- Mise à jour de l'extension `ip4r` à la version 2.1.1.
- Mise à jour de l'extension `pg_repack` à la version 1.4.3. Voir Utilisation de l'extension pg_repack (p. 1442).
- Mise à jour de l'extension `plv8` à la version 2.1.2.

Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

Pour obtenir la liste complète des extensions désormais prises en charge par Amazon RDS pour PostgreSQL, consultez Fonctions et extensions PostgreSQL prises en charge (p. 1488).

> **Note**
>
> L'extension `tsearch2` sera supprimée de la prochaine version majeure. Nous encourageons les clients qui utilisent toujours la recherche de texte dans une version antérieure à 8.3 à migrer vers les fonctionnalités intégrées équivalentes. Pour plus d'informations sur la migration, consultez la documentation PostgreSQL.

PostgreSQL version 10.3 sur Amazon RDS

PostgreSQL version 10.3 contient plusieurs correctifs de bogues pour les problèmes de la version 10. Pour plus d'informations sur les correctifs de la version 10.3, consultez la documentation sur PostgreSQL.

La version 2.1.0 de PL/v8 est désormais disponible. Si vous utilisez PL/v8 et mettez à niveau PostgreSQL vers une nouvelle version PL/v8, vous tirerez immédiatement profit de la nouvelle extension, mais les métadonnées du catalogue ne reflèteront pas ce fait. Pour accéder aux étapes permettant de synchroniser les métadonnées du catalogue avec la nouvelle version de PL/v8, consultez Mise à niveau de PL/v8 (p. 1507).

Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

Pour obtenir la liste complète des extensions désormais prises en charge par Amazon RDS pour PostgreSQL, consultez Fonctions et extensions PostgreSQL prises en charge (p. 1488).

PostgreSQL version 10.1 sur Amazon RDS

PostgreSQL version 10.1 contient plusieurs correctifs de bogues pour les problèmes de la version 10. Pour de plus amples informations sur les correctifs de la version 10.1, veuillez consulter la documentation PostgreSQL et PostgreSQL 10 commmunity announcement (l'annonce de communauté PostgreSQL 10).

Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

PostgreSQL version 10.1 inclut les modifications suivantes :

- Le Partitionnement de table déclaratif – PostgreSQL 10 ajoute le partitionnement de table à la syntaxe SQL et au routage de tuple natif.
- Requêtes parallèles – Lorsque vous créez une instance PostgreSQL 10.1, des requêtes parallèles sont activées pour le groupe de paramètres `default.postgres10`. Le paramètre max_parallel_workers_per_gather est défini sur 2 par défaut, mais vous pouvez le modifier pour prendre en charge vos exigences spécifiques de charges de travail.
- Prise en charge ICU (International Components for Unicode) – Vous pouvez utiliser la bibliothèque ICU pour fournir des classements versionnés de manière explicite. Amazon RDS pour PostgreSQL 10.1 est compilé avec la version 60.2 d'ICU. Pour plus d'informations sur la mise en œuvre d'ICU dans PostgreSQL, consultez Collation Support (Soutien de collationnement).
- Grandes pages – Les grandes pages sont une fonction du noyau Linux qui utilise les fonctions de plusieurs tailles de page des architectures matérielles modernes. Amazon RDS pour PostgreSQL prend en charge des grandes pages avec un paramètre de configuration global. Lorsque vous créez une nouvelle instance PostgreSQL 10.1 avec RDS, le paramètre `huge_pages` est défini sur `"on"` pour le groupe de paramètres `default.postgres10`. Vous pouvez modifier ce paramètre afin qu'il prenne en charge vos exigences spécifiques de charges de travail.
- Mise à jour PL/v8 – PL/v8 est un langage procédural qui vous permet d'écrire des fonctions en JavaScript que vous pouvez ensuite appeler depuis SQL. Cette version de PostgreSQL prend en charge la version 2.1.0 de PL/v8.
- Changement de nom de xlog et d'emplacement – Dans la version 10 de PostgreSQL, l'abréviation « xlog » a été remplacée par « wal » et le terme « location » a été remplacé par « lsn ». Pour plus d'informations, consultez https://www.postgresql.org/docs/10/static/release-10.html#id-1.11.6.8.4.
- Module tsearch2 – Amazon RDS continue de fournir le module `tsearch2` dans la version 10 de PostgreSQL, mais ce module sera supprimé dans la prochaine mise à jour de version majeure. Si votre application utilise des fonctions tsearch2, mettez-la à jour afin d'utiliser les fonctions équivalentes fournies par le moteur principal. Pour plus d'informations sur l'utilisation de `tsearch2`, consultez Module tsearch2.

Pour obtenir la liste complète des extensions désormais prises en charge par Amazon RDS pour PostgreSQL, consultez Fonctions et extensions PostgreSQL prises en charge (p. 1488).

Versions de PostgreSQL 9.6

Versions mineures

- PostgreSQL version 9.6.19 sur Amazon RDS (p. 1479)
- PostgreSQL version 9.6.18 sur Amazon RDS (p. 1479)
- PostgreSQL version 9.6.17 sur Amazon RDS (p. 1479)
- PostgreSQL version 9.6.16 sur Amazon RDS (p. 1479)
- PostgreSQL version 9.6.15 sur Amazon RDS (p. 1479)
- PostgreSQL version 9.6.14 sur Amazon RDS (p. 1480)

- PostgreSQL version 9.6.12 sur Amazon RDS (p. 1480)
- PostgreSQL version 9.6.11 sur Amazon RDS (p. 1480)
- PostgreSQL version 9.6.10 sur Amazon RDS (p. 1480)
- PostgreSQL version 9.6.9 sur Amazon RDS (p. 1480)
- PostgreSQL version 9.6.8 sur Amazon RDS (p. 1481)
- PostgreSQL version 9.6.6 sur Amazon RDS (p. 1481)
- PostgreSQL version 9.6.5 sur Amazon RDS (p. 1481)
- PostgreSQL version 9.6.3 sur Amazon RDS (p. 1482)
- PostgreSQL version 9.6.2 sur Amazon RDS (p. 1482)
- PostgreSQL version 9.6.1 sur Amazon RDS (p. 1482)

PostgreSQL version 9.6.19 sur Amazon RDS

PostgreSQL version 9.6.19 est désormais disponible sur Amazon RDS. PostgreSQL version 9.6.19 contient plusieurs améliorations annoncées pour la version 9.6.19 de PostgreSQL.

Cette version inclut également les modifications suivantes :

1. Mise à niveau de l'extension `pgaudit` vers la version 1.1.2.
2. Mise à niveau de l'extension `pglogical` vers la version 2.2.2.
3. Mise à niveau du module `wal2json` vers la version 2.3

Pour de plus amples informations sur les extensions et les modules, veuillez consulter Extensions et modules PostgreSQL version 9.6.x pris en charge sur Amazon RDS (p. 1500).

PostgreSQL version 9.6.18 sur Amazon RDS

PostgreSQL version 9.6.18 contient plusieurs correctifs de bogues pour palier aux problèmes de la version 9.6.17. Pour de plus amples informations sur les correctifs de PostgreSQL 9.6.18, veuillez consulter la documentation PostgreSQL 9.6.18.

Cette version inclut également la modification suivante :

1. Mise à jour de l'extension `pg_hint_plan` vers la version 1.2.6.

Pour de plus amples informations sur les extensions et les modules, veuillez consulter Extensions et modules PostgreSQL version 9.6.x pris en charge sur Amazon RDS (p. 1500).

PostgreSQL version 9.6.17 sur Amazon RDS

PostgreSQL version 9.6.17 contient plusieurs correctifs de bogues pour palier aux problèmes de la version 9.6.16. Pour de plus amples informations sur les correctifs de PostgreSQL 9.6.17, veuillez consulter la documentation PostgreSQL 9.6.17.

PostgreSQL version 9.6.16 sur Amazon RDS

PostgreSQL version 9.6.16 contient plusieurs correctifs de bogues pour les problèmes de la version 9.6.15. Pour de plus amples informations sur les correctifs de PostgreSQL 9.6.16, veuillez consulter la documentation PostgreSQL.

PostgreSQL version 9.6.15 sur Amazon RDS

PostgreSQL version 9.6.15 contient plusieurs correctifs de bogues pour les problèmes de la version 9.6.14. Pour de plus amples informations sur les correctifs de PostgreSQL 9.6.15, veuillez consulter la documentation PostgreSQL.

L'extension `PostGIS` a été mise à jour vers la version 2.5.2.

PostgreSQL version 9.6.14 sur Amazon RDS

Cette version contient des correctifs de bogue et des améliorations mises au point par la communauté PostgreSQL.

Avec cette version, l'extension `pg_hint_plan` a été mise à jour vers la version 1.2.5.

Pour plus d'informations sur les correctifs de PostgreSQL 9.6.14, consultez la documentation sur PostgreSQL.

PostgreSQL version 9.6.12 sur Amazon RDS

PostgreSQL version 9.6.12 contient plusieurs correctifs de bogues pour les problèmes de la version 9.6.11. Pour de plus amples informations sur les correctifs de la version 9.6.12, veuillez consulter la documentation PostgreSQL.

Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

PostgreSQL version 9.6.11 sur Amazon RDS

PostgreSQL version 9.6.11 contient plusieurs correctifs de bogues pour les problèmes de la version 9.6.10. Pour plus d'informations sur les correctifs de PostgreSQL 9.6.11, consultez la documentation sur PostgreSQL. Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

Avec cette version, le plug-in de décodage logique `wal2json` a été mis à jour pour prendre en charge commit `9e962ba`.

Pour obtenir la liste complète des extensions désormais prises en charge par Amazon RDS pour PostgreSQL, consultez Fonctions et extensions PostgreSQL prises en charge (p. 1488).

PostgreSQL version 9.6.10 sur Amazon RDS

PostgreSQL version 9.6.10 contient plusieurs correctifs de bogues pour les problèmes de la version 9.6.9. Pour plus d'informations sur les correctifs de la version 9.6.10, consultez la documentation sur PostgreSQL.

Cette version inclut les modifications suivantes :

- Prise en charge de l'extension `pglogical` version 2.2.0. Les prérequis pour pouvoir utiliser cette extension sont les mêmes que ceux nécessaires pour utiliser la réplication logique pour PostgreSQL, comme décrit dans Réplication logique pour PostgreSQL sur Amazon RDS (p. 1510).
- Prise en charge de l'extension `pg_similarity` version 2.2.0.
- Mise à jour de l'extension `wal2json` vers la version 01c5c1e.
- Une mise à jour de l'extension `pg_hint_plan` à la version 1.2.3.

Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

Pour obtenir la liste complète des extensions désormais prises en charge par Amazon RDS pour PostgreSQL, consultez Fonctions et extensions PostgreSQL prises en charge (p. 1488).

PostgreSQL version 9.6.9 sur Amazon RDS

PostgreSQL version 9.6.9 contient plusieurs correctifs de bogues pour les problèmes de la version 9.6.8. Pour plus d'informations sur les correctifs de la version 9.6.9, consultez la documentation sur PostgreSQL.

Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

Cette version inclut les modifications suivantes :

- La limite de taille du fichier temporaire peut être configurée par l'utilisateur. Vous devez disposer du rôle rds_superuser pour pouvoir modifier le paramètre `temp_file_limit`.
- Mettez à jour la bibliothèque `GDAL`, qui est utilisée par l'extension PostGIS. Voir Utilisation de PostGIS (p. 1443).
- Mise à jour de l'extension `ip4r` à la version 2.1.1.
- Mise à jour de l'extension `pgaudit` à la version 1.1.1. Voir Utilisation de l'extension pgaudit (p. 1440).

  Mise à jour de l'extension `pg_repack` à la version 1.4.3. Voir Utilisation de l'extension pg_repack (p. 1442).
- Mise à jour de l'extension `plv8` à la version 2.1.2.

Pour obtenir la liste complète des extensions désormais prises en charge par Amazon RDS pour PostgreSQL, consultez Fonctions et extensions PostgreSQL prises en charge (p. 1488).

PostgreSQL version 9.6.8 sur Amazon RDS

PostgreSQL version 9.6.8 contient plusieurs correctifs de bogues pour les problèmes de la version 9.6.6. Pour plus d'informations sur les correctifs de la version 9.6.8, consultez la documentation sur PostgreSQL. Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

Pour obtenir la liste complète des extensions désormais prises en charge par Amazon RDS pour PostgreSQL, consultez Fonctions et extensions PostgreSQL prises en charge (p. 1488).

PostgreSQL version 9.6.6 sur Amazon RDS

PostgreSQL version 9.6.6 contient plusieurs correctifs de bogues pour les problèmes de la version 9.6.5. Pour plus d'informations sur les correctifs de la version 9.6.6, consultez la documentation sur PostgreSQL. Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

Cette version comprend les fonctions suivantes :

- Prend en charge l'extension `orafce`, version 3.6.1. Cette extension contient des fonctions héritées des bases de données commerciales. Elle peut vous aider si vous portez une base de données commerciale vers PostgreSQL. Pour de plus amples informations sur l'utilisation de `orafce` avec Amazon RDS, veuillez consulter Utilisation de l'extension orafce (p. 1446).
- Prend en charge l'extension `prefix`, version 1.2.6. Cette extension fournit un opérateur pour les recherches de préfixe de texte. Pour plus d'informations sur `prefix`, consultez le projet de préfixe sur GitHub.
- Prise en charge de la version 2.3.4 de PostGIS, de la version 2.4.2 de pgrouting et d'une version mise à jour de wal2json.

Pour obtenir la liste complète des extensions désormais prises en charge par Amazon RDS pour PostgreSQL, consultez Fonctions et extensions PostgreSQL prises en charge (p. 1488).

PostgreSQL version 9.6.5 sur Amazon RDS

PostgreSQL version 9.6.5 contient plusieurs correctifs de bogues pour les problèmes de la version 9.6.4. Pour plus d'informations sur les correctifs de la version 9.6.5, consultez la documentation sur PostgreSQL. Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

Cette version inclut également la prise en charge des extensions pgrouting et postgresql-hll, ainsi que du module facultatif decoder_raw.

Pour obtenir la liste complète des extensions désormais prises en charge par Amazon RDS pour PostgreSQL, consultez Fonctions et extensions PostgreSQL prises en charge (p. 1488).

PostgreSQL version 9.6.3 sur Amazon RDS

PostgreSQL version 9.6.3 contient plusieurs nouvelles fonctions et correctifs de bogues. Cette version comprend les fonctions suivantes :

- Prend en charge l'extension `pg_repack`, version 1.4.0. Vous pouvez utiliser cette extension pour éliminer la distension des tableaux et des index. Pour plus d'informations sur l'utilisation de `pg_repack` avec Amazon RDS, consultez Utilisation de l'extension pg_repack (p. 1442).
- Prend en charge l'extension `pgaudit`, version 1.1.0. Cette extension fournit une session détaillée et la journalisation d'audit d'objet. Pour plus d'informations sur l'utilisation de pgaudit avec Amazon RDS, consultez Utilisation de l'extension pgaudit (p. 1440).
- Prise en charge de `wal2json`, un plug-in de sortie pour le décodage logique.
- Prise en charge du module `auto_explain`. Vous pouvez utiliser ce module pour journaliser automatiquement les plans d'exécution d'instructions lentes. L'exemple suivant montre comment utiliser `auto_explain` depuis une session Amazon RDS PostgreSQL :

  ```
  LOAD '$libdir/plugins/auto_explain';
  ```

  Pour plus d'informations sur l'utilisation de `auto_explain`, consultez la documentation PostgreSQL.

PostgreSQL version 9.6.2 sur Amazon RDS

PostgreSQL version 9.6.2 contient plusieurs nouvelles fonctions et correctifs de bogues. La nouvelle version inclut également les versions d'extension suivantes :

- PostGIS version 2.3.2
- pg_freespacemap version 1.1–Permet d'examiner la carte de l'espace disponible. Cette extension fournit une fonction surchargée appelée pg_freespace. Les fonctions affichent la valeur enregistrée dans la carte de l'espace disponible pour une page donnée ou pour toutes les pages de la relation.
- pg_hint_plan version 1.1.3–Permet de contrôler les plans d'exécution en utilisant des expressions pertinentes au début des instructions SQL.
- log_fdw version 1.0–Avec cette extension d'Amazon RDS, vous pouvez charger et interroger le journal de votre moteur de base de données à partir de la base de données. Pour plus d'informations, consultez Utilisation de l'extension log_fdw (p. 1506).
- Cette version vous permet désormais de modifier le paramètre `max_worker_processes` dans un groupe de paramètres de base de données.

PostgreSQL version 9.6.2 sur Amazon RDS prend également en charge la modification des valeur enum. Pour plus d'informations, consultez ALTER ENUM pour PostgreSQL (p. 1514).

Pour plus d'informations sur les correctifs de la version 9.6.2, consultez la documentation sur PostgreSQL. Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

PostgreSQL version 9.6.1 sur Amazon RDS

PostgreSQL version 9.6.1 contient plusieurs nouvelles fonctions et améliorations. Pour plus d'informations sur les correctifs et les améliorations dans PostgreSQL 9.6.1, consultez la documentation de PostgreSQL.

Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515). Pour des informations sur l'exécution de requêtes parallèles et de recherche d'expressions à l'aide d'Amazon RDS pour PostgreSQL 9.6.1, consultez le blog AWS Database.

PostgreSQL version 9.6.1 inclut les modifications suivantes :

- Traitement des requêtes en parallèle : Prend en charge le traitement en parallèle d'importantes requêtes en lecture seule, ce qui permet d'exécuter en parallèle des analyses séquentielles, des jointures par hachage, des boucles imbriquées et des regroupements. Par défaut, le traitement des requêtes en parallèle n'est pas activé. Pour activer le traitement des requêtes en parallèle, définissez le paramètre `max_parallel_workers_per_gather` sur une valeur supérieure à zéro.
- Extension postgres_fdw mise à jour : Prend en charge les opérations JOIN, SORT, UPDATE et DELETE à distance.
- Mise à jour PL/v8 : Fournit la version 1.5.3 du langage PL/v8.
- Mise à jour de la version PostGIS : Prend en charge POSTGIS="2.3.0 r15146" GEOS="3.5.0-CAPI-1.9.0 r4084" PROJ="Rel. 4.9.2, 08 septembre 2015" GDAL="GDAL 2.1.1, publié le 07/07/2016" LIBXML="2.9.1" LIBJSON="0.12" RASTER
- Amélioration Vacuum : Évite la numérisation inutile de pages lors d'opérations de gel vacuum.
- Prise en charge de la recherche en texte intégral pour les expressions : Prend en charge la capacité d'indiquer une requête de recherche d'expression dans l'entrée tsquery à l'aide des nouveaux opérateurs <-> et <N>.
- Deux nouvelles extensions sont prises en charge :
  - `bloom`, une méthode d'accès d'index basée sur des filtres Bloom
  - `pg_visibility`, qui fournit un moyen d'examiner la carte de visibilité et les informations de visibilité de niveau page d'une table.
- La version 9.6.2 vous permet désormais de modifier le paramètre `max_worker_processes` dans un groupe de paramètres de base de données PostgreSQL version 9.6.1.

Vous pouvez créer une instance de base de données PostgreSQL 9.6.1 à l'aide de la AWS Management Console, de l'AWS CLI, ou de l'API RDS. Vous pouvez également mettre à niveau une instance existante de PostgreSQL 9.5 vers la version 9.6.1 à l'aide d'une mise à niveau de version majeure. Si vous souhaitez mettre à niveau une instance de base de données de la version 9.4 vers la version 9.6, vous devez tout d'abord effectuer une mise à niveau par pointer-cliquer vers la version majeure suivante. Chaque opération de mise à niveau implique une courte période d'indisponibilité pour votre instance de base de données.

Versions de PostgreSQL 9.5

Versions mineures

- PostgreSQL version 9.5.23 sur Amazon RDS (p. 1484)
- PostgreSQL version 9.5.22 sur Amazon RDS (p. 1484)
- PostgreSQL version 9.5.21 sur Amazon RDS (p. 1484)
- PostgreSQL version 9.5.20 sur Amazon RDS (p. 1484)
- PostgreSQL version 9.5.19 sur Amazon RDS (p. 1484)
- PostgreSQL version 9.5.18 sur Amazon RDS (p. 1484)
- PostgreSQL version 9.5.16 sur Amazon RDS (p. 1485)
- PostgreSQL version 9.5.15 sur Amazon RDS (p. 1485)

- PostgreSQL version 9.5.14 sur Amazon RDS (p. 1485)
- PostgreSQL version 9.5.13 sur Amazon RDS (p. 1485)
- PostgreSQL version 9.5.12 sur Amazon RDS (p. 1485)
- PostgreSQL version 9.5.10 sur Amazon RDS (p. 1486)
- PostgreSQL version 9.5.9 sur Amazon RDS (p. 1486)
- PostgreSQL version 9.5.7 sur Amazon RDS (p. 1486)
- PostgreSQL version 9.5.6 sur Amazon RDS (p. 1486)
- PostgreSQL version 9.5.4 sur Amazon RDS (p. 1486)
- PostgreSQL version 9.5.2 sur Amazon RDS (p. 1487)

PostgreSQL version 9.5.23 sur Amazon RDS

PostgreSQL version 9.5.23 est désormais disponible sur Amazon RDS. PostgreSQL version 9.5.23 contient plusieurs améliorations annoncées pour la version 9.5.23 de PostgreSQL.

Pour de plus amples informations sur les extensions et les modules, veuillez consulter Extensions PostgreSQL version 9.5.x prises en charge sur Amazon RDS (p. 1502).

PostgreSQL version 9.5.22 sur Amazon RDS

PostgreSQL version 9.5.22 contient plusieurs correctifs de bogues pour palier aux problèmes de la version 9.5.21. Pour de plus amples informations sur les correctifs de PostgreSQL 9.5.22, veuillez consulter la documentation PostgreSQL 9.5.22.

Cette version inclut également la modification suivante :

1. Mise à jour de l'extension `pg_hint_plan` vers la version 1.1.9.

Pour de plus amples informations sur les extensions et les modules, veuillez consulter Extensions PostgreSQL version 9.5.x prises en charge sur Amazon RDS (p. 1502).

PostgreSQL version 9.5.21 sur Amazon RDS

PostgreSQL version 9.5.21 contient plusieurs correctifs de bogues pour palier aux problèmes de la version 9.5.20. Pour de plus amples informations sur les correctifs de PostgreSQL 9.5.21, veuillez consulter la documentation PostgreSQL 9.5.21.

PostgreSQL version 9.5.20 sur Amazon RDS

PostgreSQL version 9.5.20 contient plusieurs correctifs de bogue pour palier aux problèmes de la version 9.5.19. Pour de plus amples informations sur les correctifs de PostgreSQL 9.5.20, veuillez consulter la documentation PostgreSQL.

PostgreSQL version 9.5.19 sur Amazon RDS

PostgreSQL version 9.5.19 contient plusieurs correctifs de bogue pour palier aux problèmes de la version 9.5.18. Pour de plus amples informations sur les correctifs de PostgreSQL 9.5.19, veuillez consulter la documentation PostgreSQL.

L'extension `PostGIS` a été mise à jour vers la version 2.5.2.

PostgreSQL version 9.5.18 sur Amazon RDS

Cette version contient des correctifs de bogue et des améliorations mises au point par la communauté PostgreSQL.

Avec cette version, l'extension `pg_hint_plan` a été mise à jour vers la version 1.1.8.

Pour plus d'informations sur les correctifs de PostgreSQL 9.5.18, consultez la documentation sur PostgreSQL.

PostgreSQL version 9.5.16 sur Amazon RDS

PostgreSQL version 9.5.16 contient plusieurs correctifs de bogues pour les problèmes de la version 9.5.15. Pour de plus amples informations sur les correctifs de la version 9.5.16, veuillez consulter la documentation sur PostgreSQL. Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

Pour obtenir la liste complète des extensions désormais prises en charge par Amazon RDS pour PostgreSQL, consultez Fonctions et extensions PostgreSQL prises en charge (p. 1488).

PostgreSQL version 9.5.15 sur Amazon RDS

PostgreSQL version 9.5.15 contient plusieurs correctifs de bogues pour les problèmes de la version 9.5.14. Pour plus d'informations sur les correctifs de la version 9.5.15, consultez la documentation sur PostgreSQL. Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

Pour obtenir la liste complète des extensions désormais prises en charge par Amazon RDS pour PostgreSQL, consultez Fonctions et extensions PostgreSQL prises en charge (p. 1488).

PostgreSQL version 9.5.14 sur Amazon RDS

PostgreSQL version 9.5.14 contient plusieurs correctifs de bogues pour les problèmes de la version 9.5.13. Pour plus d'informations sur les correctifs de la version 9.5.14, consultez la documentation sur PostgreSQL.

Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

Pour obtenir la liste complète des extensions désormais prises en charge par Amazon RDS pour PostgreSQL, consultez Fonctions et extensions PostgreSQL prises en charge (p. 1488).

PostgreSQL version 9.5.13 sur Amazon RDS

PostgreSQL version 9.5.13 contient plusieurs correctifs de bogues pour les problèmes de la version 9.5.12. Pour plus d'informations sur les correctifs de la version 9.5.13, consultez la documentation sur PostgreSQL. Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

Cette version inclut également les mises à jour d'extensions suivantes :

- Mise à jour de l'extension `pgaudit` à la version 1.0.6. Voir Utilisation de l'extension pgaudit (p. 1440).
- Mise à jour de l'extension `pg_hint_plan` à la version 1.1.5.
- Mise à jour de l'extension `plv8` à la version 2.1.2.

Pour obtenir la liste complète des extensions désormais prises en charge par Amazon RDS pour PostgreSQL, consultez Fonctions et extensions PostgreSQL prises en charge (p. 1488).

PostgreSQL version 9.5.12 sur Amazon RDS

La version 9.5.12 de PostgreSQL contient plusieurs correctifs de bogues identifiés dans la version 9.5.10 Pour plus d'informations sur les correctifs dans la version 9.5.12, consultez la documentation PostgreSQL. Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

Pour obtenir la liste complète des extensions désormais prises en charge par Amazon RDS pour PostgreSQL, consultez Fonctions et extensions PostgreSQL prises en charge (p. 1488).

PostgreSQL version 9.5.10 sur Amazon RDS

La version 9.5.10 de PostgreSQL contient plusieurs correctifs de bogues pour les problèmes de la version 9.5.9. Pour plus d'informations sur les correctifs de la version 9.5.10, consultez la documentation sur PostgreSQL. Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

PostgreSQL version 9.5.9 sur Amazon RDS

La version 9.5.9 de PostgreSQL contient plusieurs correctifs de bogues pour les problèmes dans la version 9.5.8. Pour plus d'informations sur les correctifs de la version 9.5.9, consultez la documentation sur PostgreSQL. Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

PostgreSQL version 9.5.7 sur Amazon RDS

PostgreSQL version 9.5.7 contient plusieurs nouvelles fonctions et correctifs de bogues. Cette version comprend les fonctions suivantes :

- Prend en charge l'extension `pgaudit`, version 1.0.5. Cette extension fournit une session détaillée et la journalisation d'audit d'objet. Pour plus d'informations sur l'utilisation de `pgaudit` avec Amazon RDS, consultez Utilisation de l'extension pgaudit (p. 1440).
- Prise en charge de `wal2json`, un plug-in de sortie pour le décodage logique.
- Prise en charge du module `auto_explain`. Vous pouvez utiliser ce module pour journaliser automatiquement les plans d'exécution d'instructions lentes. L'exemple suivant montre comment utiliser `auto_explain` depuis une session Amazon RDS PostgreSQL.

```
LOAD '$libdir/plugins/auto_explain';
```

  Pour plus d'informations sur l'utilisation de `auto_explain`, consultez la documentation PostgreSQL.

PostgreSQL version 9.5.6 sur Amazon RDS

PostgreSQL version 9.5.6 contient plusieurs nouvelles fonctions et correctifs de bogues. La nouvelle version inclut également les versions d'extension suivantes :

- PostGIS version 2.2.5
- pg_freespacemap version 1.1–Permet d'examiner la carte de l'espace disponible. Cette extension fournit une fonction surchargée appelée pg_freespace. Cette fonction affiche la valeur enregistrée dans la carte de l'espace disponible pour une page donnée ou pour toutes les pages de la relation.
- pg_hint_plan version 1.1.3–Permet de contrôler les plans d'exécution en utilisant des expressions pertinentes au début des instructions SQL.

PostgreSQL version 9.5.6 sur Amazon RDS prend également en charge la modification des valeur enum. Pour plus d'informations, consultez ALTER ENUM pour PostgreSQL (p. 1514).

Pour plus d'informations sur les correctifs de la version 9.5.6, consultez la documentation sur PostgreSQL. Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

PostgreSQL version 9.5.4 sur Amazon RDS

PostgreSQL version 9.5.4 contient plusieurs correctifs de problèmes détectés dans les versions précédentes. Pour plus d'informations sur les correctifs de la version 9.5.4, consultez la documentation sur PostgreSQL. Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

PostgreSQL prend en charge la diffusion en continu des modifications WAL à l'aide du décodage de réplication logique. Amazon RDS prend en charge la réplication logique pour PostgreSQL 9.5.4 et versions ultérieures. Pour plus d'informations sur la réplication logique PostgreSQL sur Amazon RDS, consultez Réplication logique pour PostgreSQL sur Amazon RDS (p. 1510).

À partir de PostgreSQL version 9.5.4 pour Amazon RDS, la commande ALTER USER WITH BYPASSRLS est prise en charge.

PostgreSQL 9.5.4 et versions ultérieures prend en charge les déclencheurs d'événement et Amazon RDS prend en charge les déclencheurs d'événement pour ces versions. Vous pouvez utiliser le compte d'utilisateur principal pour créer, modifier, renommer et supprimer des déclencheurs d'événements. Les déclencheurs d'événements sont au niveau de l'instance de base de données, de sorte qu'ils peuvent s'appliquer à toutes les bases de données sur une instance. Pour plus d'informations sur les déclencheurs d'événements PostgreSQL sur Amazon RDS, consultez Déclencheurs d'événements pour PostgreSQL sur Amazon RDS (p. 1512).

PostgreSQL version 9.5.2 sur Amazon RDS

PostgreSQL version 9.5.2 contient plusieurs correctifs de problèmes détectés dans les versions précédentes. Pour plus d'informations sur les fonctions de la version 9.5.2, consultez la documentation sur PostgreSQL. Pour plus d'informations sur la mise à niveau du moteur pour votre instance de base de données PostgreSQL, consultez Mise à niveau d'une instance de base de données PostgreSQL (p. 1515).

PostgreSQL version 9.5.2 ne prend pas en charge les classes d'instance de base de données db.m1 ou db.m2. Si vous avez besoin de mettre à niveau une instance de base de données exécutant PostgreSQL version 9.4 vers la version 9.5.2 vers l'une de ces classes d'instance, vous devez mettre à l'échelle le calcul. Pour ce faire, vous avez besoin d'une classe d'instance de base de données db.t2 ou db.m3 comparable pour pouvoir mettre à niveau une instance de base de données exécutant la version 9.4 de PostgreSQL vers la version 9.5.2. Pour plus d'informations sur les classes d'instance de base de données, consultez Classes d'instances de base de données (p. 6).

La version native PostgreSQL version 9.5.2 a introduit la commande ALTER USER WITH BYPASSRLS.

Cette version inclut les mises à jour issues des versions précédentes, dont notamment les suivantes :

- CVE-2016-2193 : Corrige un problème selon lequel un plan de requête peut être réutilisé pour plusieurs RÔLES dans la même session. En raison de la réutilisation d'un plan de requête, la requête peut utiliser un ensemble erroné de stratégies RLS (Row Level Security).
- CVE-2016-3065 : Corrige un bogue de défaillance du serveur déclenché par l'utilisation de `pageinspect` avec les pages d'index BRIN. Comme un attaquant peut être en mesure d'exposer quelques octets de mémoire du serveur, cette défaillance est traitée comme un problème de sécurité.

Les améliorations majeures apportées à RDS PostgreSQL 9.5 incluent les suivantes :

- UPSERT : permet d'ignorer des commandes INSERT susceptibles de générer des conflits de contraintes ou de les transformer en commandes UPDATE
- Ajout des fonctions d'analyse GROUP BY : GROUPING SETS, CUBE et ROLLUP
- Ajout du contrôle de sécurité au niveau des lignes
- Création de mécanismes pour le suivi de l'avancement de la réplication, y compris des méthodes pour identifier l'origine des modifications individuelles au cours de la réplication logique
- Ajout des index de plage de bloc BRIN (Block Range Indexes)
- Ajout d'améliorations de performance substantielles pour le tri
- Ajout d'améliorations de performance substantielles pour les ordinateurs à plusieurs UC
- PostGIS 2.2.2 - Pour utiliser la dernière version de PostGIS, utilisez l'instruction ALTER EXTENSION UPDATE pour effectuer une mise à jour après la mise à niveau vers la version 9.5.2. Exemple :

  ALTER EXTENSION POSTGIS UPDATE TO '2.2.2'

- Amélioration de la visibilité des sessions autovacuum via l'autorisation du compte rds_superuser à visualiser les sessions autovacuum dans pg_stat_activity. Par exemple, vous pouvez identifier et résilier la session qui bloque l'exécution d'une commande ou empêche la commande de s'exécuter plus lentement qu'une commande vacuum exécutée manuellement.

RDS PostgreSQL version 9.5.2 inclut les nouvelles extensions suivantes :

- address_standardizer – Analyseur d'adresse sur une seule ligne qui prend une adresse d'entrée et la normalise en fonction d'un ensemble de règles stockées dans un tableau, un tableau de lexique d'assistant et les tableaux gaz.
- hstore_plperl – Fournit des transformations pour le type `hstore` pour PL/Perl.
- tsm_system_rows – Fournit la méthode d'échantillonnage de tableau `SYSTEM_ROWS`, qui peut être utilisée dans la clause `TABLESAMPLE` d'une commande `SELECT`.
- tsm_system_time – Fournit la méthode d'échantillonnage de tableau `SYSTEM_TIME`, qui peut être utilisée dans la clause `TABLESAMPLE` d'une commande `SELECT`.

Fonctions et extensions PostgreSQL prises en charge

Amazon RDS prend en charge un grand nombre d'extensions et de fonctionnalités PostgreSQL parmi les plus courantes.

Rubriques

- Extensions et modules PostgreSQL pris en charge sur Amazon RDS (p. 1488)
- Mise à niveau de PL/v8 (p. 1507)
- Fonctions PostgreSQL prises en charge (p. 1509)
- Limites pour les instances de bases de données PostgreSQL (p. 1514)
- Mise à niveau d'une instance de base de données PostgreSQL (p. 1515)
- Utilisation de SSL avec une instance de base de données PostgreSQL (p. 1515)

Extensions et modules PostgreSQL pris en charge sur Amazon RDS

PostgreSQL prend en charge de nombreux modules et extensions PostgreSQL. Les modules et extensions complètent la fonctionnalité fournie par le moteur PostgreSQL. Les sections suivantes présentent les extensions et modules pris en charge par Amazon RDS pour les versions majeures de PostgreSQL.

Rubriques

- Extensions et modules PostgreSQL version 13 pris en charge sur Amazon RDS (p. 1489)
- Extensions et modules PostgreSQL version 12 pris en charge sur Amazon RDS (p. 1491)
- Extensions et modules PostgreSQL version 11.x pris en charge sur Amazon RDS (p. 1494)
- Extensions et modules PostgreSQL version 10.x pris en charge sur Amazon RDS (p. 1496)
- Extensions et modules PostgreSQL version 9.6.x pris en charge sur Amazon RDS (p. 1500)
- Extensions PostgreSQL version 9.5.x prises en charge sur Amazon RDS (p. 1502)
- Prise en charge des extensions PostgreSQL pour PostGIS sur Amazon RDS (p. 1504)
- Utilisation de l'extension log_fdw (p. 1506)

Vous trouverez une liste des extensions prises en charge par Amazon RDS dans le groupe de paramètres de base de données par défaut pour cette version de PostgreSQL. Vous pouvez également consulter

la liste actuelle des extensions utilisant `psql` en affichant le paramètre `rds.extensions` comme dans l'exemple suivant.

```
SHOW rds.extensions;
```

> **Note**
>
> Les paramètres ajoutés à une version mineure peuvent s'afficher de manière incorrecte lors de l'utilisation du paramètre `rds.extensions` dans `psql`.

Extensions et modules PostgreSQL version 13 pris en charge sur Amazon RDS

Le tableau suivant affiche les extensions et modules PostgreSQL pour PostgreSQL version 13 qui sont actuellement pris en charge sur Amazon RDS. Pour de plus amples informations sur les extensions PostgreSQL, veuillez consulter Packaging Related Objects into an Extension (Emballage d'objets associés dans une extension).

Extensions et modules	Version 13 bêta 3
address_standardizer	3.0.2
address_standardizer_data_us	3.0.2
Module amcheck	1.2
aws_commons : veuillez consulter Importation de données dans PostgreSQL sur Amazon RDS	1.0
aws_s3 : veuillez consulter Importation de données dans PostgreSQL sur Amazon RDS	1.0
bloom	1.0
btree_gin	1.3
btree_gist	1.5
citext	1.6
cube	1.4
dblink	1.2
dict_int	1.0
dict_xsyn	1.0
earthdistance	1.1
fuzzystrmatch	1.1
hstore	1,7
hstore_plperl	1.0
intagg	1.1
intarray	1.3
ip4r	2,4

Extensions et modules	Version 13 bêta 3
isn	1.2
jsonb_plperl	1.0
log_fdw—voir Utilisation de l'extension log_fdw (p. 1506)	1.2
ltree	1.2
pageinspect	1.8
pg_buffercache	1.3
pg_freespacemap	1.2
pg_prewarm	1.2
pg_similarity	1.0
pg_stat_statements	1.8
pg_transport — voir Transport de bases de données PostgreSQL entre des instances de base de données (p. 1405)	1.0
pg_trgm	1.5
pg_visibility	1.2
pgaudit	1.5
pgcrypto	1.3
pgrouting	3.0.0
pgrowlocks	1.2
pgstattuple	1.5
pgTAP	1.1.0
plcoffee	2.3.15
plls	2.3.15
plperl	1.0
plpgsql	1.0
plprofiler	4.1
pltcl	1.0
plv8	2.3.15
PostGIS	3.0.2
postgis_raster	3.0.2
postgis_tiger_geocoder	3.0.2

Extensions et modules	Version 13 bêta 3
postgis_topology	3.0.2
postgres_fdw	1.0
prefix	1.2.0
rdkit	3.8
sslinfo	1.2
tablefunc	1.0
test_parser	1.0
tsm_system_rows	1.0
tsm_system_time	1.0
unaccent	1.1
uuid-ossp	1.1

Extensions et modules PostgreSQL version 12 pris en charge sur Amazon RDS

Le tableau suivant affiche les extensions et modules PostgreSQL pour PostgreSQL version 12 qui sont actuellement pris en charge sur Amazon RDS. Pour de plus amples informations sur les extensions PostgreSQL, veuillez consulter Packaging Related Objects into an Extension (Emballage d'objets associés dans une extension).

Extensions et modules	12.2	12.3	12.4
address_standardizer	3.0.0	3.0.0	3.0.0
address_standardizer_data_us	3.0.0	3.0.0	3.0.0
Module amcheck	1.2	1.2	1.2
aws_commons : veuillez consulter Importation de données dans PostgreSQL sur Amazon RDS	1.0	1.0	1.0
aws_s3 : veuillez consulter Importation de données dans PostgreSQL sur Amazon RDS	1.0	1.0	1.1
bloom	1.0	1.0	1.0
btree_gin	1.3	1.3	1.3
btree_gist	1.5	1.5	1.5
citext	1.6	1.6	1.6

Extensions et modules	12.2	12.3	12.4
cube	1.4	1.4	1.4
dblink	1.2	1.2	1.2
dict_int	1.0	1.0	1.0
dict_xsyn	1.0	1.0	1.0
earthdistance	1.1	1.1	1.1
fuzzystrmatch	1.1	1.1	1.1
hll	2.14	2.14	2.14
hstore	1.6	1.6	1.6
hstore_plperl	1.0	1.0	1.0
intagg	1.1	1.1	1.1
intarray	1.2	1.2	1.2
ip4r	2,4	2,4	2,4
isn	1.2	1.2	1.2
jsonb_plperl	1.0	1.0	1.0
log_fdw—voir Utilisation de l'extension log_fdw (p. 1506)	1.1	1.1	1.1
ltree	1.1	1.1	1.1
orafce	3.8	3.8	3.8
pageinspect	1.7	1.7	1.7
pg_buffercache	1.3	1.3	1.3
pg_freespacemap	1.2	1.2	1.2
pg_hint_plan	1.3.4	1.3.5	1.3.5
pg_prewarm	1.2	1.2	1.2
pg_proctab	NA	NA	0.0.9
pg_repack	1.4.5	1.4.5	1.4.5
pg_similarity	1.0	1.0	1.0
pg_stat_statements	1.7	1.7	1.7
pg_transport — voir Transport de bases de données PostgreSQL entre des instances de base de données (p. 1405)	1.0	1.0	1.0

Extensions et modules	12.2	12.3	12.4
pg_trgm	1.4	1.4	1.4
pg_visibility	1.2	1.2	1.2
pgaudit	1.4	1.4	1.4
pgcrypto	1.3	1.3	1.3
pglogical	2.3.0	2.3.1	2.3.2
pgrouting	3.0.0	3.0.0	3.0.0
pgrowlocks	1.2	1.2	1.2
pgstattuple	1.5	1.5	1.5
pgTAP	1.1.0	1.1.0	1.1.0
plcoffee	2.3.14	2.3.14	2.3.14
plls	2.3.14	2.3.14	2.3.14
plperl	1.0	1.0	1.0
plpgsql	1.0	1.0	1.0
plprofiler	4.1	4.1	4.1
pltcl	1.0	1.0	1.0
plv8	2.3.14	2.3.14	2.3.14
PostGIS	3.0.0	3.0.0	3.0.0
postgis_raster	3.0.0	3.0.0	3.0.0
postgis_tiger_geocoder	3.0.0	3.0.0	3.0.0
postgis_topology	3.0.0	3.0.0	3.0.0
postgres_fdw	1.0	1.0	1.0
prefix	1.2.0	1.2.0	1.2.0
rdkit	NA	NA	3.8
sslinfo	1.2	1.2	1.2
tablefunc	1.0	1.0	1.0
test_parser	1.0	1.0	1.0
tsm_system_rows	1.0	1.0	1.0
tsm_system_time	1.0	1.0	1.0
unaccent	1.1	1.1	1.1
uuid-ossp	1.1	1.1	1.1
Module `wal2json`	2.1	2.1	2.3

Extensions et modules PostgreSQL version 11.x pris en charge sur Amazon RDS

Les tableaux suivants affichent les extensions et modules PostgreSQL pour PostgreSQL version 11.x qui sont actuellement pris en charge par PostgreSQL sur Amazon RDS. « s.o. » indique que l'extension ou le module n'est pas disponible pour la version PostgreSQL. Pour de plus amples informations sur les extensions PostgreSQL, veuillez consulter Packaging Related Objects into an Extension (Emballage d'objets associés dans une extension).

Extension	11.1	11.2	11.4	11.5	11.6	11.7	11.8	11.9
address_standardizer	2.5.1	2.5.1	2.5.1	2.5.1	2.5.1	2.5.1	2.5.1	2.5.1
address_standardizer_data_us	2.5.1	2.5.1	2.5.1	2.5.1	2.5.1	2.5.1	2.5.1	2.5.1
aws_s3 : veuillez consulter Importation de données dans PostgreSQL sur Amazon RDS	S/O	S/O	S/O	S/O	S/O	S/O	S/O	1.1
bloom	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
btree_gin	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
btree_gist	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5
citext	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5
cube	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4
dblink	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
dict_int	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
dict_xsyn	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
earthdistance	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
fuzzystrmatch	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
hstore	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5
hstore_plperl	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
intagg	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
intarray	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
ip4r	2.3	2.3	2.3	2.3	2.3	2.3	2.3	2.3
isn	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
log_fdw —voir Utilisation de	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0

Extension	11.1	11.2	11.4	11.5	11.6	11.7	11.8	11.9
l'extension log_fdw (p. 1506)								
libprotobuf	1.3.0	1.3.0	1.3.0	1.3.0	1.3.0	1.3.0	1.3.0	1.3.0
ltree	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
orafce	3.7	3.7	3.7	3.7	3.7	3.8	3.8	3.8
pageinspect	1.6	1.6	1.6	1.6	1.6	1.6	1.6	1.6
pg_buffercache	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
pg_freespacemap	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
pg_hint_plan	1.3.2	1.3.2	1.3.4	1.3.4	1.3.4	1.3.4	1.3.5	1.3.5
pg_prewarm	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
pg_proctab	S/O	S/O	S/O	S/O	S/O	S/O	S/O	0.0.9
pg_repack	1.4.4	1.4.4	1.4.4	1.4.4	1.4.4	1.4.4	1.4.4	1.4.4
pg_similarity	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
pg_stat_statements	1.6	1.6	1.6	1.6	1.6	1.6	1.6	1.6
pg_transport	S/O	S/O	N/A	1.0	1.0	1.0	1.0	1.0
pg_trgm	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4
pg_visibility	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
pgaudit	1.3.0	1.3.0	1.3.0	1.3.0	1.3.0	1.3.0	1.3.0	1.3.1
pgcrypto	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
pglogical	2.2.1	2.2.1	2.2.1	2.2.1	2.2.1	2.2.1	2.2.1	2.2.2
pgrowlocks	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
pgrouting	2.6.1	2.6.1	2.6.1	2.6.1	2.6.1	2.6.1	2.6.1	2.6.1
pgstattuple	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5
pgTAP	S/O	1.0	1.0	1.0	1.1.0	1.1.0	1.1.0	1.1.0
plcoffee	2.3.8	2.3.8	2.3.8	2.3.8	2.3.8	2.3.8	2.3.8	2.3.8
plls	2.3.8	2.3.8	2.3.8	2.3.8	2.3.8	2.3.8	2.3.8	2.3.8
plperl	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
plpgsql	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
plprofiler	S/O	S/O	S/O	S/O	4.1	4.1	4.1	4.1
pltcl	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
plv8	2.3.8	2.3.8	2.3.8	2.3.8	2.3.8	2.3.8	2.3.8	2.3.8
PostGIS	2.5.1	2.5.1	2.5.1	2.5.2	2.5.2	2.5.2	2.5.2	2.5.2

Extension	11.1	11.2	11.4	11.5	11.6	11.7	11.8	11.9
postgis_tiger_geocoder	2.5.1	2.5.1	2.5.1	2.5.1	2.5.1	2.5.1	2.5.1	2.5.1
postgis_topology	2.5.1	2.5.1	2.5.1	2.5.1	2.5.1	2.5.1	2.5.1	2.5.1
postgres_fdw	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
postgresql-hll	2.11	2.11	2.11	2.11	2.11	2.11	2.11	2.11
prefix	1.2.8	1.2.8	1.2.8	1.2.8	1.2.8	1.2.8	1.2.8	1.2.8
rdkit	S/O	S/O	S/O	S/O	S/O	S/O	S/O	3.8
sslinfo	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
tablefunc	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
test_parser	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
tsm_system_rows	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
tsm_system_time	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
unaccent	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
uuid-ossp	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1

Les modules suivants sont pris en charge comme indiqué pour PostgreSQL version 11.x.

Module	11.1	11.2	11.4	11.5	11.6	11.7	11.8	11.9
amcheck	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
auto_explain	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
decoder_raw	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
ICU	Version 60.2 prise en charge	Version 60.2 prise en charge	Version 60.2 prise en charge	Version 60.2 prise en charge	Version 60.2 prise en charge	Version 60.2 prise en charge	Version 60.2 prise en charge	Version 60.2 prise en charge
test_decoding	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
wal2json	Commit hash 9e962bad	Commit hash 9e962bad	Commit hash 9e962bad	Commit hash 9e962bad	Commit hash 9e962bad	version 2.1	version 2.1	version 2.3

Extensions et modules PostgreSQL version 10.x pris en charge sur Amazon RDS

Les tableaux suivants affichent les extensions et modules PostgreSQL pour PostgreSQL version 10 qui sont actuellement pris en charge par PostgreSQL sur Amazon RDS. « s.o. » indique que l'extension ou

le module n'est pas disponible pour la version PostgreSQL. Pour de plus amples informations sur les extensions PostgreSQL, veuillez consulter Packaging Related Objects into an Extension (Emballage d'objets associés dans une extension).

Extensi	10.1	10.3	10.4	10.5	10.6	10.7	10.9	10.10	10.11	10.12	10.13	10.14
address_standardizer	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2
address_standardizer_data_us	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2
aws_s3 veuillez consulter Importation de données dans PostgreSQL sur Amazon RDS	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	1.1
bloom	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
btree_gin	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
btree_gist	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5
chkpass	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
citext	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4
cube	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
dblink	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
dict_int	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
dict_xsyn	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
earthdistance	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
fuzzystrmatch	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
hstore	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4
hstore_plperl	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
intagg	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
intarray	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
ip4r	2.0	2.0	2.1.1	2.1.1	2.1.1	2.1.1	2.1.1	2.1.1	2.1.1	2.1.1	2.1.1	2.1.1
isn	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
log_fdw —voir Utilisation de l'extension log_fdw (p. 1506)	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0

Extensi	10.1	10.3	10.4	10.5	10.6	10.7	10.9	10.10	10.11	10.12	10.13	10.14
libprotobuf	N/A	S/O	N/A	1.3.0	1.3.0	1.3.0	1.3.0	1.3.0	1.3.0	1.3.0	1.3.0	1.3.0
ltree	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
orafce	3.6.1	3.6.1	3.6.1	3.6.1	3.6.1	3.6.1	3.6.1	3.6.1	3.6.1	3.8	3.8	3.8
pgaudit	1.2.0	1.2.0	1.2.0	1.2.0	1.2.0	1.2.0	1.2.0	1.2.0	1.2.0	1.2.0	1.2.0	1.2.1
pg_buffercache	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
pg_freespacemap	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
pg_hint_plan	1.3.0	1.3.0	1.3.0	1.3.1	1.3.1	1.3.1	1.3.3	1.3.3	1.3.3	1.3.3	1.3.5	1.3.5
pg_prewarm	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
pg_repack	1.4.2	1.4.2	1.4.3	1.4.3	1.4.3	1.4.3	1.4.3	1.4.3	1.4.3	1.4.3	1.4.3	1.4.3
pg_similarity	N/A	S/O	N/A	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
pg_stat_statements	1.5	1.5	1.5	1.5	1.6	1.6	1.6	1.6	1.6	1.6	1.6	1.6
pg_transport	S/O	S/O	S/O	S/O	S/O	S/O	N/A	1.0	1.0	1.0	1.0	1.0
pg_trgm	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
pg_visibility	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
pgcrypto	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
pageinspect	N/A	S/O	N/A	1.6	1.6	1.6	1.6	1.6	1.6	1.6	1.6	1.6
pglogical	S/O	S/O	N/A	2.2.0	2.2.0	2.2.0	2.2.0	2.2.0	2.2.0	2.2.0	2.2.0	2.2.2
pgrowlocks	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
pgrouting	2.5.2	2.5.2	2.5.2	2.5.2	2.5.2	2.5.2	2.5.2	2.5.2	2.5.2	2.5.2	2.5.2	2.5.2
pgstattuple	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5
plcoffee	2.1.0	2.1.0	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2
plls	2.1.0	2.1.0	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2
plperl	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
plpgsql	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
plprofiler	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	4.1	4.1	4.1	4.1
pltcl	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
plv8	2.1.0	2.1.0	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2
PostGIS	2.4.2	2.4.2	2.4.4	2.4.4	2.4.4	2.4.4	2.4.4	2.5.2	2.5.2	2.5.2	2.5.2	2.5.2
postgis_tiger_geocoder	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2
postgis_topology	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2
postgres_fdw	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0

Extensi	10.1	10.3	10.4	10.5	10.6	10.7	10.9	10.10	10.11	10.12	10.13	10.14
postgresql-hll	2.10.2	2.10.2	2.10.2	2.10.2	2.10.2	2.10.2	2.10.2	2.10.2	2.10.2	2.10.2	2.10.2	2.10.2
prefix	1.2.0	1.2.0	1.2.0	1.2.0	1.2.0	1.2.0	1.2.0	1.2.0	1.2.0	1.2.0	1.2.0	1.2.0
sslinfo	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
tablefunc	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
test_parser	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
tsearch2 (obsolète dans la version 10)	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
tsm_system_rows	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
tsm_system_time	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
unaccent	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
uuid-ossp	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1

L'extension `tsearch2` est obsolète dans la version 10. L'équipe de PostgreSQL prévoit de retirer `tsearch2` de la prochaine version majeure de PostgreSQL.

Les modules suivants sont pris en charge comme indiqué pour les versions de PostgreSQL 10.

Module	10.1	10.3	10.4	10.5	10.6	10.7	10.9	10.10	10.11	10.12	10.13	10.14
amcheck	Non pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
auto_explain	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
decoderraw	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
ICU	Version 60.2 prise en charge	Version 60.2 prise en charge	Version 60.2 prise en charge	Version 60.2 prise en charge	Version 60.2 prise en charge	Version 60.2 prise en charge	Version 60.2 prise en charge	Version 60.2 prise en charge	Version 60.2 prise en charge	Version 60.2 prise en charge	Version 60.2 prise en charge	Version 60.2 prise en charge
test_decoding	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge

Module	10.1	10.3	10.4	10.5	10.6	10.7	10.9	10.10	10.11	10.12	10.13	10.14
wal2json	Commit hash 5352cc4	Commit hash 5352cc4	Commit hash 5352cc4	Commit hash 401c5c1e	Commit hash 9e962ba	Commit hash 9e962ba	Commit hash 9e962ba	Commit hash 9e962ba	Commit hash 9e962ba	version 2.1	version 2.1	version 2.3

Extensions et modules PostgreSQL version 9.6.x pris en charge sur Amazon RDS

Les tableaux suivants affichent les extensions et modules PostgreSQL pour PostgreSQL version 9.6.x qui sont actuellement pris en charge par PostgreSQL sur Amazon RDS. « s.o. » indique que l'extension ou le module n'est pas disponible pour la version PostgreSQL. Pour de plus amples informations sur les extensions PostgreSQL, veuillez consulter Packaging Related Objects into an Extension (Emballage d'objets associés dans une extension).

Exter	9.6.1	9.6.2	9.6.3	9.6.5	9.6.6	9.6.8	9.6.9	9.6.1	9.6.1	9.6.1	9.6.1	9.6.1	9.6.1	9.6.1	9.6.1	9.6.1	9.6.19
address_standardizer	2.3.0	2.3.2	2.3.2	2.3.2	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4
address_standardizer_data_us	2.3.0	2.3.2	2.3.2	2.3.2	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4
bloom	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
btree_gin	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
btree_gist	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
chkpass	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
citext	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
cube	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
dblink	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
dict_int	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
dict_xsyn	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
earthdistance	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
fuzzystrmatch	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
hstore	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4
hstore_plperl	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
intagg	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
intarray	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
ip4r	2.0	2.0	2.0	2.0	2.0	2.0	2.1.1	2.1.1	2.1.1	2.1.1	2.1.1	2.1.1	2.1.1	2.1.1	2.1.1	2.1.1
isn	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
log_fdw — voir Utilisation de	N/A	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0

Exter	9.6.1	9.6.2	9.6.3	9.6.5	9.6.6	9.6.8	9.6.9	9.6.1	9.6.1	9.6.1	9.6.1	9.6.1	9.6.1	9.6.1	9.6.1	9.6.19
l'extension log_fdw (p. 1506)																
ltree	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
orafce	s.o.	S/O	S/O	s.o.	3.6.1	3.6.1	3.6.1	3.6.1	3.6.1	3.6.1	3.6.1	3.6.1	3.6.1	3.8	3.8	3.8
pgaudit	N/A	N/A	1.1	1.1	1.1	1.1	1.1.1	1.1.1	1.1.1	1.1.1	1.1.1	1.1.1	1.1.1	1.1.1	1.1.1	1.1.2
pg_buffercache	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
pg_freespacemap	s.o.	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
pg_hint_plan	N/A	1.1.3	1.1.3	1.1.3	1.1.3	1.2.2	1.2.2	1.2.3	1.2.3	1.2.3	1.2.5	1.2.5	1.2.5	1.2.5	1.2.6	1.2.6
pg_prewarm	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
pg_repack	N/A	N/A	1.4.0	1.4.1	1.4.2	1.4.2	1.4.3	1.4.3	1.4.3	1.4.3	1.4.3	1.4.3	1.4.3	1.4.3	1.4.3	1.4.3
pg_similarity	N/A	S/O	S/O	S/O	S/O	S/O	N/A	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
pg_stat_statements	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4
pg_trgm	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
pg_visibility	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
pgcrypto	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
pglogical	S/O	S/O	S/O	S/O	S/O	S/O	N/A	2.2.0	2.2.0	2.2.0	2.2.0	2.2.0	2.2.0	2.2.0	2.2.0	2.2.2
pgrowlocks	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
pgrouting	N/A	S/O	s.o.	2.3.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2	2.4.2
pgstattuple	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4	1.4
plcoffee	1.5.3	1.5.3	1.5.3	1.5.3	1.5.3	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2
plls	1.5.3	1.5.3	1.5.3	1.5.3	1.5.3	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2
plperl	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
plpgsql	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
pltcl	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
plv8	1.5.3	1.5.3	1.5.3	1.5.3	1.5.3	2.1.0	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2
PostGIS	2.3.0	2.3.2	2.3.2	2.3.2	2.3.4	2.3.4	2.3.7	2.3.7	2.3.7	2.3.7	2.3.7	2.5.2	2.5.2	2.5.2	2.5.2	2.5.2
postgis_tiger_geocoder	2.3.0	2.3.2	2.3.2	2.3.2	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4
postgis_topology	2.3.0	2.3.2	2.3.2	2.3.2	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4	2.3.4
postgres_fdw	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
postgresql-hll	s.o.	S/O	s.o.	2.10.2	2.10.2	2.10.2	2.10.2	2.10.2	2.10.2	2.10.2	2.10.2	2.10.2	2.10.2	2.10.2	2.10.2	2.10.2
prefix	s.o.	S/O	S/O	s.o.	1.2.6	1.2.6	1.2.6	1.2.6	1.2.6	1.2.6	1.2.6	1.2.6	1.2.6	1.2.6	1.2.6	1.2.6

Exter	9.6.1	9.6.2	9.6.3	9.6.5	9.6.6	9.6.8	9.6.9	9.6.1	9.6.1	9.6.1	9.6.1	9.6.1	9.6.1	9.6.1	9.6.1	9.6.19
sslinfo	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
tablefunc	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
test_parser	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
tsearch2	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
tsm_system_rows	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
tsm_system_time	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
unaccent	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
uuid-ossp	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1

Les modules suivants sont pris en charge comme indiqué pour les versions de PostgreSQL 9.6.

Modu	9.6.1	9.6.2	9.6.3	9.6.5	9.6.8	9.6.9	9.6.1	9.6.1	9.6.1	9.6.1	9.6.1	9.6.1	9.6.1	9.6.1	9.6.1	9.6.19
auto_explain	N/A	S/O	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
decoderaw	N/A	S/O	S/O	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
test_decoding	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
wal2json	S/O	s.o.	Commit hash 28284	Commit hash 645ab	Commit hash 5352c	Commit hash 5352c	Commit hash 41c5c	Commit hash 9e962	Commit hash 9e962	Commit hash 9e962	Commit hash 9e962	Commit hash 9e962	Commit hash 9e962ba	version 2.1	version 2.1	version 2.3

Extensions PostgreSQL version 9.5.x prises en charge sur Amazon RDS

Les tableaux suivants affichent les extensions et modules PostgreSQL pour PostgreSQL version 9.5.x qui sont actuellement pris en charge par PostgreSQL sur Amazon RDS. « s.o. » indique que l'extension ou le module n'est pas disponible pour la version PostgreSQL. Pour de plus amples informations sur les extensions PostgreSQL, veuillez consulter Packaging Related Objects into an Extension (Emballage d'objets associés dans une extension).

Exter	9.5.2	9.5.4	9.5.6	9.5.7	9.5.9	9.5.1	9.5.1	9.5.1	9.5.1	9.5.1	9.5.1	9.5.1	9.5.1	9.5.2	9.5.2	9.5.2	9.5.23
address_standardizer	2.2.2	2.2.2	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5
address_standardizer_data_us	2.2.2	2.2.2	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5
bloom	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O
btree_gin	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0

Exter	9.5.2	9.5.4	9.5.6	9.5.7	9.5.9	9.5.1	9.5.1	9.5.1	9.5.1	9.5.1	9.5.1	9.5.1	9.5.1	9.5.2	9.5.2	9.5.2	9.5.23
btree_gist	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
chkpass	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
citext	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
cube	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
dblink	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
dict_int	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
dict_xsyn	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
earthdistance	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
fuzzystrmatch	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
hstore	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
hstore_plpern	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
intagg	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
intarray	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
ip4r	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0
isn	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
log_fdw — voir Utilisation de l'extension log_fdw (p. 1506)	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O
ltree	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
pgaudit	N/A	S/O	N/A	1.0.5	1.0.5	1.0.5	1.0.5	1.0.6	1.0.6	1.0.6	1.0.6	1.0.6	1.0.6	1.0.6	1.0.6	1.0.6	1.0.6
pg_buffercache	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
pg_freespacemap	S/O	N/A	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
pg_hint_plan	S/O	N/A	1.1.3	1.1.3	1.1.3	1.1.3	1.1.3	1.1.5	1.1.5	1.1.5	1.1.5	1.1.8	1.1.8	1.1.8	1.1.8	1.1.9	1.1.9
pg_prewarm	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
pg_stat_statements	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3
pg_trgm	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
pg_visibility	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O	S/O
pgcrypto	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2	1.2
pgrowlocks	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1
pgstattuple	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3	1.3

Exter	9.5.2	9.5.4	9.5.6	9.5.7	9.5.9	9.5.1	9.5.1	9.5.1	9.5.1	9.5.1	9.5.1	9.5.1	9.5.1	9.5.2	9.5.2	9.5.2	9.5.23
plcoffee	1.4.4	1.4.4	1.4.4	1.4.4	1.4.4	1.4.4	2.1.0	2.1.0	2.1.0	2.1.0	2.1.0	2.1.0	2.1.0	2.1.0	2.1.0	2.1.0	2.1.0
plls	1.4.4	1.4.4	1.4.4	1.4.4	1.4.4	1.4.4	2.1.0	2.1.0	2.1.0	2.1.0	2.1.0	2.1.0	2.1.0	2.1.0	2.1.0	2.1.0	2.1.0
plperl	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
plpgsql	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
pltcl	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
plv8	1.4.4	1.4.4	1.4.4	1.4.4	1.4.4	1.4.4	2.1.0	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2	2.1.2
PostGIS	2.2.2	2.2.2	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.5.2	2.5.2	2.5.2	2.5.2	2.5.2
postgis_tiger_geocoder	2.2.2	2.2.2	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5
postgis_topology	2.2.2	2.2.2	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5	2.2.5
postgres_fdw	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
sslinfo	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
tablefunc	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
test_parser	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
tsearch2	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
tsm_system_rows	S/O	N/A	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
tsm_system_time	S/O	N/A	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
unaccent	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
uuid-ossp	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0

Les modules suivants sont pris en charge comme indiqué pour les versions de PostgreSQL 9.5.

Modu	9.5.2	9.5.4	9.5.6	9.5.7	9.5.9	9.5.1	9.5.1	9.5.1	9.5.1	9.5.1	9.5.1	9.5.1	9.5.2	9.5.2	9.5.2	9.5.23
auto_explain	N/A	S/O	S/O	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
test_decoding	S/O	S/O	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
wal2json	S/O	s.o.	S/O	Commit hash 2828409	Commit hash 2828409	Commit hash 2828409	Commit hash 2828409	Commit hash 2828409	Commit hash 2828409	Commit hash 2828409	Commit hash 2828409	Commit hash 2828409	Commit hash 2828409	version 2.1	version 2.1	version 2.1

Prise en charge des extensions PostgreSQL pour PostGIS sur Amazon RDS

Avant de pouvoir utiliser l'extension PostGIS, vous devez la créer en exécutant la commande suivante.

```
CREATE EXTENSION POSTGIS;
```

Le tableau suivant montre les versions des composants PostGIS qui accompagnent les versions Amazon RDS pour PostgreSQL.

PostgreSQL	PostGIS	GEOS	GDAL	PROJ
9.5.2	2.2.2 r14797	3.5.0-CAPI-1.9.0 r4084	2.0.2, publiée le 26/01/2016	Vers. 4.9.2, 8 septembre 2015
9.5.4	2.2.2 r14797	3.5.0-CAPI-1.9.0 r4084	2.0.3, publiée le 01/07/2016	Vers. 4.9.2, 8 septembre 2015
9.5.6	2.2.5 r15298	3.5.1-CAPI-1.9.1 r4246	2.0.3, publiée le 01/07/2016	Vers. 4.9.3, 15 septembre 2016
9.5.7	2.2.5 r15298	3.5.1-CAPI-1.9.1 r4246	2.0.3, publiée le 01/07/2016	Vers. 4.9.3, 15 septembre 2016
9.6.1	2.3.0 r15146	3.5.0-CAPI-1.9.0 r4084	2.1.1, publiée le 07/07/2016	Vers. 4.9.2, 8 septembre 2016
9.6.2	2.3.2 r15302	3.5.1-CAPI-1.9.1 r4246	2.1.3, publiée le 20/01/2017	Vers. 4.9.3, 15 septembre 2016
9.6.3	2.3.2 r15302	3.5.1-CAPI-1.9.1 r4246	2.1.3, publiée le 20/01/2017	Vers. 4.9.3, 15 septembre 2016
9.6.6	2.3.4 r16009	3.6.2-CAPI-1.10.2 4d2925d6	2.1.3, publiée le 20/01/2017	Vers. 4.9.3, 15 septembre 2016
9.6.8	2.3.4 r16009	3.6.2-CAPI-1.10.2 4d2925d6	2.1.3, publiée le 20/01/2017	Vers. 4.9.3, 15 septembre 2016
9.6.9	2.3.7 r16523	3.6.2-CAPI-1.10.2 4d2925d6	2.1.4, publiée le 23/06/2017	Vers. 4.9.3, 15 septembre 2016
9.6.10	2.3.7 r16523	3.6.2-CAPI-1.10.2 4d2925d6	2.1.4, publiée le 23/06/2017	Vers. 4.9.3, 15 septembre 2016
9.6.11	2.3.7 r16523	3.6.2-CAPI-1.10.2 4d2925d6	2.1.4, publiée le 23/06/2017	Vers. 4.9.3, 15 septembre 2016
10.1	2.4.2	3.6.2-CAPI-1.10.2 4d2925d6	2.1.3, publiée le 20/01/2017	Vers. 4.9.3, 15 septembre 2016
10.3	2.4.2	3.6.2-CAPI-1.10.2 4d2925d6	2.1.3, publiée le 20/01/2017	Vers. 4.9.3, 15 septembre 2016
10.4	2.4.4 r16526	3.6.2-CAPI-1.10.2 4d2925d6	2.1.4, publiée le 23/06/2017	Vers. 4.9.3, 15 septembre 2016
10.5	2.4.4 r16526	3.6.2-CAPI-1.10.2 4d2925d6	2.1.4, publiée le 23/06/2017	Vers. 4.9.3, 15 septembre 2016
10.6	2.4.4 r16526	3.6.2-CAPI-1.10.2 4d2925d6	2.1.4, publiée le 23/06/2017	Vers. 4.9.3, 15 septembre 2016

PostgreSQL	PostGIS	GEOS	GDAL	PROJ
11.1	2.5.1 r17027	3.7.0-CAPI-1.11.0 673b9939	2.3.1, publiée le 22/06/2018	Vers. 5.2.0, 15 septembre 2018

Note

PostgreSQL 10.5 prend désormais en charge l'extension `libprotobuf` version 1.3.0 pour le composant PostGIS.

Utilisation de l'extension log_fdw

L'extension `log_fdw` est nouvelle dans Amazon RDS pour la version 9.6.2 de PostgreSQL et les versions ultérieures. Elle vous permet d'accéder au journal de votre moteur de base de données à l'aide d'une interface SQL. Outre les fichiers journaux stderr qui sont générés par défaut sur RDS, vous pouvez afficher des journaux CSV (réglez le paramètre `log_destination` dans `csvlog`) et créer des tableaux source dans lesquels les données sont réparties sur plusieurs colonnes.

Cette extension introduit deux nouvelles fonctions qui facilitent la création de tables source pour les journaux de base de données :

- `list_postgres_log_files()` – Répertorie les fichiers dans le répertoire du journal de base de données et indique la taille des fichiers en octets.
- `create_foreign_table_for_log_file(table_name text, server_name text, log_file_name text)` – Crée un tableau source pour le fichier spécifié dans la base de données actuelle.

Toutes les fonctions créées par `log_fdw` appartiennent à `rds_superuser`. Les membres du rôle `rds_superuser` peuvent accorder l'accès à ces fonctions à d'autres utilisateurs de base de données.

L'exemple suivant montre comment utiliser l'extension `log_fdw`.

Pour utiliser l'extension log_fdw

1. Procurez-vous l'extension `log_fdw`.

```
postgres=> CREATE EXTENSION log_fdw;
CREATE EXTENSION
```

2. Créez le serveur de journal en tant que wrapper de données externes.

```
postgres=> CREATE SERVER log_server FOREIGN DATA WRAPPER log_fdw;
CREATE SERVER
```

3. Sélectionnez l'ensemble des fichiers journaux d'une liste.

```
postgres=> SELECT * from list_postgres_log_files() order by 1;
```

Voici un exemple de réponse.

```
            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. Créez une table avec une seule colonne « log_entry » pour les fichiers non CSV.

```
postgres=> SELECT create_foreign_table_for_log_file('my_postgres_error_log',
     'log_server', 'postgresql.log.2016-08-09-22.csv');
```

Voici un exemple de réponse.

```
-----------------------------------

(1 row)
```

5. Sélectionnez un exemple de fichier journal. Le code suivant récupère l'heure du journal et la description du message d'erreur.

```
postgres=> SELECT log_time, message from my_postgres_error_log order by 1;
```

Voici un exemple de réponse.

```
             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)
```

Mise à niveau de PL/v8

Si vous utilisez PL/v8 et mettez à niveau PostgreSQL vers une nouvelle version de PL/v8, vous profitez immédiatement de la nouvelle extension. Effectuez les étapes suivantes pour synchroniser les métadonnées du catalogue avec la nouvelle version de PL/v8. Ces étapes sont facultatives, mais nous vous recommandons fortement de les compléter afin d'éviter des avertissements de décalage des métadonnées.

Pour synchroniser les métadonnées de votre catalogue avec une nouvelle version de PL/v8

1. Vérifiez que vous devez mettre à jour. Pour ce faire, exécutez la commande suivante tout en étant connecté à votre instance.

   ```
   select * from pg_available_extensions where name in
   ('plv8','plls','plcoffee');
   ```

   Si les résultats contiennent des valeurs pour une version installée avec un numéro inférieur à celui de la version par défaut, poursuivez cette procédure pour mettre à jour vos extensions.

   Par exemple, l'ensemble de résultats suivant indique que vous devez procéder à la mise à jour.

   ```
   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
   (3 rows)
   ```

2. Prenez un instantané de votre instance par précaution, car la mise à niveau supprime toutes vos fonctions PL/v8. Vous pouvez poursuivre avec les étapes suivantes tandis que l'instantané est en cours de création.

   Pour connaître les étapes de création d'un instantané, consultez Création d'un instantané de base de données (p. 327).

3. Faites le compte du nombre de fonctions PL/v8 de votre instance de manière à pouvoir valider le fait qu'elles sont toutes en place après la mise à niveau.

   Le code suivant renvoie le nombre de fonctions écrites en PL/v8, plcoffee ou plls.

   ```
   select proname, nspname, lanname
   from pg_proc p, pg_language l, pg_namespace n
   where p.prolang = l.oid
   and n.oid = p.pronamespace
   and lanname in ('plv8','plcoffee','plls');
   ```

4. Utiliser pg_dump pour créer un fichier de vidage schema-only.

   Le code suivant crée un fichier sur votre ordinateur client dans le répertoire /tmp.

   ```
   ./pg_dump -Fc --schema-only -U master postgres > /tmp/test.dmp
   ```

   Cet exemple utilise les options suivantes :

   - -FC « format personnalisé »
   - --schema-only « vide uniquement les commandes nécessaires pour créer un schéma (les fonctions dans notre cas) »
   - -U « nom d'utilisateur maître rds »
   - database « nom de la base de données dans notre instance »

   Pour de plus amples informations sur pg_dump, veuillez consulter la page pg_dump de la documentation PostgreSQL.

5. Extrayez la déclaration DDL « CREATE FUNCTION » présente dans le fichier de vidage.

Le code suivant extrait la déclaration DDL nécessaire pour créer les fonctions. Vous l'utiliserez dans les étapes suivantes pour recréer les fonctions. Le code utilise la commande `grep` pour extraire les instructions dans un fichier.

```
./pg_restore -l /tmp/test.dmp | grep FUNCTION > /tmp/function_list/
```

Pour plus d'informations sur pg_restore, consultez pg_restore.

6. Supprimez les fonctions et les extensions.

   Le code suivant supprime tous les objets basés sur PL/v8. L'option cascade garantit que les objets dépendants sont supprimés.

   ```
   drop extension plv8 cascade;
   ```

   Si votre instance PostgreSQL contient des objets basés sur plcoffee ou plls, répétez l'étape pour ces extensions.

7. Créez les extensions.

   Le code suivant crée les extensions PL/v8, plcoffee et plls.

   ```
   create extension plv8;

   create extension plcoffee;

   create extension plls;
   ```

8. Créez les fonctions à l'aide du fichier de vidage et du fichier « pilote ».

   Le code suivant recrée les fonctions que vous avez extraites précédemment.

   ```
   ./pg_restore -U master -d postgres -Fc -L /tmp/function_list /tmp/test.dmp
   ```

9. Vérifiez le nombre de fonctions

   Vérifiez que vos fonctions ont toutes été recréées en exécutant l'instruction de code suivante.

   ```
   select * from pg_available_extensions where name in
   ('plv8','plls','plcoffee');
   ```

   Note

   PL/v8 version 2 ajoute la ligne supplémentaire suivante à votre ensemble de résultats :

   ```
       proname     |  nspname   | lanname
   ---------------+------------+----------
    plv8_version  | pg_catalog | plv8
   ```

Fonctions PostgreSQL prises en charge

Amazon RDS prend en charge un grand nombre de fonctionnalités PostgreSQL parmi les plus courantes. Il s'agit des licences suivantes :

Rubriques

- Réplication logique pour PostgreSQL sur Amazon RDS (p. 1510)
- Déclencheurs d'événements pour PostgreSQL sur Amazon RDS (p. 1512)
- Grandes pages pour Amazon RDS pour PostgreSQL (p. 1512)
- Espaces de table pour PostgreSQL sur Amazon RDS (p. 1513)

- Autovacuum pour PostgreSQL sur Amazon RDS (p. 1513)
- Disque RAM pour le stats_temp_directory (p. 1513)
- ALTER ENUM pour PostgreSQL (p. 1514)

Réplication logique pour PostgreSQL sur Amazon RDS

Dès PostgreSQL version 10.4, RDS prend en charge la syntaxe SQL de publication et d'abonnement pour la réplication logique PostgreSQL 10.

Pour activer la réplication logique pour une instance de base de données Amazon RDS pour PostgreSQL

1. Le compte d'utilisateur AWS nécessite le rôle rds_superuser pour effectuer la réplication logique pour la base de données PostgreSQL sur Amazon RDS.
2. Définissez le paramètre statique `rds.logical_replication` sur 1.
3. Modifiez les règles entrantes du groupe de sécurité pour l'instance de l'éditeur (production) pour permettre à l'instance de l'abonné (réplica) de se connecter. Cela se fait généralement en incluant l'adresse IP de l'abonné dans le groupe de sécurité.
4. Redémarrez l'instance de base de données pour que les modifications apportées au paramètre statique `rds.logical_replication` prennent effet.

Pour plus d'informations sur la réplication logique PostgreSQL, consultez la documentation PostgreSQL.

Décodage logique et réplication logique

RDS for PostgreSQL prend en charge la diffusion en continu des modifications WAL à l'aide des emplacements de réplication logique. Amazon RDS prend en charge le décodage logique pour une instance de base de données PostgreSQL 9.5.4 et versions ultérieures. Vous pouvez configurer des emplacements logiques de réplication sur votre instance et diffuser les modifications de base de données à travers ces emplacements pour un client comme `pg_recvlogical`. Les emplacements logiques de réplication sont créés au niveau de la base de données et prennent en charge les connexions de réplication avec une seule base de données.

Les clients plus courants pour la réplication logique PostgreSQL sont AWS Database Migration Service ou un hôte géré de manière personnalisée sur une instance EC2 AWS. L'emplacement de réplication logique ne sait rien sur le récepteur du flux et la cible n'est pas nécessairement la cible d'une base de données réplica. Si vous configurez un emplacement de réplication logique et que vous ne lisez pas à partir de l'emplacement, les données peuvent être écrites dans le stockage de votre instance de base de données et le remplir rapidement.

La réplication logique et le décodage logique PostgreSQL sur Amazon RDS sont activés avec un nouveau paramètre, un nouveau type de connexion de réplication et un rôle de sécurité. Le client pour le décodage logique peut être n'importe quel client capable d'établir une connexion de réplication avec une base de données sur une instance de base de données PostgreSQL.

Pour activer le décodage logique pour une instance de base de données Amazon RDS pour PostgreSQL

1. Le compte d'utilisateur nécessite le rôle rds_superuser pour activer la réplication logique. Le compte d'utilisateur a également besoin du rôle rds_replication pour accorder les autorisations requises pour gérer les emplacements logiques et diffuser les données à l'aide des emplacements logiques.
2. Définissez le paramètre statique `rds.logical_replication` sur 1. Pour l'application de ce paramètre, nous définissons également les paramètres `wal_level`, `max_wal_senders`, `max_replication_slots` et `max_connections`. Ces modifications de paramètres

peuvent accroître la génération WAL de sorte que vous ne devez définir le paramètre `rds.logical_replication` que lorsque vous utilisez des emplacements logiques.

3. Redémarrez l'instance de base de données pour que le paramètre statique `rds.logical_replication` prenne effet.
4. Créez un emplacement de réplication logique comme expliqué dans la section suivante. Cela nécessite que vous précisiez un plug-in de décodage. Actuellement, nous prenons en charge les plug-ins de sortie `test_decoding` et `wal2json` livrés avec PostgreSQL.

Pour plus d'informations sur le décodage logique PostgreSQL, consultez la documentation PostgreSQL.

Utilisation des emplacements de réplication logique

Vous pouvez utiliser les commandes SQL pour utiliser les emplacements logiques. Par exemple, la commande suivante crée un emplacement logique nommé test_slot à l'aide du plug-in de sortie PostgreSQL par défaut test_decoding.

```
SELECT * FROM pg_create_logical_replication_slot('test_slot', 'test_decoding');
```

La sortie doit ressembler à ce qui suit.

```
slot_name    | xlog_position
-----------------+---------------
regression_slot | 0/16B1970
(1 row)
```

Pour lister les emplacements logiques, utilisez la commande suivante.

```
SELECT * FROM pg_replication_slots;
```

Pour supprimer un emplacement logique, utilisez la commande suivante.

```
SELECT pg_drop_replication_slot('test_slot');
```

La sortie doit ressembler à ce qui suit.

```
pg_drop_replication_slot
------------------------

(1 row)
```

Pour plus d'exemples sur l'utilisation des emplacements de réplication logique, consultez Exemples de décodage logique dans la documentation PostgreSQL.

Une fois l'emplacement de réplication logique créé, vous pouvez commencer la diffusion en continu. L'exemple suivant montre comment le décodage logique est contrôlé via le protocole de réplication de diffusion en continu, à l'aide du programme pg_recvlogical inclus dans la distribution de PostgreSQL. Cela nécessite que l'authentification du client soit configurée pour autoriser les connexions de réplication.

```
pg_recvlogical -d postgres --slot test_slot -U master
    --host sg-postgresql1.c6c8mresaghgv0.us-west-2.rds.amazonaws.com
    -f -  --start
```

Déclencheurs d'événements pour PostgreSQL sur Amazon RDS

PostgreSQL 9.5.4 et versions ultérieures prend en charge les déclencheurs d'événement et Amazon RDS prend en charge les déclencheurs d'événement pour ces versions. Le compte d'utilisateur principal peut être utilisé pour créer, modifier, renommer et supprimer des déclencheurs d'événements. Les déclencheurs d'événements sont au niveau de l'instance de base de données, de sorte qu'ils peuvent s'appliquer à toutes les bases de données sur une instance.

Par exemple, le code suivant crée un déclencheur d'événement qui imprime l'utilisateur actuel à la fin de chaque commande DDL.

```
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();
```

Pour plus d'informations sur les déclencheurs d'événements PostgreSQL, consultez Déclencheurs d'événements dans la documentation de PostgreSQL.

Il existe plusieurs restrictions quant à l'utilisation de déclencheurs d'événements PostgreSQL sur Amazon RDS. Il s'agit des licences suivantes :

- Vous ne pouvez pas créer de déclencheurs d'événements sur les réplicas en lecture. En revanche, vous pouvez créer de déclencheurs d'événements sur une source de réplica en lecture. Les déclencheurs d'événements sont ensuite copiés sur le réplica en lecture. Les déclencheurs d'événements sur le réplica en lecture ne s'activent pas sur le réplica en lecture lorsque les modifications sont poussées depuis la source. En revanche, si le réplica en lecture est promu, les déclencheurs d'événements existants s'activent lorsque des opérations de base de données ont lieu.
- Pour effectuer une mise à niveau de version majeure vers une instance de base de données PostgreSQL qui utilise des déclencheurs d'événements, vous devez supprimer les déclencheurs d'événements avant de procéder à la mise à niveau de l'instance.

Grandes pages pour Amazon RDS pour PostgreSQL

Amazon RDS for PostgreSQL prend en charge plusieurs tailles de page pour PostgreSQL 9.5.6 et versions ultérieures, et 9.6.2 et versions ultérieures. Cette prise en charge inclut les tailles de page 4 Ko et 2 Mo.

Les grandes pages réduisent la charge de traitement lors de l'utilisation de grands fragments de mémoire contigus. Vous allouez de grandes pages pour votre application en utilisant des appels à la mémoire partagée mmap ou SYSV. Vous pouvez activer les grandes pages sur une base de données Amazon RDS pour PostgreSQL à l'aide du paramètre `huge_pages`. Définissez ce paramètre sur « activé » pour activer de grandes pages.

Pour PostgreSQL 10 ou version ultérieure, les grandes pages sont activées pour toutes les classes d'instance. Pour les versions de PostgreSQL antérieures à la version 10, les grandes pages sont activées par défaut pour les classes d'instance db.r4.*, db.m4.16xlarge et db.m5.*. Pour les autres classes d'instance, les grandes pages sont désactivées par défaut.

Lorsque vous définissez le paramètre `huge_pages` sur « on », Amazon RDS utilise les grandes pages sur la base de la mémoire partagée disponible. Si l'instance de base de données n'est pas capable d'utiliser les grandes pages en raison des contraintes de mémoire partagée, Amazon RDS empêche le démarrage de l'instance et affecte au statut de l'instance de base de données un état indiquant l'incompatibilité des paramètres. Dans ce cas, vous pouvez affecter la valeur « off » au paramètre `huge_pages` pour autoriser Amazon RDS à démarrer l'instance de bases de données.

Le paramètre `shared_buffers` est essentiel pour définir le pool de mémoire partagée requis pour utiliser les grandes pages. La valeur par défaut du paramètre `shared_buffers` est définie sur un pourcentage du total des 8 000 pages disponibles pour la mémoire de cette instance. Lorsque vous utilisez les grandes pages, celles-ci sont allouées dans des grandes pages colocalisées. Amazon RDS affecte à une instance de base de données dans un état indiquant l'incompatibilité des paramètres si les paramètres de mémoire partagée définis requièrent plus de 90 % de la mémoire de l'instance de base de données. Pour plus d'informations sur la définition de la mémoire partagée pour PostgreSQL, consultez la documentation sur PostgreSQL.

> **Note**
>
> Les grandes pages ne sont pas prises en charge pour les classes d'instance de base de données db.m1, db.m2 et db.m3.

Espaces de table pour PostgreSQL sur Amazon RDS

Les espaces de table sont pris en charge dans PostgreSQL sur Amazon RDS à des fins de compatibilité. Comme l'ensemble du stockage s'effectue sur un volume logique unique, les espaces de table ne peuvent pas être utilisés pour l'isolement ni la répartition des I/O. Nos évaluations et notre expérience pratique montrent qu'un volume logique unique constitue la meilleure configuration dans la plupart des cas d'utilisation.

Autovacuum pour PostgreSQL sur Amazon RDS

La fonction autovacuum de PostgreSQL est activée par défaut sur les nouvelles instances de base de données PostgreSQL. La fonction autovacuum est facultative, mais nous vous recommandons vivement de ne pas la désactiver. Pour de plus amples informations sur l'utilisation d'auto-vacuum avec Amazon RDS pour PostgreSQL, veuillez consulter Utilisation de la fonction autovacuum de PostgreSQL sur Amazon RDS (p. 1431).

Disque RAM pour le stats_temp_directory

Le paramètre Amazon RDS pour PostgreSQL, `rds.pg_stat_ramdisk_size`, peut être utilisé pour spécifier la mémoire système allouée à un disque RAM afin de stocker le code PostgreSQL `stats_temp_directory`. Le paramètre de disque RAM est disponible pour toutes les versions de PostgreSQL sur Amazon RDS.

Sous certaines charges de travail, ce paramètre peut améliorer les performances et réduire les exigences d'I/O. Pour de plus amples informations sur le paramètre `stats_temp_directory`, veuillez consulter la documentation sur PostgreSQL.

Pour activer un disque RAM pour votre `stats_temp_directory`, définissez le paramètre `rds.pg_stat_ramdisk_size` à une valeur différente de zéro dans le groupe de paramètres utilisé par votre instance de base de données. La valeur du paramètre est exprimée en Mo. Vous devez redémarrer l'instance de base de données pour que les modifications prennent effet.

Par exemple, la commande d'AWS CLI suivante définit le paramètre de disque RAM à 256 Mo.

```
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"
```

Après le redémarrage, exécutez la commande suivante pour afficher le statut de `stats_temp_directory` :

```
postgres=>show stats_temp_directory;
```

La commande doit renvoyer les éléments suivants :

```
stats_temp_directory
----------------------------
/rdsdbramdisk/pg_stat_tmp
(1 row)
```

ALTER ENUM pour PostgreSQL

Amazon RDS pour PostgreSQL versions 9.6.2, 9.5.6 et ultérieures prend en charge la modification des énumérations. Cette fonctionnalité n'est pas disponible dans les autres versions d'Amazon RDS.

Le code suivant présente un exemple de modification d'une valeur enum.

```
postgres=> CREATE TYPE rainbow AS ENUM ('red', 'orange', 'yellow', 'green', 'blue',
 'purple');
CREATE TYPE
postgres=> CREATE TABLE t1 (colors rainbow);
CREATE TABLE
postgres=> INSERT INTO t1 VALUES ('red'), ( 'orange');
INSERT 0 2
postgres=> 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)
```

Limites pour les instances de bases de données PostgreSQL

Voici une liste de limitations pour PostgreSQL sur Amazon RDS :

- Vous pouvez avoir jusqu'à 40 instances de bases de données PostgreSQL.

- Pour les limites de stockage, veuillez consulter Stockage d'instance de base de données Amazon RDS (p. 30).
- Amazon RDS réserve jusqu'à 3 connexions pour la maintenance du système. Si vous spécifiez une valeur pour le paramètre des connexions utilisateur, vous devez ajouter 3 au nombre de connexions que vous envisagez d'utiliser.

Mise à niveau d'une instance de base de données PostgreSQL

Vous pouvez gérer deux types de mises à niveau pour votre instance de base de données PostgreSQL:

- Mises à jour du SE – Il peut arriver que Amazon RDS doive mettre à jour le système d'exploitation sous-jacent de votre instance de base de données afin d'appliquer des correctifs de sécurité ou des modifications du SE. Vous pouvez décider quand Amazon RDS doit appliquer les mises à jour du système d'exploitation en utilisant la console RDS, AWS Command Line Interface (AWS CLI) ou l'API RDS.

  Pour plus d'informations sur les mises à jour de SE, consultez Application des mises à jour pour une instance de base de données (p. 262).
- Mises à niveau de moteur de base de données – Lorsque Amazon RDS prend en charge une nouvelle version d'un moteur de base de données, vous pouvez mettre à niveau vos instances de base de données vers cette nouvelle version. Il existe deux sortes de mises à jour : les mises à niveau de version majeure et les mises à niveau mineures. Amazon RDS prend en charge les mises à jour mineures et majeures de version pour les instances de base de données PostgreSQL.

  Pour plus d'informations sur les mises à niveau de moteur de base de données PostgreSQL, consultez Mise à niveau du moteur de base de données PostgreSQL pour Amazon RDS (p. 1373).

Utilisation de SSL avec une instance de base de données PostgreSQL

Amazon RDS prend en charge le chiffrement SSL pour les instances de bases de données PostgreSQL. En utilisant SSL, vous pouvez chiffrer une connexion PostgreSQL entre vos applications et vos instances de bases de données PostgreSQL. Vous pouvez également forcer toutes les connexions à votre instance de base de données PostgreSQL à utiliser SSL.

Pour de plus amples informations sur la prise en charge de SSL et les bases de données PostgreSQL, veuillez consulter SSL Support dans la documentation PostgreSQL. Pour de plus amples informations sur l'utilisation d'une connexion SSL sur JDBC, veuillez consulter Configuring the Client dans la documentation PostgreSQL.

Rubriques

- Exiger une connexion SSL à une instance de base de données PostgreSQL (p. 1516)
- Détermination du statut de la connexion SSL (p. 1517)

Le support SSL est disponible pour PostgreSQL dans toutes les régions AWS. Amazon RDS crée un certificat SSL pour votre instance de base de données PostgreSQL lorsque l'instance est créée. Si vous activez la vérification du certificat SSL, ce dernier inclut le point de terminaison de l'instance de base de données en tant que nom commun du certificat SSL pour assurer une protection contre les attaques par usurpation.

Pour se connecter à une instance de base de données PostgreSQL via SSL

1. Téléchargez le certificat.

Pour de plus amples informations sur le téléchargement de certificats, veuillez consulter Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).

2. Importez le certificat dans votre système d'exploitation.
3. Connectez-vous à votre instance de base de données PostgreSQL sur SSL.

   Lors de la connexion avec SSL, votre client peut choisir de vérifier ou pas la chaîne du certificat. Si vos paramètres de connexion spécifient `sslmode=verify-ca` ou `sslmode=verify-full`, votre client nécessite que les certificats de l'autorité de certification RDS soient dans leur magasin d'approbations ou référencés dans l'URL de connexion. L'exigence nécessite de vérifier la chaîne du certificat qui signe le certificat de votre base de données.

   Quand un client, tel que psql ou JDBC, est configuré avec la prise en charge du protocole SSL, le comportement par défaut est le suivant : le client essaie d'abord de se connecter à la base de données avec le protocole SSL. En cas d'impossibilité, le client revient à la connexion sans protocole SSL. Le mode `sslmode` utilisé par défaut diffère selon qu'il s'agit de clients libpq (comme psql) ou de clients JDBC. Pour les clients libpq, la valeur par défaut est `prefer`, alors qu'elle est `verify-full` pour les clients JDBC.

   Utilisez le paramètre `sslrootcert` pour référencer le certificat, par exemple, `sslrootcert=rds-ssl-ca-cert.pem`.

Voici un exemple d'utilisation de psql pour se connecter à une instance de base de données PostgreSQL.

```
$ psql -h testpg.cdhmuqifdpib.us-east-1.rds.amazonaws.com -p 5432 \
    "dbname=testpg user=testuser sslrootcert=rds-ca-2019-root.pem sslmode=verify-full"
```

Exiger une connexion SSL à une instance de base de données PostgreSQL

Vous pouvez exiger que les connexions à votre instance de base de données PostgreSQL utilisent SSL en utilisant le paramètre `rds.force_ssl`. Par défaut, le paramètre `rds.force_ssl` a pour valeur 0 (désactivé). Vous pouvez affecter au paramètre `rds.force_ssl` la valeur 1 (activé) pour exiger SSL pour les connexions à votre instance de base de données. La mise à jour du paramètre `rds.force_ssl` affecte également la valeur 1 (activé) au paramètre `ssl` PostgreSQL et modifie le fichier `pg_hba.conf` de votre instance de base de données pour qu'elle prenne en charge la nouvelle configuration SSL.

Vous pouvez définir la valeur du paramètre `rds.force_ssl` en mettant à jour le groupe de paramètres pour votre instance de base de données. Si le groupe de paramètres pour votre instance de base de données n'est pas le groupe de paramètres par défaut et que le paramètre `ssl` a déjà pour valeur 1 lorsque vous affectez la valeur 1 au paramètre `rds.force_ssl`, vous n'avez pas besoin de redémarrer votre instance de base de données. Dans le cas contraire, vous devez redémarrer l'instance de base de données pour que la modification prenne effet. Pour plus d'informations sur les groupes de paramètres, consultez Utilisation de groupes de paramètres de base de données (p. 225).

Lorsque le paramètre `rds.force_ssl` a pour valeur 1 pour une instance de base de données, vous voyez une sortie similaire à la suivante lorsque vous vous connectez, indiquant que SSL est à présent requis :

```
$ psql postgres -h SOMEHOST.amazonaws.com -p 8192 -U someuser
. . .
SSL connection (cipher: DHE-RSA-AES256-SHA, bits: 256)
Type "help" for help.

postgres=>
```

Détermination du statut de la connexion SSL

Le statut chiffré de votre connexion est affiché dans la page d'accueil d'ouverture de session lorsque vous vous connectez à l'instance de base de données :

```
Password for user master:
psql (10.3)
SSL connection (cipher: DHE-RSA-AES256-SHA, bits: 256)
Type "help" for help.

postgres=>
```

Vous pouvez également charger l'extension `sslinfo`, puis appeler la fonction `ssl_is_used()` pour déterminer si SSL est utilisé. La fonction renvoie `t` si la connexion utilise SSL ; sinon, elle renvoie `f`.

```
postgres=> create extension sslinfo;
CREATE EXTENSION

postgres=> select ssl_is_used();
 ssl_is_used
---------
t
(1 row)
```

Vous pouvez utiliser la commande `select ssl_cipher()` pour déterminer le chiffrement SSL :

```
postgres=> select ssl_cipher();
ssl_cipher
--------------------
DHE-RSA-AES256-SHA
(1 row)
```

Si vous activez `set rds.force_ssl` et redémarrez l'instance, les connexions non-SSL sont refusées avec le message suivant :

```
$ export PGSSLMODE=disable
$ psql postgres -h SOMEHOST.amazonaws.com -p 8192 -U someuser
psql: FATAL: no pg_hba.conf entry for host "host.ip", user "someuser", database "postgres",
 SSL off
$
```

Pour de plus amples informations sur l'option `sslmode`, veuillez consulter Database Connection Control Functions dans la documentation PostgreSQL.

Sécurité dans Amazon RDS

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre AWS et vous-même. Le modèle de responsabilité partagée décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud – AWS est responsable de la protection de l'infrastructure qui exécute des services AWS dans le cloud AWS. AWS vous fournit également les services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformité AWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon RDS, consultez Services AWS concernés par le programme de conformité.
- Sécurité dans le cloud – Votre responsabilité est déterminée par le service AWS que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre organisation, et la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de Amazon RDS. Les rubriques suivantes vous montrent comment configurer Amazon RDS pour répondre à vos objectifs de sécurité et de conformité. Vous pouvez également apprendre à utiliser d'autres services AWS qui vous permettent de surveiller et de sécuriser vos ressources Amazon RDS.

Vous pouvez gérer l'accès à vos ressources Amazon RDS et à vos bases de données sur une instance de base de données. La méthode que vous utilisez pour gérer l'accès dépend du type de tâche que l'utilisateur doit effectuer avec Amazon RDS :

- Exécutez votre instance de base de données dans un VPC basé sur le service Amazon VPC pour disposer du meilleur contrôle d'accès réseau possible. Pour plus d'informations sur la création d'une instance de base de données dans un VPC, consultez VPC Amazon Virtual Private Cloud et Amazon RDS (p. 1610).
- Utilisez des stratégies AWS Identity and Access Management (IAM) pour attribuer des autorisations afin de déterminer qui peut gérer les ressources Amazon RDS. Par exemple, vous pouvez utiliser IAM pour déterminer qui est autorisé à créer, décrire, modifier et supprimer des instances de base de données, attribuer des balises à des ressources ou modifier des groupes de sécurité.
- Utilisez les groupes de sécurité pour contrôler quelles adresses IP ou instances Amazon EC2 peuvent se connecter à vos bases de données sur une instance de base de données. Quand vous créez une instance de base de données pour la première fois, son pare-feu empêche tout accès aux bases de données sauf via les règles spécifiées par un groupe de sécurité associé.
- Utilisez des connexions SSL (Secure Socket Layer) ou TLS (Transport Layer Security) avec les instances de base de données exécutant les moteurs de base de données MySQL, MariaDB, PostgreSQL, Oracle ou Microsoft SQL Server. Pour de plus amples informations sur l'utilisation de SSL avec une instance de base de données, veuillez consulter Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).
- Utilisez Amazon RDS pour sécuriser vos instances de base de données et les instantanés au repos. Le chiffrement Amazon RDS utilise l'algorithme standard de chiffrement AES-256 pour chiffrer vos données sur le serveur qui héberge votre instance de base de données. Pour plus d'informations, consultez Chiffrement des ressources Amazon RDS (p. 1522).
- Utilisez un chiffrement réseau et un chiffrement TDE (Transparent Data Encryption) avec les instances de base de données Oracle. Pour plus d'informations, consultez Oracle NNE (Native Network Encryption) (p. 1062) et Oracle Transparent Data Encryption (p. 1091)

- Utilisez les fonctions de sécurité de votre moteur de base de données pour contrôler qui peut se connecter aux bases de données sur une instance de base de données. Ces fonctions agissent comme si la base de données se trouvait sur votre réseau local.

  Note

  Vous devez uniquement configurer la sécurité de vos cas d'utilisation. Vous n'avez pas à configurer l'accès de sécurité pour les processus gérés par Amazon RDS. Cela inclut, par exemple, la création de sauvegardes et la réplication de données entre une instance de base de données principale et un réplica en lecture, et d'autres processus.

Pour plus d'informations sur la gestion de l'accès aux ressources Amazon RDS et à vos bases de données sur une instance de base de données, consultez les rubriques suivantes.

Rubriques

- Authentification de base de données avec Amazon RDS (p. 1519)
- Protection des données dans Amazon RDS (p. 1521)
- Identity and Access Management dans Amazon RDS (p. 1536)
- Journalisation et surveillance dans Amazon RDS (p. 1583)
- Validation de la conformité pour Amazon RDS (p. 1584)
- Résilience dans Amazon RDS (p. 1585)
- Sécurité de l'infrastructure dans Amazon RDS (p. 1586)
- Amazon RDS et interface des points de terminaison VPC (AWS PrivateLink) (p. 1587)
- Bonnes pratiques de sécurité pour Amazon RDS (p. 1590)
- Contrôle d'accès par groupe de sécurité (p. 1590)
- Privilèges du compte utilisateur principal (p. 1605)
- Utilisation des rôles liés à un service pour Amazon RDS (p. 1606)
- VPC Amazon Virtual Private Cloud et Amazon RDS (p. 1610)

Authentification de base de données avec Amazon RDS

Amazon RDS prend en charge plusieurs façons d'authentifier les utilisateurs de base de données.

Rubriques

- Authentification par mot de passe (p. 1519)
- Authentification de base de données IAM (p. 1520)
- Authentification Kerberos (p. 1520)

Authentification par mot de passe

Avec l'authentification par mot de passe, votre instance de base de données effectue toute l'administration des comptes d'utilisateurs. Vous créez des utilisateurs avec des instructions SQL telles que `CREATE USER` et spécifiez des mots de passe dans la clause `IDENTIFIED BY`.

Tous les moteurs de base de données RDS supportent l'authentification par mot de passe. Pour de plus amples informations sur l'authentification par mot de passe, consultez la documentation de votre moteur de base de données.

Avec l'authentification par mot de passe, votre base de données contrôle et authentifie les comptes d'utilisateurs. Si un moteur de base de données dispose de fonctionnalités de gestion de mot de passe solides, il peut améliorer la sécurité. L'authentification de base de données peut être plus facile à administrer en utilisant l'authentification par mot de passe lorsque vous avez de petites communautés d'utilisateurs. Étant donné que des mots de passe en texte clair sont générés dans ce cas, l'intégration avec AWS Secrets Manager peut améliorer la sécurité.

Pour de plus amples informations sur l'utilisation de Secrets Manager avec Amazon RDS, veuillez consulterr Création d'un secret de base et Rotation de secrets pour les Amazon RDS bases de données prises en charge dans le Guide de l'utilisateur AWS Secrets Manager. Pour plus d'informations sur la récupération par programme de vos secrets dans vos applications personnalisées, consultez Récupération de la valeur secrète dans le Guide de l'utilisateur AWS Secrets Manager.

Authentification de base de données IAM

Vous pouvez vous authentifier auprès du de votre instance de base de données à l'aide de l'authentification de base de données AWS Identity and Access Management (IAM). L'authentification de base de données IAM fonctionne avec MySQL et PostgreSQL. Grâce à cette méthode d'authentification, vous n'avez plus besoin de mot de passe pour vous connecter au d'une instance de base de données. En revanche, un jeton d'authentification est nécessaire.

Pour de plus amples informations sur l'authentification de base de données IAM, y compris sur la disponibilité de moteurs DB spécifiques, veuillez consulter Authentification de base de données IAM pour MySQL et PostgreSQL (p. 1554).

Authentification Kerberos

Amazon RDS prend en charge l'authentification externe des utilisateurs de bases de données avec Kerberos et Microsoft Active Directory. Kerberos est un protocole d'authentification réseau qui utilise les tickets et la cryptographie de clé symétrique pour vous éviter d'acheminer vos mots de passe via le réseau. Intégré dans Active Directory, Kerberos est conçu pour authentifier les utilisateurs sur les ressources réseau, par exemple les bases de données.

La prise en charge de Kerberos et Active Directory par Amazon RDS procure les avantages d'une authentification unique et centralisée des utilisateurs de bases de données. Vous pouvez conserver vos informations d'identification utilisateur dans Active Directory. Active Directory vous offre un endroit centralisé de stockage et de gestion des informations d'identification pour plusieurs instances de base de données.

Vous pouvez permettre à vos utilisateurs de bases de données de s'authentifier auprès des instances de bases de données de deux façons. Ils peuvent utiliser les informations d'identification stockées dans AWS Directory Service for Microsoft Active Directory (Enterprise Edition) ou dans votre Active Directory sur site.

Les instances de base de données Microsoft SQL Server, MySQL et PostgreSQL prennent en charge les relations d'approbation de forêt unidirectionnelles et bidirectionnelles. Les instances de base de données Oracle prennent en charge les relations d'approbation de forêt et les relations d'approbation externes unidirectionnelles et bidirectionnelles. Pour de plus amples informations, veuillez consulter Quand créer une relation d'approbation dans le Guide d'administration AWS Directory Service.

Pour de plus amples informations sur l'authentification Kerberos avec un moteur de base de données spécifique, veuillez consulter les sections suivantes :

- Utilisation de l'authentification Windows avec une instance de base de données Amazon RDS pour SQL Server (p. 676)
- Utilisation de l'authentification Kerberos pour MySQL (p. 885)
- Utilisation de l'authentification Kerberos avec Amazon RDS for Oracle (p. 1168)

- Utilisation de l'authentification Kerberos avec Amazon RDS pour PostgreSQL (p. 1450)

> **Note**
>
> Actuellement, l'authentification Kerberos n'est pas prise en charge pour les instances de base de données MariaDB.

Protection des données dans 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 sensitive identifying information, such as your customers' account numbers, into 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 Amazon RDS or other services might get picked up for inclusion in diagnostic logs. When you provide a URL to an external server, don't include credentials information in the URL to validate your request to that server.

Rubriques

- Protection des données à l'aide du chiffrement (p. 1521)
- Confidentialité du trafic inter-réseaux (p. 1535)

Protection des données à l'aide du chiffrement

Vous pouvez activer le chiffrement pour vos ressources de base de données. Vous pouvez également chiffrer les connexions aux instances de base de données.

Rubriques

- Chiffrement des ressources Amazon RDS (p. 1522)

- Gestion de la clé principale client (CMK) (p. 1524)
- Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525)
- Rotation de votre certificat SSL/TLS (p. 1527)

Chiffrement des ressources Amazon RDS

Vous pouvez chiffrer vos instances de base de données Amazon RDS et vos instantanés au repos en activant l'option de chiffrement pour vos instances de base de données Amazon RDS. Les données chiffrées au repos incluent le stockage sous-jacent pour les instances de base de données, les sauvegardes automatiques, les réplicas en lecture et les instantanés.

Les instances de base de données chiffrée Amazon RDS utilisent l'algorithme de chiffrement AES-256 standard pour chiffrer vos données sur le serveur qui héberge vos instances de base de données Amazon RDS. Une fois que vos données ont été chiffrées, Amazon RDS traite l'authentification de l'accès et le déchiffrement de vos données de façon transparente, avec un impact minimal sur les performances. Vous n'avez pas besoin de modifier vos applications clientes de base de données pour utiliser le chiffrement.

> **Note**
>
> Pour les instances de base de données chiffrées et non chiffrées, les données en transit entre la source et le réplica en lecture sont chiffrées, même en cas de réplication entre régions AWS.

Rubriques

- Présentation du chiffrement des ressources Amazon RDS (p. 1522)
- Activation du chiffrement Amazon RDS pour une instance de base de données (p. 1523)
- Disponibilité du chiffrement Amazon RDS (p. 1523)
- Limitations des instances de base de données chiffrées Amazon RDS (p. 1524)

Présentation du chiffrement des ressources Amazon RDS

Les instances de base de données chiffrée Amazon RDS fournissent une couche supplémentaire de protection des données en sécurisant vos données contre tout accès non autorisé au stockage sous-jacent. Vous pouvez utiliser le chiffrement Amazon RDS pour renforcer la protection des données de vos applications déployées dans le cloud et pour satisfaire aux exigences de conformité pour le chiffrement des données au repos.

Amazon RDS prend également en charge le chiffrement d'une instance de base de données Oracle ou SQL Server à l'aide du chiffrement TDE (Transparent Data Encryption). Le chiffrement TDE peut être utilisé avec le chiffrement au repos, bien que l'utilisation simultanée de ces deux chiffrements puisse affecter quelque peu les performances de votre base de données. Vous devez gérer des clés différentes pour chaque méthode de chiffrement. Pour de plus amples informations sur TDE, veuillez consulter Oracle Transparent Data Encryption (p. 1091) ou Prise en charge de Transparent Data Encryption dans SQL Server (p. 704).

Pour gérer les clés principales client (CMK) utilisées pour le chiffrement et le déchiffrement de vos ressources Amazon RDS, utilisez AWS Key Management Service (AWS KMS). AWS KMS combine du matériel et des logiciels sécurisés et hautement disponibles pour fournir un système de gestion de clés à l'échelle du cloud. En utilisant AWS KMS, vous pouvez créer des clés CMK et définir les stratégies qui contrôlent la manière dont ces clés CMK peuvent être utilisées. AWS KMS prend en charge CloudTrail, afin de vous permettre de vérifier que l'utilisation des clés CMK est appropriée. Vous pouvez utiliser vos clés CMK AWS KMS avec Amazon RDS et les services AWS pris en charge tels que Amazon S3, Amazon EBS et Amazon Redshift. Pour obtenir la liste des services qui prennent en charge AWS KMS, consultez Services pris en charge dans le Guide du développeur AWS Key Management Service.

Pour une instance de base de données chiffrée Amazon RDS, tous les journaux, sauvegardes et instantanés sont chiffrés. Un réplica en lecture d'une instance Amazon RDS chiffrée est également chiffré avec la même clé CMK que l'instance de base de données principale lorsque tous deux se trouvent dans la même région AWS. Si l'instance de base de données principale et le réplica en lecture se trouvent dans des régions AWS différentes, vous les chiffrez à l'aide de la clé CMK correspondant à leur région AWS spécifique.

Activation du chiffrement Amazon RDS pour une instance de base de données

Pour activer le chiffrement pour un nouveau cluster de base de données, sélectionnez Enable encryption (Activer le chiffrement) dans la console Amazon RDS. Pour de plus amples informations sur la création d'une instance de base de données, veuillez consulter Création d'une instance de base de données Amazon RDS (p. 146).

Si vous utilisez la commande d'AWS CLI create-db-instance pour créer une instance de base de données chiffrée, affectez au paramètre `--storage-encrypted` la valeur true. Si vous utilisez l'opération d'API CreateDBInstance, affectez au paramètre `StorageEncrypted` la valeur true.

Lorsque vous créez une instance de base de données chiffrée, vous pouvez également fournir l'identificateur de clé principale client (CMK) AWS KMS pour votre clé CMK. Si vous ne spécifiez pas d'identificateur de clé CMK AWS KMS, alors Amazon RDS utilise votre clé CMK par défaut pour votre nouvelle instance de base de données. AWS KMS crée votre clé CMK par défaut pour Amazon RDS pour votre compte AWS. Votre compte AWS dispose d'une clé CMK par défaut différente pour chaque région AWS.

Une fois que vous avez créé une instance de base de données chiffrée, vous ne pouvez pas modifier le type de clé CMK utilisé par cette instance de base de données. Vous devez donc prendre soin de déterminer vos besoins en termes de clés CMK avant de créer votre instance de base de données chiffrée.

Si vous utilisez la commande d'AWS CLI `create-db-instance` pour créer une instance de base de données chiffrée, définissez le paramètre `--kms-key-id` sur l'Amazon Resource Name (ARN) de la clé CMK AWS KMS pour l'instance de base de données. Si vous utilisez l'action d'API Amazon RDS `CreateDBInstance`, affectez au paramètre `KmsKeyId` le nom ARN de votre clé CMK AWS KMS pour l'instance de base de données.

Vous pouvez utiliser le nom ARN d'une clé CMK issue d'un autre compte pour chiffrer une instance de base de données. Vous pouvez aussi créer une instance de base de données à l'aide du compte AWS qui détient la clé CMK AWS KMS utilisée pour chiffrer cette nouvelle instance de base de données. Dans ce cas, l'identificateur de clé AWS KMS que vous passez peut être l'alias de clé CMK AWS KMS au lieu de l'ARN de la clé CMK.

Disponibilité du chiffrement Amazon RDS

Le chiffrement Amazon RDS est actuellement disponible pour tous les moteurs de base de données et types de stockage.

Le chiffrement Amazon RDS est disponible pour la plupart des classes d'instance de base de données. Le tableau suivant répertorie les classes d'instance de base de données qui ne prennent pas en charge le chiffrement Amazon RDS :

Type d'instance	Classe d'instance
Usage général (M1)	db.m1.small db.m1.medium db.m1.large

Type d'instance	Classe d'instance
	db.m1.xlarge
Mémoire optimisée (M2)	db.m2.xlarge db.m2.2xlarge db.m2.4xlarge
Capacité de transmission en rafales (T2)	db.t2.micro

> **Note**
>
> Le chiffrement au repos n'est pas disponible pour les instances de base de données exécutant SQL Server Express Edition.

Limitations des instances de base de données chiffrées Amazon RDS

Les limitations suivantes existent pour les instances de base de données chiffrées Amazon RDS :

- Vous pouvez uniquement activer le chiffrement pour une instance de base de données Amazon RDS lorsque vous la créez, et non pas après sa création.

  Cependant, parce que vous pouvez chiffrer une copie d'un instantané de base de données non chiffré, vous pouvez ajouter le chiffrement efficacement à une instance de base de données non chiffrée. Autrement dit, vous pouvez créer un instantané de votre instance de base de données et ensuite créer une copie chiffrée de l'instantané. Vous pouvez ensuite restaurer une instance de base de données à partir de l'instantané chiffré et vous aurez une copie chiffrée de votre instance de base de données d'origine. Pour plus d'informations, consultez Copie d'un instantané (p. 332).
- Les d'instances de base de données qui sont chiffrés ne peuvent pas être modifiés pour désactiver le chiffrement.
- Vous ne pouvez pas avoir un réplica en lecture chiffré d'une instance de base de données non chiffrée ni un réplica en lecture non chiffré d'une instance de base de données chiffrée.
- Les réplicas en lecture chiffrés doivent être chiffrés avec la même clé CMK que l'instance de base de données source lorsque tous deux se trouvent dans la même région AWS.
- Vous ne pouvez pas restaurer un instantané non chiffré ou une sauvegarde non chiffrée vers une instance de base de données chiffrée.
- Pour copier un instantané chiffré d'une région AWS à une autre, vous devez spécifier l'identifiant de clé AWS KMS de la région AWS de destination. En effet, les clés CMK AWS KMS sont spécifiques à la région AWS dans laquelle elles sont créées.

  L'instantané source reste chiffré tout au long du processus de copie. AWS KMS utilise le chiffrement d'enveloppe pour protéger les données pendant le processus de copie. Pour de plus amples informations sur le fonctionnement du chiffrement d'enveloppe, veuillez consulter Chiffrement d'enveloppe.

Gestion de la clé principale client (CMK)

Vous pouvez gérer les clés principales client (CMK) utilisées pour les d' instances de base de données chiffrées Amazon RDS à l'aide de AWS Key Management Service(AWS KMS) dans la console AWS KMS . Si vous souhaitez un contrôle total sur une clé CMK, vous devez en créer une gérée par le client.

Vous ne pouvez pas supprimer, révoquer, ni alterner les clés CMK par défaut mises en service par AWS KMS. Vous ne pouvez pas partager un instantané chiffré à l'aide de la clé CMK AWS KMS par défaut du compte AWS qui a partagé l'instantané.

Vous pouvez consulter les journaux d'audit de chaque action effectuée à l'aide d'une clé CMK gérée par le client en utilisant AWS CloudTrail.

> **Important**
>
> Quand RDS rencontre une instance de base de données chiffré(e) par une clé CMK à laquelle RDS n'a pas accès, RDS place l'instance de base de données dans un état final. Dans cet état, l'instance de base de données n'est plus disponible et l'état actuel de la base de données ne peut pas être récupéré. Pour restaurer l'instance de base de données, vous devez réactiver l'accès à la clé de CMK pour RDS, puis restaurer l'instance de base de données à partir d'une sauvegarde.

Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données

Vous pouvez utiliser SSL ou TLS à partir de votre application pour chiffrer une connexion à une instance de base de données exécutant MySQL, MariaDB, SQL Server, Oracle ou PostgreSQL. Chaque moteur DB possède son propre processus d'implémentation SSL/TLS. Pour apprendre à implémenter SSL/TLS pour votre instance de base de données, utilisez le lien suivant qui correspond à votre moteur DB :

- Utilisation de SSL avec une instance de base de données MariaDB (p. 551)
- Utilisation de SSL avec une instance DB Microsoft SQL Server (p. 669)
- Utilisation de SSL avec une instance de base de données MySQL (p. 788)
- Utilisation de SSL avec une instance de base de données Oracle (p. 937)
- Utilisation de SSL avec une instance de base de données PostgreSQL (p. 1515)

> **Important**
>
> Pour de plus amples informations sur la configuration de votre certificat, veuillez consulter Rotation de votre certificat SSL/TLS (p. 1527).

> **Note**
>
> Tous les certificats sont disponibles uniquement pour le téléchargement sur des connexions SSL/TLS.

Pour obtenir un certificat racine qui fonctionne pour toutes les régions AWS, à l'exception des régions d'adhésion AWS, téléchargez-le à partir de ttps://s3.amazonaws.com/rds-downloads/rds-ca-2019-root.pem.

Ce certificat racine est une entité racine approuvée et elle doit fonctionner dans la plupart des cas, mais peut échouer si votre application n'accepte pas les chaînes de certificats. Si votre application n'accepte pas les chaînes de certificats, téléchargez le certificat spécifique à la région AWS dans la liste des certificats intermédiaires fournie ultérieurement dans cette section.

Vous pouvez télécharger un ensemble de certificats contenant les certificats intermédiaires et racine à l'adresse https://s3.amazonaws.com/rds-downloads/rds-combined-ca-bundle.pem.

Si votre application est sur Microsoft Windows et nécessite un fichier PKCS7, vous pouvez télécharger l'ensemble de certificats PKCS7. Cet ensemble contient les certificats intermédiaires et racine à l'adresse https://s3.amazonaws.com/rds-downloads/rds-combined-ca-bundle.p7b.

> **Note**
>
> Amazon RDS Proxy utilise des certificats de la AWS Certificate Manager (ACM). Si vous utilisez RDS Proxy, vous n'avez pas besoin de télécharger des certificats Amazon RDS ou de mettre à jour des applications utilisant des connexions RDS Proxy. Pour de plus amples informations sur

l'utilisation de TLS/SSL avec RDS Proxy, veuillez consulter Utilisation de TLS/SSL avec RDS Proxy (p. 172).

Certificats racine pour les régions d'adhésion AWS

Si vous utilisez une région d'adhésion AWS, vous pouvez télécharger le certificat racine à partir du tableau suivant.

Région d'adhésion AWS	Certificat racine
Afrique (Le Cap)	rds-ca-af-south-1-2019-root.pem
Asie-Pacifique (Hong Kong)	rds-ca-ap-east-1-2019-root.pem
Europe (Milan)	rds-ca-eu-south-1-2019-root.pem
Moyen-Orient (Bahreïn)	rds-ca-me-south-1-2019-root.pem

Certificats intermédiaires

Vous devrez peut-être utiliser un certificat intermédiaire pour vous connecter à votre région AWS. Par exemple, vous devez utiliser un certificat intermédiaire pour vous connecter à la région AWS GovCloud (USA Ouest) à l'aide de SSL/TLS. Si vous avez besoin d'un certificat intermédiaire pour une région AWS donnée, téléchargez le certificat depuis la table suivante :

Région AWS	Certificat intermédiaire
Asie-Pacifique (Mumbai)	rds-ca-2019-ap-south-1.pem
Asie-Pacifique (Tokyo)	rds-ca-2019-ap-northeast-1.pem
Asie-Pacifique (Séoul)	rds-ca-2019-ap-northeast-2.pem
Asie-Pacifique (Osaka-Local)	rds-ca-2019-ap-northeast-3.pem
Asie-Pacifique (Singapour)	rds-ca-2019-ap-southeast-1.pem
Asie-Pacifique (Sydney)	rds-ca-2019-ap-southeast-2.pem
Canada (Centre)	rds-ca-2019-ca-central-1.pem
Europe (Francfort)	rds-ca-2019-eu-central-1.pem
Europe (Irlande)	rds-ca-2019-eu-west-1.pem
Europe (Londres)	rds-ca-2019-eu-west-2.pem
Europe (Paris)	rds-ca-2019-eu-west-3.pem
Europe (Stockholm)	rds-ca-2019-eu-north-1.pem
Amérique du Sud (São Paulo)	rds-ca-2019-sa-east-1.pem
USA Est (Virginie du Nord)	rds-ca-2019-us-east-1.pem
USA Est (Ohio)	rds-ca-2019-us-east-2.pem
USA Ouest (Californie du Nord)	rds-ca-2019-us-west-1.pem
USA Ouest (Oregon)	rds-ca-2019-us-west-2.pem

Certificats AWS GovCloud (US)

Vous pouvez télécharger le certificat racine pour la région AWS GovCloud (US) depuis la liste suivante :

AWS GovCloud (US, côte est) (Root CA-2017)

AWS GovCloud (US, côte ouest) (Root CA-2017)

Vous pouvez télécharger le certificat intermédiaire pour la région AWS GovCloud (USA) depuis la liste suivante :

AWS GovCloud (US, côte est) (CA-2017)

AWS GovCloud (US, côte ouest) (CA-2017)

AWS GovCloud (US, côte ouest) (CA-2012)

Pour obtenir un ensemble de certificats contenant les certificats intermédiaire et racine pour les régions AWS GovCloud (US), téléchargez-le à l'adresse https://s3.us-gov-west-1.amazonaws.com/rds-downloads/rds-combined-ca-us-gov-bundle.pem.

Rotation de votre certificat SSL/TLS

En date du 5 mars 2020, les certificats CA-2015 Amazon RDS ont expiré. Si vous utilisez ou prévoyez d'utiliser le protocole SSL (Secure Sockets Layer) ou TLS (Transport Layer Security) avec vérification de certificat pour vous connecter à vos instances de base de données RDS, vous avez besoin de certificats CA-2019 Amazon RDS, qui sont activés par défaut pour les nouvelles instances de base de données. Si vous n'utilisez pas actuellement le protocole SSL/TLS avec vérification de certificat, il se peut que vous ayez encore des certificats CA-2015 expirés et que vous deviez les mettre à jour vers des certificats CA-2019 si vous prévoyez d'utiliser le protocole SSL/TLS avec vérification de certificat pour vous connecter à vos bases de données RDS.

Suivez ces instructions pour effectuer vos mises à jour. Avant de mettre à jour vos instances de base de données pour utiliser le nouveau certificat CA, veillez à mettre à jour vos clients ou applications connectés à vos bases de données RDS.

Dans le cadre des bonnes pratiques de sécurité AWS, Amazon RDS fournit de nouveaux certificats d'autorité de certification. Pour de plus amples informations sur les nouveaux certificats et les régions AWS prises en charge, veuillez consulter Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).

> **Note**
>
> Amazon RDS Proxy utilise des certificats de la AWS Certificate Manager (ACM). Si vous utilisez RDS Proxy, lorsque vous effectuez la rotation de votre certificat SSL/TLS, vous n'avez pas besoin de mettre à jour les applications qui utilisent des connexions RDS Proxy. Pour de plus amples informations sur l'utilisation de TLS/SSL avec RDS Proxy, veuillez consulter Utilisation de TLS/SSL avec RDS Proxy (p. 172).

> **Note**
>
> Si vous utilisez une application Go version 1.15 avec une instance de base de données créée ou mise à jour vers le certificat `rds-ca-2019` avant le 28 juillet 2020, vous devez mettre à jour à nouveau le certificat. Exécutez la commande `modify-db-instance` indiquée dans la section AWS CLI en utilisant `rds-ca-2019` comme identifiant de certificat d'autorité de certification. Dans ce cas, il n'est pas possible de mettre à jour le certificat via AWS Management Console. Si vous avez créé votre instance de base de données ou mis à jour son certificat après le 28 juillet 2020, aucune action n'est requise. Pour de plus amples informations, veuillez consulter le problème GitHub Go 39568.

Rubriques

- Mise à jour de votre certificat CA en modifiant votre instance de base de données (p. 1528)
- Mise à jour de votre certificat CA en appliquant la maintenance de l'instance de base de données (p. 1530)
- Exemple de script pour importer les certificats dans votre magasin d'approbations (p. 1534)

Mise à jour de votre certificat CA en modifiant votre instance de base de données

Procédez comme suit pour mettre à jour votre certificat CA.

Mise à jour de votre certificat CA en modifiant votre instance de base de données

1. Téléchargez le nouveau certificat SSL/TLS comme décrit dans la section Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).
2. Mettez à jour vos applications de sorte à utiliser le nouveau certificat SSL/TLS.

   Les méthodes de mise à jour des applications pour les nouveaux certificats SSL/TLS dépendent de vos applications spécifiques. Faites-vous aider par vos développeurs d'applications pour la mise à jour des certificats SSL/TLS de vos applications.

   Pour de plus amples informations sur la vérification des connexions SSL/TLS et la mise à jour des applications pour chaque moteur de bases de données, veuillez consulter les rubriques suivantes :

   - Mise à jour des applications pour se connecter aux instances de bases de données MariaDB à l'aide des nouveaux certificats SSL/TLS (p. 560)
   - Mise à jour des applications pour se connecter aux instances de bases de données Microsoft SQL Server à l'aide des nouveaux certificats SSL/TLS (p. 625)
   - Mise à jour des applications pour se connecter aux instances de bases de données MySQL à l'aide des nouveaux certificats SSL/TLS (p. 799)
   - Mise à jour des applications pour se connecter aux instances de bases de données Oracle à l'aide des nouveaux certificats SSL/TLS (p. 969)
   - Mise à jour des applications pour se connecter aux instances de bases de données PostgreSQL à l'aide des nouveaux certificats SSL/TLS (p. 1369)

   Pour obtenir un exemple de script qui met à jour le magasin d'approbations d'un système d'exploitation Linux, consultez Exemple de script pour importer les certificats dans votre magasin d'approbations (p. 1534).

   > **Note**
   >
   > L'ensemble de certificats contient des certificats pour le nouveau et l'ancien CA, ce qui signifie que vous pouvez mettre à niveau votre application en toute sécurité et conserver la connectivité pendant la période de transition. Si vous utilisez AWS Database Migration Service pour migrer une base de données vers une instance de base de données, nous vous recommandons d'utiliser l'ensemble de certificats pour garantir la connectivité pendant la migration.
3. Modifiez l'instance de base de données afin de remplacer le CA rds-ca-2015 par rds-ca-2019.

   > **Important**
   >
   > Par défaut, cette opération redémarre votre instance de base de données. Si vous ne souhaitez pas redémarrer votre instance de base de données au cours de cette opération, vous pouvez utiliser la commande d'interface de ligne de commande `modify-db-instance` et spécifier l'option `--no-certificate-rotation-restart`.
   > Cette option permet de ne pas effectuer la rotation du certificat avant le prochain redémarrage de la base de données, que ce soit pour une maintenance planifiée ou non planifiée. Cette option n'est recommandée que si vous n'utilisez pas SSL/TLS.

Si vous rencontrez des problèmes de connectivité après l'expiration du certificat, utilisez l'option Appliquer immédiatement en la spécifiant dans la console ou en spécifiant l'option `--apply-immediately` à l'aide d'AWS CLI. Par défaut, il est prévu que cette opération soit exécutée pendant votre prochaine fenêtre de maintenance.

Vous pouvez utiliser AWS Management Console ou l'AWS CLI pour remplacer le certificat CA rds-ca-2015 par rds-ca-2019 pour une instance de base de données.

Console

Pour remplacer le certificat CA rds-ca-2015 par rds-ca-2019 pour une instance de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le panneau de navigation, choisissez Bases de données, puis l'instance de base de données que vous souhaitez modifier.
3. Sélectionnez Modify (Modifier).

La page Modifier l'instance de base de données s'affiche.

4. Dans la section Réseau et sécurité, choisissez rds-ca-2019.

5. Choisissez Continuer et vérifiez le récapitulatif des modifications.
6. Pour appliquer les modifications immédiatement, choisissez Appliquer immédiatement.

   Important

   En choisissant cette option, votre base de données redémarre immédiatement.

7. Sur la page de confirmation, examinez vos modifications. Si elles sont correctes, choisissez Modification d'une instance de base de données pour enregistrer vos modifications.

> **Important**
>
> Lorsque vous planifiez cette opération, assurez-vous d'avoir mis à jour votre magasin d'approbation côté client au préalable.

Ou choisissez Retour pour revoir vos modifications, ou choisissez Annuler pour les annuler.

AWS CLI

Pour utiliser l'AWS CLI afin de remplacer le certificat CA rds-ca-2015 par rds-ca-2019 pour une instance de base de données, appelez la commande modify-db-instance. Spécifiez l'identifiant d'instance de base de données et l'option `--ca-certificate-identifier`.

> **Important**
>
> Lorsque vous planifiez cette opération, assurez-vous d'avoir mis à jour votre magasin d'approbation côté client au préalable.

Example

Le code suivant modifie `mydbinstance` en définissant le certificat CA sur `rds-ca-2019`. Les modifications sont appliquées pendant le créneau de maintenance suivant à l'aide de `--no-apply-immediately`. Pour appliquer les modifications immédiatement, utilisez `--apply-immediately`.

> **Important**
>
> Par défaut, cette opération redémarre votre instance de base de données. Si vous ne souhaitez pas redémarrer votre instance de base de données au cours de cette opération, vous pouvez utiliser la commande de l'interface de ligne de commande `modify-db-instance` et spécifier l'option `--no-certificate-rotation-restart`.
> Cette option permet de ne pas effectuer la rotation du certificat avant le prochain redémarrage de la base de données, que ce soit pour une maintenance planifiée ou non planifiée. Cette option n'est recommandée que si vous n'utilisez pas SSL/TLS.
> Pour appliquer la mise à jour immédiatement, utilisez `--apply-immediately`. Par défaut, il est prévu que cette opération soit exécutée pendant votre prochaine fenêtre de maintenance.

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --ca-certificate-identifier rds-ca-2019 \
    --no-apply-immediately
```

Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --ca-certificate-identifier rds-ca-2019 ^
    --no-apply-immediately
```

Mise à jour de votre certificat CA en appliquant la maintenance de l'instance de base de données

Procédez comme suit pour mettre à jour votre certificat CA en appliquant la maintenance d'instance de base de données.

Mise à jour de votre certificat CA en appliquant la maintenance d'instance de base de données

1. Téléchargez le nouveau certificat SSL/TLS comme décrit dans la section Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).
2. Mettez à jour vos applications de base de données de façon à utiliser le nouveau certificat SSL/TLS.

   Les méthodes de mise à jour des applications pour les nouveaux certificats SSL/TLS dépendent de vos applications spécifiques. Faites-vous aider par vos développeurs d'applications pour la mise à jour des certificats SSL/TLS de vos applications.

   Pour de plus amples informations sur la vérification des connexions SSL/TLS et la mise à jour des applications pour chaque moteur de bases de données, veuillez consulter les rubriques suivantes :

   - Mise à jour des applications pour se connecter aux instances de bases de données MariaDB à l'aide des nouveaux certificats SSL/TLS (p. 560)
   - Mise à jour des applications pour se connecter aux instances de bases de données Microsoft SQL Server à l'aide des nouveaux certificats SSL/TLS (p. 625)
   - Mise à jour des applications pour se connecter aux instances de bases de données MySQL à l'aide des nouveaux certificats SSL/TLS (p. 799)
   - Mise à jour des applications pour se connecter aux instances de bases de données Oracle à l'aide des nouveaux certificats SSL/TLS (p. 969)
   - Mise à jour des applications pour se connecter aux instances de bases de données PostgreSQL à l'aide des nouveaux certificats SSL/TLS (p. 1369)

   Pour obtenir un exemple de script qui met à jour le magasin d'approbations d'un système d'exploitation Linux, consultez Exemple de script pour importer les certificats dans votre magasin d'approbations (p. 1534).

   > **Note**
   >
   > L'ensemble de certificats contient des certificats pour le nouveau et l'ancien CA, ce qui signifie que vous pouvez mettre à niveau votre application en toute sécurité et conserver la connectivité pendant la période de transition.
3. Appliquez la maintenance d'instance de base de données pour changer le certificat CA de rds-ca-2015 à rds-ca-2019.

   > **Important**
   >
   > Vous pouvez choisir d'appliquer la modification immédiatement. Par défaut, il est prévu que cette opération soit exécutée pendant votre prochaine fenêtre de maintenance.

Vous pouvez utiliser AWS Management Console pour effectuer la maintenance des instances de base de données afin de modifier le certificat d'autorité de certification de rds-ca-2015 en rds-ca-2019 pour plusieurs instances de base de données.

Mise à jour de votre certificat CA en appliquant la maintenance à plusieurs instances de base de données

Utilisez la AWS Management Console pour modifier le certificat CA pour plusieurs instances de base de données.

Modification du certificat CA rds-ca-2015 par rds-ca-2019 pour une plusieurs instances de base de données

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.

2. Dans la panneau de navigation, choisissez Databases (Bases de données).

   Le panneau de navigation affiche l'option Certificate update (Mise à jour du certificat) qui indique le nombre total d'instances de base de données affectées.

   Choisissez Certificate update (Mise à jour du certificat) dans le panneau de navigation.

   La page Mise à jour de vos certificats Amazon RDS SSL/TLS s'affiche.

> **Note**
>
> Cette page affiche uniquement les instances de base de données de la région AWS actuelle. Si vous avez des instances de base de données dans plusieurs régions AWS, consultez cette page dans chaque région AWS pour voir toutes les instances de base de données avec d'anciens certificats SSL/TLS.

3. Choisissez l'instance de base de données que vous voulez mettre à jour.

   Vous pouvez planifier la rotation du certificat pour votre prochaine fenêtre de maintenance en sélectionnant Mettre à jour lors de la prochaine fenêtre de maintenance. Appliquez la rotation immédiatement en choisissant Update now (Mettre à jour maintenant).

   > **Important**
   >
   > Lorsque votre certificat d'autorité de certification procède à une rotation, l'opération redémarre votre instance de base de données.
   > Si vous rencontrez des problèmes de connectivité après l'expiration du certificat, utilisez l'option Update now (Mettre à jour maintenant).

4. Si vous choisissez Mettre à jour dans la prochaine fenêtre de maintenance ou Mettre à jour maintenant, vous êtes invité à confirmer la rotation du certificat CA.

   > **Important**
   >
   > Avant de planifier la rotation du certificat CA sur votre base de données, mettez à jour toutes les applications clientes qui utilisent SSL/TLS et le certificat de serveur pour se connecter. Ces mises à jour sont spécifiques à votre moteur de base de données. Pour déterminer si vos applications utilisent SSL/TLS et le certificat de serveur pour se connecter, consultez Étape n° 2 : mettez à jour vos applications de base de données pour utiliser le nouveau certificat SSL/TLS. (p. 1531). Après avoir mis à jour ces applications clientes, vous pouvez confirmer la rotation du certificat CA.

Pour continuer, cochez la case, puis cliquez sur Confirmation.

5. Répétez les étapes 3 et 4 pour chaque instance de base de données que vous souhaitez mettre à jour.

Exemple de script pour importer les certificats dans votre magasin d'approbations

Voici des exemples de scripts shell qui importent le lot de certificats dans un magasin d'approbations.

Rubriques

- Exemple de script d'importation de certificats sur Linux (p. 1534)
- Exemple de script d'importation de certificats sur macOS (p. 1535)

Exemple de script d'importation de certificats sur Linux

Voici un exemple de script shell qui importe le lot de certificats vers un magasin d'approbations sur un système d'exploitation Linux.

```
mydir=tmp/certs
if [ ! -e "${mydir}" ]
then
mkdir -p "${mydir}"
fi

truststore=${mydir}/rds-truststore.jks
storepassword=changeit

curl -sS "https://s3.amazonaws.com/rds-downloads/rds-combined-ca-bundle.pem" > ${mydir}/
rds-combined-ca-bundle.pem
awk 'split_after == 1 {n++;split_after=0} /-----END CERTIFICATE-----/ {split_after=1}{print
 > "rds-ca-" n ".pem"}' < ${mydir}/rds-combined-ca-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}/rds-combined-ca-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
```

Exemple de script d'importation de certificats sur macOS

Voici un exemple de script shell qui importe le lot de certificats vers un magasin d'approbations sur macOS.

```
mydir=tmp/certs
if [ ! -e "${mydir}" ]
then
mkdir -p "${mydir}"
fi

truststore=${mydir}/rds-truststore.jks
storepassword=changeit

curl -sS "https://s3.amazonaws.com/rds-downloads/rds-combined-ca-bundle.pem" > ${mydir}/
rds-combined-ca-bundle.pem
split -p "-----BEGIN CERTIFICATE-----" ${mydir}/rds-combined-ca-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}/rds-combined-ca-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
```

Confidentialité du trafic inter-réseaux

Les connexions sont protégées entre Amazon RDS et les applications sur site, ainsi qu'entre Amazon RDS et d'autres ressources AWS dans la même région AWS.

Trafic entre les clients de service et sur site et les applications

Vous disposez de deux options de connectivité entre votre réseau privé et AWS :

- Une connexion VPN site à site AWS. Pour plus d'informations, consultez Qu'est-ce qu'AWS Site-to-Site VPN ?
- Une connexion AWS Direct Connect. Pour plus d'informations, consultez Qu'est-ce qu'AWS Direct Connect ?

Vous accédez à Amazon RDS via le réseau en utilisant les opérations d'API publiées par AWS. Les clients doivent prendre en charge le protocole Transport Layer Security (TLS) 1.0. Nous recommandons TLS 1.2. Les clients doivent également prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La plupart des systèmes modernes tels que Java 7 et versions ultérieures prennent en charge ces modes. En outre, les demandes doivent être signées à l'aide d'un identificateur de clé d'accès et d'une clé d'accès secrète associée à un mandataire IAM. Vous pouvez également utiliser le service AWS Security Token Service (STS) pour générer les informations d'identification de sécurité temporaire pour signe des demandes.

Identity and Access Management dans Amazon RDS

AWS Identity and Access Management (IAM) est un service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux ressources AWS. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (disposant des autorisations) à utiliser les ressources Amazon RDS. IAM est un service AWS que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé (p. 1536)
- Authentification avec des identités (p. 1537)
- Gestion de l'accès à l'aide de stratégies (p. 1539)
- Comment Amazon RDS fonctionne avec IAM (p. 1540)
- Exemples de stratégies basées sur l'identité Amazon RDS (p. 1544)
- Authentification de base de données IAM pour MySQL et PostgreSQL (p. 1554)
- Résolution des problèmes liés à Identity and Access Amazon RDS (p. 1581)

Public ciblé

Votre utilisation d'AWS Identity and Access Management (IAM) évolue selon la tâche que vous réalisez dans Amazon RDS.

Utilisateur du service – Si vous utilisez le service Amazon RDS pour effectuer votre tâche, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Plus vous utiliserez de fonctionnalités Amazon RDS pour effectuer votre travail, plus vous pourrez avoir besoin d'autorisations supplémentaires. Comprendre la gestion des accès peut vous aider à demander à votre administrateur les autorisations appropriées. Si vous ne pouvez pas accéder à une fonctionnalité dans Amazon RDS, consultez Résolution des problèmes liés à Identity and Access Amazon RDS (p. 1581).

Administrateur du service – Si vous êtes le responsable des ressources Amazon RDS de votre entreprise, vous bénéficiez probablement d'un accès total à Amazon RDS. C'est à vous de déterminer les fonctionnalités et les ressources Amazon RDS auxquelles vos employés pourront accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM avec Amazon RDS, consultez Comment Amazon RDS fonctionne avec IAM (p. 1540).

Administrateur IAM – Si vous êtes un administrateur IAM, vous souhaiterez peut-être obtenir des détails sur la façon dont vous pouvez écrire des stratégies pour gérer l'accès à Amazon RDS. Pour obtenir des exemples de stratégies Amazon RDS basées sur l'identité que vous pouvez utiliser dans IAM, consultez Exemples de stratégies basées sur l'identité Amazon RDS (p. 1544).

Authentification avec des identités

L'authentification correspond au processus par lequel vous vous connectez à AWS via vos informations d'identification. Pour plus d'informations sur la signature à l'aide d'AWS Management Console, consultez La console et la page de connexion IAM dans le IAM Guide de l'utilisateur.

Vous devez être authentifié (connecté à AWS) en tant que Utilisateur racine d'un compte AWS ou utilisateurIAM, ou en assumant un rôle IAM. Vous pouvez également utiliser l'authentification de connexion unique de votre entreprise ou vous connecter via Google ou Facebook. Dans ce cas, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS avec des informations d'identification d'une autre entreprise, vous assumez indirectement un rôle.

Pour vous connecter directement à la AWS Management Console, utilisez votre mot de passe avec votre e-mail utilisateur racine ou votre nom d'utilisateur IAM. Vous pouvez accéder à AWS par programmation avec vos clés d'accès utilisateur utilisateur racine ou IAM. AWS fournit un kit de développement logiciel (SDK) et des outils de ligne de commande pour signer de manière cryptographique votre requête avec vos informations d'identification. Si vous n'utilisez pas les outils AWS, vous devez signer la requête vous-même. Pour ce faire, utilisez Signature Version 4, un protocole permettant d'authentifier les demandes d'API entrantes. Pour en savoir plus sur l'authentification des demandes, consultez Processus de signature Signature Version 4 dans AWS General Reference.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être également fournir des informations de sécurité supplémentaires. Par exemple, AWS vous recommande d'utiliser l'authentification multi-facteurs (MFA) pour améliorer la sécurité de votre compte. Pour en savoir plus, consultez Utilisation de Multi-Factor Authentication (MFA) dans AWS dans le IAM Guide de l'utilisateur.

Utilisateur racine d'un compte AWS

Lorsque vous créez un compte AWS, vous commencez avec une seule identité de connexion disposant d'un accès complet à tous les services et ressources AWS du compte. Cette identité est appelée la utilisateur racinedu compte AWS et elle est accessible après connexion à l'aide de l'adresse e-mail et du mot de passe utilisés pour la création du compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes, y compris pour les tâches administratives. Au lieu de cela, respectez la bonne pratique qui consiste à avoir recours à l'utilisateur racine uniquement pour créer le premier utilisateurIAM. Ensuite, mettez en sécurité les informations d'identification de l'utilisateur racine et utilisez-les pour effectuer uniquement certaines tâches de gestion des comptes et des services.

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité dans votre compte AWS qui dispose d'autorisations spécifiques pour une seule personne ou application. Un utilisateur IAM peut disposer d'informations d'identification à long terme comme un nom d'utilisateur et un mot de passe ou un ensemble de clés d'accès. Pour savoir comment générer des clés d'accès, consultez Gestion des clés d'accès pour les utilisateurs IAM dans le IAM Guide de l'utilisateur. Lorsque vous générez des clés d'accès pour un utilisateur IAM, veillez à afficher et enregistrer la paire de clés de manière sécurisée. Vous ne pourrez plus récupérer la clé d'accès secrète à l'avenir. Au lieu de cela, vous devrez générer une nouvelle paire de clés d'accès.

Un groupe IAM est une identité qui spécifie un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé Admins IAM et accorder à ce groupe les autorisations leur permettant d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le IAM Guide de l'utilisateur.

Vous pouvez vous authentifier auprès de votre d'instance de base de données à l'aide de l'authentification de base de données IAM.

L'authentification de base de données IAM fonctionne avec les moteurs de base de données suivants :

- Amazon RDS pour MySQL
- Amazon RDS pour PostgreSQL

Pour plus d'informations sur l'authentification auprès de votre d'instance de base de données avec IAM, consultez Authentification de base de données IAM pour MySQL et PostgreSQL (p. 1554).

Rôles IAM

Un rôle IAM est une entité au sein de votre compte AWS qui dispose d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais un rôle n'est pas associé à une personne en particulier. Vous pouvez temporairement endosser un rôle IAM dans l'AWS Management Console grâce au changement de rôle. Vous pouvez obtenir un rôle en appelant une opération d'API AWS CLI ou AWS à l'aide d'une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le IAM Guide de l'utilisateur.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Autorisations utilisateur IAM temporaires – Un utilisateur IAM peut endosser un rôle IAM pour accepter différentes autorisations temporaires concernant une tâche spécifique.
- Accès d'utilisateurs fédérés – Au lieu de créer un utilisateur IAM, vous pouvez utiliser des identités d'utilisateur préexistantes provenant d'AWS Directory Service, de l'annuaire d'utilisateurs de votre entreprise ou d'un fournisseur d'identité web. On parle alors d'utilisateurs fédérés. AWS attribue un rôle à un utilisateur fédéré lorsque l'accès est demandé via un fournisseur d'identité. Pour plus d'informations sur les utilisateurs fédérés, consultez Utilisateurs fédérés et rôles dans le IAM Guide de l'utilisateur.
- Accès entre comptes – Vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (mandataire de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès entre plusieurs comptes. Toutefois, certains services AWS vous permettent d'attacher une stratégie directement à une ressource (au lieu d'utiliser un rôle en tant que proxy). Pour en savoir plus sur la différence entre les rôles et les stratégies basées sur les ressources pour l'accès entre comptes, consultez Différence entre les rôles IAM et les stratégies basées sur les ressources dans le IAM Guide de l'utilisateur.
- Accès à un service AWS –Un rôle de service est un rôle IAM qu'un service assume pour effectuer des actions dans votre compte en votre nom. Lorsque vous configurez certains environnements de services AWS, vous devez définir un rôle que ce service devra assumer. Ce rôle de service doit comprendre toutes les autorisations nécessaires pour que le service puisse accéder aux ressources AWS dont il a besoin. Les rôles de service varient d'un service à un service, mais nombre d'entre eux vous permettent de choisir vos autorisations, tant que vous respectez les exigences documentées pour le service en question. Les rôles de service fournissent un accès uniquement au sein de votre compte et ne peuvent pas être utilisés pour accorder l'accès à des services dans d'autres comptes. Vous créez, modifiez et supprimez un rôle de service à partir d'IAM. Par exemple, vous pouvez créer un rôle qui permet à Amazon Redshift d'accéder à un compartiment Amazon S3 en votre nom, puis de charger les données stockées dans ce compartiment dans un cluster Amazon Redshift. Pour plus d'informations, consultez Création d'un rôle pour déléguer des autorisations à un service AWS dans le IAM Guide de l'utilisateur.
- Applications qui s'exécutent sur Amazon EC2 –Vous pouvez utiliser un rôle IAM pour gérer des informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et

effectuent des demandes d'API AWS CLI ou AWS. Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un rôle AWS à une instance EC2 et le rendre disponible à toutes les applications associées, vous pouvez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le IAM Guide de l'utilisateur.

Pour savoir si vous devez utiliser ces rôles IAM ou non, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le IAM Guide de l'utilisateur.

Gestion de l'accès à l'aide de stratégies

Vous contrôlez les accès dans AWS en créant des stratégies et en les attachant à des identités IAM ou à des ressources AWS. Une stratégie est un objet dans AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit les autorisations de ces dernières. AWS évalue ces stratégies lorsqu'une entité (utilisateur racine, utilisateur IAM ou rôle IAM) envoie une demande. Les autorisations dans les stratégies déterminent si la demande est autorisée ou refusée. La plupart des stratégies sont stockées dans AWS en tant que documents JSON. Pour plus d'informations sur la structure et le contenu du document de stratégie JSON, consultez Présentation des stratégies JSON dans le IAM Guide de l'utilisateur.

Les stratégies permettent à un administrateur IAM de spécifier qui a accès aux ressources AWSet quelles actions ces personnes peuvent exécuter sur ces ressources. Chaque entité IAM (utilisateur ou rôle) démarre sans autorisation. En d'autres termes, par défaut, les utilisateurs ne peuvent rien faire, pas même changer leurs propres mots de passe. Pour autoriser un utilisateur à effectuer une opération, un administrateur doit associer une stratégie d'autorisations à ce dernier. Il peut également ajouter l'utilisateur à un groupe disposant des autorisations prévues. Lorsqu'un administrateur accorde des autorisations à un groupe, tous les utilisateurs de ce groupe se voient octroyer ces autorisations.

Les stratégies IAM définissent les autorisations d'une action quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une stratégie qui autorise l'action `iam:GetRole`. Un utilisateur avec cette stratégie peut obtenir des informations utilisateur à partir de l'AWS Management Console, de l'AWS CLI ou de l'API AWS.

Stratégies basées sur l'identité

Les stratégies basées sur l'identité sont des documents de stratégie d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un rôle ou un groupe IAM. Ces stratégies contrôlent les actions que peut exécuter cette identité, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une stratégie basée sur l'identité, consultez Création de stratégies IAM dans le IAM Guide de l'utilisateur.

Les stratégies basées sur l'identité peuvent être classées comme étant des stratégies en ligne ou des stratégies gérées. Les stratégies en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les stratégies gérées sont des stratégies autonomes que vous pouvez lier à plusieurs utilisateurs, groupes et rôles de votre compte AWS. Les stratégies gérées incluent les stratégies gérées par AWS et les stratégies gérées par le client. Pour découvrir comment choisir entre une politique gérée ou une politique en ligne, consultez Choix entre les stratégies gérées et les stratégies en ligne dans le IAM Guide de l'utilisateur.

Les stratégies gérées par AWS suivantes, que vous pouvez attacher aux utilisateurs de votre compte, sont propres à Amazon RDS :

- AmazonRDSReadOnlyAccess – Accorde un accès en lecture seule à toutes les ressources Amazon RDS pour le compte AWS spécifié.
- AmazonRDSFullAccess – Accorde l'accès total à toutes les ressources Amazon RDS pour le compte AWS spécifié.

Autres types de stratégie

AWS prend en charge d'autres types de stratégies moins courantes. Ces types de stratégies peuvent définir le nombre maximal d'autorisations qui vous sont accordées par des types de stratégies plus courants.

- Limite d'autorisations – Une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez les autorisations maximales qu'une stratégie basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations obtenues représentent la combinaison des stratégies basées sur l'identité de l'entité et de ses limites d'autorisations. Les stratégies basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces stratégies remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le IAM Guide de l'utilisateur.
- Stratégies de contrôle de service (SCP) – Les SCP sont des stratégies JSON qui spécifient le nombre maximal d'autorisations pour une organisation ou une unité d'organisation (OU) dans AWS Organizations. AWS Organizations est un service qui vous permet de regrouper et de gérer de façon centralisée plusieurs comptes AWS détenus par votre entreprise. Si vous activez toutes les fonctions d'une organisation, vous pouvez appliquer les stratégies de contrôle de service (SCP) à l'un ou à l'ensemble de vos comptes. La politique de contrôle des services limite les autorisations pour les entités dans les comptes membres, y compris dans chaque Utilisateur racine d'un compte AWS. Pour plus d'informations sur les Organisations et les SCP, consultez Fonctionnement des stratégies de contrôle de service dans le Manuel de l'utilisateur AWS Organizations.
- Stratégies de session – Les stratégies de session sont des stratégies avancées que vous transmettez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de la session obtenue sont une combinaison des stratégies basées sur l'identité de l'utilisateur ou du rôle et des stratégies de session. Les autorisations peuvent également provenir d'une stratégie basée sur les ressources. Un refus explicite dans l'une de ces stratégies remplace l'autorisation. Pour plus d'informations, consultez Stratégies de session dans le IAM Guide de l'utilisateur.

Plusieurs types de stratégie

Lorsque plusieurs types de stratégies s'appliquent à la requête, les autorisations obtenues sont plus compliquées à comprendre. Pour découvrir la façon dont AWS détermine s'il convient d'autoriser une requête en présence de plusieurs types de stratégies, consultez Logique d'évaluation de stratégies dans le IAM Guide de l'utilisateur.

Pour plus d'informations sur la gestion des identités et des accès pour Amazon RDS, continuez vers les pages suivantes :

- Comment Amazon RDS fonctionne avec IAM (p. 1540)
- Résolution des problèmes liés à Identity and Access Amazon RDS (p. 1581)

Comment Amazon RDS fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Amazon RDS, vous devez comprendre quelles sont les fonctions IAM disponibles à utiliser avec Amazon RDS. Pour obtenir une vue globale de la façon dont Amazon RDS et d'autres services AWS fonctionnent avec IAM, veuillez consulter les services AWS qui fonctionnent avec IAM dans le IAM Guide de l'utilisateur.

Rubriques

- Stratégies basées sur l'identité Amazon RDS (p. 1541)

- Stratégies basées sur les ressources Amazon RDS (p. 1543)
- Autorisation basée sur les balises Amazon RDS (p. 1543)
- Amazon RDS Rôles IAM (p. 1543)

Stratégies basées sur l'identité Amazon RDS

Avec les stratégies basées sur une identité IAM, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Amazon RDS prend en charge des actions, ressources et clés de condition spécifiques. Pour en savoir plus sur tous les éléments que vous utilisez dans une stratégie JSON, veuillez consulter Références des éléments de stratégie JSON IAM dans le IAM Guide de l'utilisateur.

Actions

L'élément `Action` d'une stratégie basée sur une identité IAM décrit les actions spécifiques qui seront autorisées ou refusées par la stratégie. Les actions de stratégie possèdent généralement le même nom que l'opération d'API AWS associée. L'action est utilisée dans une stratégie pour permettre d'effectuer l'opération associée.

Les actions de stratégie dans Amazon RDS utilisent le préfixe suivant avant l'action : `rds:`.
Par exemple, pour accorder à une personne l'autorisation de décrire les instances de base de données à l'aide de l'opération d'API Amazon RDS`DescribeDBInstances` , vous incluez l'action `rds:DescribeDBInstances` dans sa stratégie. Les déclarations de stratégie doivent inclure un élément `Action` ou `NotAction`. Amazon RDS définit son propre ensemble d'actions qui décrivent les tâches que vous pouvez effectuer avec ce service.

Pour spécifier plusieurs actions dans une seule déclaration, séparez-les par des virgules comme suit :

```
"Action": [
      "rds:action1",
      "rds:action2"
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Describe`, incluez l'action suivante :

```
"Action": "rds:Describe*"
```

Pour afficher la liste des actions Amazon RDS, veuillez consulter Actions définies par Amazon RDS dans le IAM Guide de l'utilisateur.

Ressources

L'élément `Resource` spécifie les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Vous spécifiez une ressource à l'aide d'un ARN ou du caractère générique (*) pour indiquer que l'instruction s'applique à toutes les ressources.

La ressource d'instance de base de données possède l'ARN suivant :

```
arn:${Partition}:rds:${Region}:${Account}:{ResourceType}/${Resource}
```

(Pour plus d'informations sur le format des ARN, consultez Noms ARN (Amazon Resource Name) et espaces de noms du service AWS.

Par exemple, pour spécifier l'instance de base de données `dbtest` dans votre instruction, utilisez l'ARN suivant :

```
"Resource": "arn:aws:rds:us-west-2:123456789012:db:dbtest"
```

Pour spécifier toues les instances qui appartiennent à un compte spécifique, utilisez le caractère générique (*) :

```
"Resource": "arn:aws:rds:us-east-1:123456789012:db:*"
```

Certaines opérations d'API RDS, telles que la création de ressources, ne peuvent pas être exécutées sur une ressource spécifique. Dans ces cas-là, vous devez utiliser le caractère générique (*).

```
"Resource": "*"
```

De nombreuses opérations d'API Amazon RDS nécessitent plusieurs ressources. Par exemple, `CreateDBInstance` crée une instance de base de données. Vous pouvez spécifier qu'un utilisateur IAM doit utiliser un groupe de sécurité spécifique et un groupe de paramètres lors de la création d'une instance de base de données. Pour spécifier plusieurs ressources dans une seule instruction, séparez leurs ARN par des virgules.

```
"Resource": [
      "resource1",
      "resource2"
```

Pour voir la liste des types de ressources Amazon RDS et de leurs ARN, consultez Ressources définies par Amazon RDS dans le IAM Guide de l'utilisateur. Pour en savoir plus sur les actions avec lesquelles vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par Amazon RDS.

Clés de condition

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, comme égal ou inférieur, pour faire correspondre la condition de la stratégie aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une opération `OR` logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM . Pour de plus amples informations, veuillez consulter Éléments des stratégies IAM : variables et balises dans le Guide de l'utilisateur IAM.

Amazon RDS définit son propre ensemble de clés de condition et prend également en charge l'utilisation des clés de condition globales. Pour voir toutes les clés de condition globales AWS, veuillez consulter Clés de contexte de condition globales AWS dans le IAM Guide de l'utilisateur.

Toutes les opérations d'API RDS prennent en charge la clé de condition `aws:RequestedRegion`.

Pour afficher la liste des clés de conditions Amazon RDS, consultez Clés de condition pour Amazon RDS dans le IAM Guide de l'utilisateur. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par Amazon RDS.

Exemples

Pour voir des exemples de stratégies Amazon RDS basées sur l'identité, consultez Exemples de stratégies basées sur l'identité Amazon RDS (p. 1544).

Stratégies basées sur les ressources Amazon RDS

Amazon RDS ne prend pas en charge les stratégies basées sur les ressource.

Autorisation basée sur les balises Amazon RDS

Vous pouvez attacher des balises aux ressources de Amazon RDS, ou transmettre des balises dans une demande à Amazon RDS. Pour contrôler l'accès basé sur des balises, vous devez fournir les informations de balises dans l'élément de condition d'une stratégie utilisant les clés de condition `rds:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`. Pour plus d'informations sur le balisage des ressources Amazon RDS, consultez Spécification de conditions : Utilisation de balises personnalisées (p. 1551).

Pour visualiser un exemple de stratégie basée sur l'identité permettant de limiter l'accès à une ressource en fonction des balises de cette ressource, consultez Accorder une autorisation pour des actions sur une ressource à l'aide d'une balise spécifique avec deux valeurs différentes (p. 1548).

Amazon RDS Rôles IAM

Un rôle IAM est une entité au sein de votre compteAWS qui dispose d'autorisations spécifiques.

Utilisation des informations d'identification temporaires avec Amazon RDS

Vous pouvez utiliser des informations d'identification temporaires pour vous connecter avec la fédération, assumer un rôle IAM, ou encore pour assumer un rôle entre comptes. Vous obtenez des informations d'identification de sécurité temporaires en appelant des opérations d'API AWS STS comme AssumeRole ou GetFederationToken.

Amazon RDS prend en charge l'utilisation des informations d'identification temporaires.

Rôles liés à un service

Les rôles liés à un service permettent aux services AWS d'accéder à des ressources dans d'autres services pour effectuer une action en votre nom. Les rôles liés à un service apparaissent dans la liste Rôles d'IAM Management Console et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier les autorisations concernant les rôles liés à un service.

Amazon RDS prend en charge les rôles liés à un service. Pour plus d'informations sur la création ou la gestion des rôles liés à un service Amazon RDS, consultez Utilisation des rôles liés à un service pour Amazon RDS (p. 1606).

Rôles de service

Cette fonction permet à un service d'endosser un rôle de service en votre nom. Ce rôle autorise le service à accéder à des ressources d'autres services pour effectuer une action en votre nom. Les rôles de service apparaissent dans la liste Rôles d'IAM Management Console et appartiennent à votre compte. Cela signifie qu'un administrateur IAM peut modifier les autorisations associées à ce rôle. Toutefois, une telle action peut perturber le bon fonctionnement du service.

Amazon RDS prend en charge les rôles de service.

Exemples de stratégies basées sur l'identité Amazon RDS

Par défaut, les utilisateurs et les rôles IAM ne sont pas autorisés à créer ou modifier les ressources Amazon RDS. Ils ne peuvent pas non plus exécuter des tâches à l'aide de AWS Management Console, AWS CLI ou de l'API AWS. Un administrateur IAM doit créer des stratégies IAM autorisant les utilisateurs et les rôles à exécuter des opérations d'API spécifiques sur les ressources spécifiées dont ils ont besoin. Il doit ensuite attacher ces stratégies aux utilisateurs ou aux groupes IAM ayant besoin de ces autorisations.

Pour apprendre à créer une stratégie basée sur l'identité IAM à l'aide de ces exemples de documents de stratégie JSON, veuillez consulter Création de stratégies dans l'onglet JSON dans le IAM Guide de l'utilisateur.

Rubriques

- Bonnes pratiques en matière de stratégies (p. 1544)
- Utilisation de la console Amazon RDS (p. 1545)
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations (p. 1545)
- Autoriser un utilisateur à créer des instances de base de données dans un compte AWS (p. 1546)
- Autorisations requises pour utiliser la console (p. 1547)
- Autoriser un utilisateur à effectuer une action Describe sur une ressource RDS (p. 1547)
- Autoriser un utilisateur à créer une instance de base de données qui utilise les groupes de sécurité et de paramètres de base de données spécifiés (p. 1548)
- Accorder une autorisation pour des actions sur une ressource à l'aide d'une balise spécifique avec deux valeurs différentes (p. 1548)
- Empêcher un utilisateur de supprimer une instance de base de données (p. 1549)
- Refuser tout accès à une ressource (p. 1549)
- Exemples de stratégies : Utilisation des clés de condition (p. 1549)
- Spécification de conditions : Utilisation de balises personnalisées (p. 1551)

Bonnes pratiques en matière de stratégies

Les stratégies basées sur l'identité sont très puissantes. Elles déterminent si une personne peut créer, consulter ou supprimer des ressources Amazon RDS dans votre compte. Ces actions peuvent entraîner des frais pour votre compte AWS. Lorsque vous créez ou modifiez des stratégies basées sur l'identité, suivez ces instructions et recommandations :

- Commencer à utiliser des stratégies gérées AWS – Pour commencer à utiliser Amazon RDS rapidement, utilisez les politiques gérées AWS pour accorder à vos employés les autorisations dont ils ont besoin. Ces stratégies sont déjà disponibles dans votre compte et sont gérées et mises à jour par AWS. Pour plus d'informations, consultez la section Mise en route avec les autorisations à l'aide des stratégies gérées AWS dans le IAM Guide de l'utilisateur.
- Accorder le privilège le plus faible – Lorsque vous créez des stratégies personnalisées, accordez uniquement les autorisations requises pour exécuter une seule tâche. Commencez avec un minimum d'autorisations et accordez-en d'autres si nécessaire. Cette méthode est plus sûre que de commencer avec des autorisations trop permissives et d'essayer de les restreindre plus tard. Pour plus d'informations, consultez Accorder les privilèges les plus faibles possible dans le IAM Guide de l'utilisateur.
- Activer MFA pour les opérations sensibles – Pour plus de sécurité, obligez les utilisateurs IAM à utiliser l'authentification multi-facteurs (MFA) pour accéder à des ressources ou à des opérations d'API sensibles. Pour plus d'informations, consultez Utilisation de Multi-Factor Authentication (MFA) dans AWS dans le IAM Guide de l'utilisateur.

- Utiliser des conditions de stratégie pour une plus grande sécurité – Tant que cela reste pratique pour vous, définissez les conditions dans lesquelles vos stratégies basées sur l'identité autorisent l'accès à une ressource. Par exemple, vous pouvez rédiger les conditions pour spécifier une plage d'adresses IP autorisées d'où peut provenir une demande. Vous pouvez également écrire des conditions pour autoriser les requêtes uniquement à une date ou dans une plage de temps spécifiée, ou pour imposer l'utilisation de SSL ou de MFA. Pour de plus amples informations, veuillez consulter Éléments de stratégie JSON IAM : condition dans le IAM Guide de l'utilisateur.

Utilisation de la console Amazon RDS

Pour accéder à la console Amazon RDS, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et visualiser les informations relatives aux ressources Amazon RDS de votre compte AWS. Vous pouvez créer une stratégie basée sur une identité qui soit plus restrictive que les autorisations minimales requises. Cependant, dans ce cas, la console ne fonctionne pas comme prévu pour les entités (rôles ou utilisateurs IAM) avec cette stratégie.

Pour garantir que ces entités pourront continuer à utiliser la console Amazon RDS, attachez également la stratégie gérée AWS suivante aux entités. Pour de plus amples informations, veuillez consulter Ajout d'autorisations à un utilisateur dans le IAM Guide de l'utilisateur.

```
AmazonRDSReadOnlyAccess
```

Vous n'avez pas besoin d'accorder les autorisations minimales de console aux utilisateurs qui effectuent des appels uniquement vers la AWS CLI ou l'API AWS. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API que vous tentez d'effectuer.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une stratégie qui permet aux utilisateurs IAM d'afficher les stratégies en ligne et gérées attachées à leur identité d'utilisateur. Cette stratégie inclut les autorisations nécessaires pour réaliser cette action sur la console ou par programmation à l'aide de l’AWS CLI ou de l'API AWS.

```
{
       "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": "*"
            }
        ]
    }
```

Autoriser un utilisateur à créer des instances de base de données dans un compte AWS

Voici un exemple de stratégie autorisant un utilisateur portant l'ID `123456789012` à créer des instances de base de données pour votre compte AWS. La stratégie exige que le nom de la nouvelle instance de base de données commence par `test`. La nouvelle instance de base de données doit également utiliser le moteur de base de données MySQL et la classe d'instance de base de données `db.t2.micro`. En outre, la nouvelle instance de base de données doit utiliser un groupe d'options et un groupe de paramètres de base de données commençant par `default`, et elle doit utiliser le groupe de sous-réseaux `default`.

```
{
    "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"
                }
            }
        }
    ]
}
```

La stratégie inclut une instruction unique spécifiant les autorisations suivantes pour l'utilisateur IAM :

- La stratégie autorise l'utilisateur IAM à créer une instance de base de données à l'aide de l'opération d'API CreateDBInstance (cela s'applique également à la commande create-db-instance de l'AWS CLI et de la AWS Management Console).
- L'élément `Resource` spécifie que l'utilisateur peut effectuer des actions sur et avec des ressources. Vous indiquez des ressources à l'aide d'un nom ARN (Amazon Resources Name). Ce nom ARN inclut le nom du service auquel appartient la ressource (`rds`), la région AWS (`*` indique une région dans cet exemple), le numéro de compte de l'utilisateur (`123456789012` est l'ID utilisateur dans cet exemple) ainsi que le type de ressource. Pour plus d'informations sur la création de noms ARN, consultez Utilisation des Amazon Resource Names (ARN) dans Amazon RDS (p. 298).

  L'élément `Resource` dans l'exemple spécifie les contraintes de stratégie suivantes sur les ressources de l'utilisateur :

  - L'identifiant d'instance de base de données de la nouvelle instance de base de données doit commencer par `test` (par exemple, `testCustomerData1`, `test-region2-data`).
  - Le groupe d'options de la nouvelle instance de base de données doit commencer par `default`.
  - Le groupe de paramètres de base de données de la nouvelle instance de base de données doit commencer par `default`.
  - Le groupe de sous-réseaux de la nouvelle instance de base de données doit être le groupe de sous-réseaux `default`.
- L'élément `Condition` indique que le moteur de base de données doit être MySQL et la classe d'instance de base de données doit être `db.t2.micro`. L'élément `Condition` indique les conditions lorsqu'une stratégie doit entrer en vigueur. Vous pouvez ajouter des autorisations ou des restrictions supplémentaires à l'aide de l'élément `Condition`. Pour plus d'informations sur la spécification de conditions, consultez Clés de condition (p. 1542). Cet exemple spécifie les conditions `rds:DatabaseEngine` et `rds:DatabaseClass`. Pour plus d'informations sur les valeurs de conditions valides pour `rds:DatabaseEngine`, consultez la liste en dessous du paramètre `Engine` dans CreateDBInstance. Pour de plus amples informations sur les valeurs de conditions valides pour `rds:DatabaseClass`, veuillez consulter Moteurs de base de données pris en charge pour les classes d'instance de base de données (p. 7) .

La stratégie ne spécifie pas l'élément `Principal` car, dans une stratégie basée sur une identité, vous ne spécifiez pas le mandataire qui obtient l'autorisation. Quand vous attachez une stratégie à un utilisateur, l'utilisateur est le mandataire implicite. Lorsque vous attachez une stratégie d'autorisation à un rôle IAM, le mandataire identifié dans la stratégie d'approbation de ce rôle obtient les autorisations.

Pour afficher la liste des actions Amazon RDS, veuillez consulter Actions définies par Amazon RDS dans le IAM Guide de l'utilisateur.

Autorisations requises pour utiliser la console

Pour qu'un utilisateur puisse utiliser la console, il doit avoir un ensemble minimal d'autorisations. Ces autorisations permettent à l'utilisateur de décrire les ressources Amazon RDS de leur compte AWS et de fournir d'autres informations associées, dont les informations relatives à la sécurité Amazon EC2 et au réseau.

Si vous créez une stratégie IAM plus restrictive que les autorisations minimales requises, la console ne fonctionne pas comme prévu pour les utilisateurs dotés de cette stratégie IAM. Pour garantir que ces utilisateurs puissent continuer à utiliser la console, attachez également la stratégie gérée `AmazonRDSReadOnlyAccess` à l'utilisateur, comme décrit dans Gestion de l'accès à l'aide de stratégies (p. 1539).

Vous n'avez pas besoin d'accorder les autorisations minimales de console pour les utilisateurs qui effectuent des appels uniquement à l'interface AWS CLI ou API Amazon RDS.

La stratégie suivante accorde l'accès total à toutes les ressources Amazon RDS pour le compte AWS racine :

```
AmazonRDSFullAccess
```

Autoriser un utilisateur à effectuer une action Describe sur une ressource RDS

La stratégie d'autorisation suivante accorde des autorisations à un utilisateur lui permettant d'exécuter toutes les actions commençant par `Describe`. Ces actions affichent des informations sur une ressource

RDS, telle qu'une instance de base de données. Le caractère générique (*) figurant dans l'élément `Resource` indique que les actions sont autorisées pour toutes les ressources Amazon RDS détenues par le compte.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowRDSDescribe",
         "Effect":"Allow",
         "Action":"rds:Describe*",
         "Resource":"*"
      }
   ]
}
```

Autoriser un utilisateur à créer une instance de base de données qui utilise les groupes de sécurité et de paramètres de base de données spécifiés

La stratégie d'autorisation suivante accorde des autorisations permettant à un utilisateur de créer uniquement une instance de base de données devant utiliser le groupe de paramètres DB `mysql-production` et le groupe de sécurité DB `db-production`.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowMySQLProductionCreate",
         "Effect":"Allow",
         "Action":"rds:CreateDBInstance",
         "Resource":[
            "arn:aws:rds:us-west-2:123456789012:pg:mysql-production",
            "arn:aws:rds:us-west-2:123456789012:secgrp:db-production"
         ]
      }
   ]
}
```

Accorder une autorisation pour des actions sur une ressource à l'aide d'une balise spécifique avec deux valeurs différentes

Vous pouvez utiliser des conditions dans votre stratégie basée sur l'identité pour contrôler l'accès aux ressources Amazon RDS en fonction des balises. La stratégie suivante accorde l'autorisation d'exécuter les API `ModifyDBInstance` et `CreateDBSnapshot` sur les instances de base de données avec la balise `stage` définie sur `development` ou sur `test`.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowDevTestCreate",
         "Effect":"Allow",
         "Action":[
            "rds:ModifyDBInstance",
            "rds:CreateDBSnapshot"
         ],
```

```
            "Resource":"*",
            "Condition":{
               "StringEquals":{
                  "rds:db-tag/stage":[
                     "development",
                     "test"
                  ]
               }
            }
         }
      ]
}
```

Empêcher un utilisateur de supprimer une instance de base de données

La stratégie d'autorisation suivante accorde des autorisations empêchant un utilisateur de supprimer une instance de base de données spécifique. Par exemple, il est possible de refuser la capacité à supprimer vos instances de base de données de production à un utilisateur quelconque qui n'est pas un administrateur.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyDelete1",
         "Effect":"Deny",
         "Action":"rds:DeleteDBInstance",
         "Resource":"arn:aws:rds:us-west-2:123456789012:db:my-mysql-instance"
      }
   ]
}
```

Refuser tout accès à une ressource

Vous pouvez refuser explicitement l'accès à une ressource. Les stratégies de refus ont priorité sur les stratégies d'autorisation. La stratégie suivante refuse explicitement à un utilisateur la possibilité de gérer une ressource :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "rds:*",
      "Resource": "arn:aws:rds:us-east-1:123456789012:db:mydb"
    }
  ]
}
```

Exemples de stratégies : Utilisation des clés de condition

Les exemples suivants montrent comment vous pouvez utiliser des clés de condition dans les stratégies d'autorisation IAM Amazon RDS.

Exemple 1 : Accorder l'autorisation de créer une instance de base de données qui utilise un moteur de base de données spécifique et n'utilise pas plusieurs zones de disponibilité

La stratégie suivante utilise une clé de condition RDS et autorise un utilisateur à créer seulement des instances de bases de données qui utilisent le moteur de base de données MySQL et n'utilisent pas plusieurs zones de disponibilité. L'élément `Condition` indique l'exigence que le moteur de base de données soit MySQL.

```
{

   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowMySQLCreate",
         "Effect":"Allow",
         "Action":"rds:CreateDBInstance",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "rds:DatabaseEngine":"mysql"
            },
            "Bool":{
                    "rds:MultiAz": false
            }
         }
      }
   ]
}
```

Exemple 2 : Refuser explicitement l'autorisation de créer des instances de bases de données pour certaines classes d'instance de base de données et de créer des instances de bases de données qui utilisent les IOPS provisionnées

La stratégie suivante refuse explicitement l'autorisation de créer des instances de bases de données qui utilisent les classes d'instance de base de données `r3.8xlarge` et `m4.10xlarge`, lesquelles représentent les classes d'instances de base de données les plus grandes et les plus onéreuses. Cette stratégie empêche également les utilisateurs de créer des instances de bases de données qui utilisent les IOPS provisionnées, ce qui génère un coût additionnel.

Le refus explicite d'une autorisation a priorité sur toutes les autres autorisations accordées. Cela garantit que des identités n'obtiendront pas par erreur une autorisation que vous ne souhaitez pas accorder.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyLargeCreate",
         "Effect":"Deny",
         "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"
            }
         }
      }
   ]
}
```

Exemple 3 : Limiter l'ensemble de clés et de valeurs de balise pouvant être utilisées pour baliser une ressource

La politique suivante utilise une clé de condition RDS et autorise l'ajout d'une balise avec la clé `stage` à une ressource avec les valeurs `test`, `qa` et `production`.

```
{

 {
    "Version" : "2012-10-17",
    "Statement" : [{
       "Effect" : "Allow",
       "Action" : [ "rds:AddTagsToResource", "rds:RemoveTagsFromResource"
       ],
       "Resource" : "*",
       "Condition" : { "streq" : { "rds:req-tag/stage" : [ "test", "qa",
       "production" ] } }
  }
 ]
}
}
```

Spécification de conditions : Utilisation de balises personnalisées

Amazon RDS prend en charge la spécification de conditions dans une stratégie IAM à l'aide de balises personnalisées.

Par exemple, supposons que vous ajoutiez une balise nommée `environment` à vos instances de base de données avec des valeurs telles que `beta`, `staging`, `production`, etc. Dans ce cas, vous pouvez créer une stratégie qui limite certains utilisateurs aux instances de base de données fondées sur la valeur de balise `environment`.

> **Note**
>
> Les identifiants des balises personnalisées sont sensibles à la casse.

Le tableau suivant répertorie les identifiants des balises RDS que vous pouvez utiliser dans un élément `Condition`.

Identifiant de balise RDS	S'applique à
`db-tag`	Instances de base de données, y compris les réplicas en lecture

Identifiant de balise RDS	S'applique à
`snapshot-tag`	Snapshots DB
`ri-tag`	Instances DB réservées
`secgrp-tag`	Groupes de sécurité DB
`og-tag`	Groupes d'options DB
`pg-tag`	Groupes de paramètres DB
`subgrp-tag`	Groupes de sous-réseaux DB
`es-tag`	Abonnements aux événements
`cluster-tag`	Clusters DB
`cluster-pg-tag`	Groupes de paramètres de cluster DB
`cluster-snapshot-tag`	Instantanés de cluster DB

La syntaxe d'une condition de balise personnalisée est la suivante :

```
"Condition":{"StringEquals":{"rds:rds-tag-identifier/tag-name": ["value"]} }
```

Par exemple, l'élément `Condition` suivant s'applique aux instances de bases de données avec une balise nommée `environment` et la valeur de balise `production`.

```
"Condition":{"StringEquals":{"rds:db-tag/environment": ["production"]} }
```

Pour plus d'informations sur la création de balises, consultez Balisage de ressources Amazon RDS (p. 293).

> **Important**
>
> Si vous gérez l'accès à vos ressources RDS à l'aide du balisage, nous vous recommandons de sécuriser l'accès aux balises pour vos ressources RDS. Vous pouvez gérer l'accès aux balises en créant des stratégies pour les actions `AddTagsToResource` et `RemoveTagsFromResource`. Par exemple, la stratégie suivante refuse aux utilisateurs la capacité à ajouter ou supprimer des balises pour toutes les ressources. Vous pouvez alors créer des stratégies pour autoriser des utilisateurs spécifiques à ajouter ou supprimer des balises.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyTagUpdates",
         "Effect":"Deny",
         "Action":[
            "rds:AddTagsToResource",
            "rds:RemoveTagsFromResource"
         ],
         "Resource":"*"
      }
   ]
}
```

Pour afficher la liste des actions Amazon RDS, veuillez consulter Actions définies par Amazon RDS dans le IAM Guide de l'utilisateur.

Exemples de stratégies : Utilisation de balises personnalisées

Les exemples suivants montrent comment vous pouvez utiliser des balises personnalisées dans les stratégies d'autorisation IAM Amazon RDS. Pour plus d'informations sur l'ajout de balises à une ressource Amazon RDS, consultez Utilisation des Amazon Resource Names (ARN) dans Amazon RDS (p. 298).

> **Note**
>
> Tous les exemples utilisent la région us-west-2 et contiennent des ID de compte fictifs.

Exemple 1 : Accorder une autorisation pour des actions sur une ressource à l'aide d'une balise spécifique avec deux valeurs différentes

La stratégie suivante accorde l'autorisation d'exécuter les API `ModifyDBInstance` et `CreateDBSnapshot` sur les instances de base de données avec la balise `stage` définie sur `development` ou sur `test`.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowDevTestCreate",
         "Effect":"Allow",
         "Action":[
            "rds:ModifyDBInstance",
            "rds:CreateDBSnapshot"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "rds:db-tag/stage":[
                  "development",
                  "test"
               ]
            }
         }
      }
   ]
}
```

Exemple 2 : Refuser explicitement l'autorisation de créer une instance de base de données qui utilise les groupes de paramètres DB spécifiés

La stratégie suivante refuse explicitement l'autorisation de créer une instance de base de données qui utilise les groupes de paramètres DB avec des valeurs de balise spécifiques. Vous pouvez appliquer cette stratégie si vous avez besoin qu'un groupe de paramètres DB créé par le client soit toujours utilisé lors de la création des instances de bases de données. Notez que les stratégies qui utilisent `Deny` sont le plus souvent utilisées pour limiter un accès accordé par une stratégie plus large.

Le refus explicite d'une autorisation a priorité sur toutes les autres autorisations accordées. Cela garantit que des identités n'obtiendront pas par erreur une autorisation que vous ne souhaitez pas accorder.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyProductionCreate",
         "Effect":"Deny",
         "Action":"rds:CreateDBInstance",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "rds:pg-tag/usage":"prod"
```

```
            }
         }
      }
   ]
}
```

Exemple 3 : Accorder une autorisation pour des actions sur une instance de base de données dont le nom d'instance a un nom d'utilisateur comme préfixe

La stratégie suivante accorde l'autorisation d'appeler une API quelconque (à l'exception de `AddTagsToResource` et de `RemoveTagsFromResource`) sur une instance de base de données dont le nom d'instance de base de données a comme préfixe le nom de l'utilisateur et a une balise nommée `stage` égale à `devo` ou qui n'a pas de balise nommée `stage`.

La ligne `Resource` dans la stratégie identifie une ressource par son Amazon Resource Name (ARN). Pour plus d'informations sur l'utilisation des noms ARN avec les ressources Amazon RDS, consultez Utilisation des Amazon Resource Names (ARN) dans Amazon RDS (p. 298).

```
{
   "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"
            }
         }
      }
   ]
}
```

Authentification de base de données IAM pour MySQL et PostgreSQL

Vous pouvez vous authentifier auprès du de votre instance de base de données à l'aide de l'authentification de base de données AWS Identity and Access Management (IAM). L'authentification de base de données IAM fonctionne avec MySQL et PostgreSQL. Grâce à cette méthode d'authentification, vous n'avez plus besoin de mot de passe pour vous connecter au d'une instance de base de données. En revanche, un jeton d'authentification est nécessaire.

Un jeton d'authentification est une chaîne de caractères unique générée par Amazon RDS sur demande. Les jetons d'authentification sont générés au moyen d'AWS Signature Version 4. Chaque jeton a une durée de vie de 15 minutes. Il n'est pas nécessaire de stocker des informations d'identification utilisateur dans la base de données, car l'authentification est gérée de manière externe avec IAM. Vous pouvez aussi toujours utiliser l'authentification de base de données standard.

L'authentification de base de données IAM offre les avantages suivants :

- Le trafic réseau à destination et en provenance de la base de données est chiffré à l'aide de Secure Socket Layer (SSL) ou de Transport Layer Security (TLS). Pour de plus amples informations sur l'utilisation de SSL/TLS avec Amazon RDS, veuillez consulter Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).

- Vous pouvez utiliser IAM pour gérer de façon centralisée l'accès à vos ressources de base de données, au lieu de gérer l'accès de manière individuelle sur chaque instance ou de bases de données.
- Pour les applications exécutées sur Amazon EC2, vous pouvez utiliser des informations d'identification spécifiques à votre instance EC2 pou accéder à la base de données, ce qui garantit une meilleure sécurité qu'un mot de passe.

Rubriques

- Disponibilité de l'authentification de base de données IAM (p. 1555)
- Limites de l'authentification de base de données IAM (p. 1555)
- Recommandations MySQL pour l'authentification de base de données IAM (p. 1555)
- Activation et désactivation de l'authentification de base de données IAM (p. 1556)
- Création et utilisation d'une stratégie IAM pour l'accès à une base de données IAM (p. 1558)
- Création d'un compte de base de données à l'aide de l'authentification IAM (p. 1561)
- Connexion à votre instance de base de données à l'aide de l'authentification IAM. (p. 1562)

Disponibilité de l'authentification de base de données IAM

L'authentification de base de données IAM est disponible pour les moteurs de bases de données suivants :

- MySQL 8.0, version mineure 8.0.16 ou supérieure.
- MySQL 5.7, version mineure 5.7.16 ou ultérieure
- MySQL 5.6, version mineure 5.6.34 ou ultérieure
- PostgreSQL 12, toutes les versions mineures
- PostgreSQL 11, toutes les versions mineures
- Pour PostgreSQL 10, version mineure 10.6 ou ultérieure
- Pour PostgreSQL 9.6, version mineure 9.6.11 ou ultérieure
- Pour PostgreSQL 9.5, version mineure 9.5.15 ou ultérieure

Limites de l'authentification de base de données IAM

Les limitations suivantes s'appliquent lors de l'utilisation de l'authentification de base de données IAM :

- Le nombre maximal de connexions par seconde à votre d'instances de base de données peut être limité en fonction de sa classe d'instance de base de données et de votre charge de travail.
- Actuellement, l'authentification de base de données IAM ne prend pas en charge les clés de contexte de condition globale.

  Pour de plus amples informations sur les clés de contexte de condition globale, veuillez consulter Clés de contexte de condition globale AWS dans le Manuel de l'utilisateur IAM.
- Actuellement, l'authentification de base de données IAM n'est pas prise en charge pour les CName.

Recommandations MySQL pour l'authentification de base de données IAM

Nous recommandons les pratiques suivantes lors de l'utilisation du moteur MySQL de base de données :

- Utilisez l'authentification de base de données IAM comme mécanisme pour l'accès personnel temporaire aux bases de données.

- Utilisez l'authentification de base de données IAM pour les charges de travail pouvant facilement être relancées uniquement.
- Utilisez l'authentification de base de données IAM si votre application exige moins de 200 nouvelles connexions d'authentification de base de données IAM par seconde.

  Les moteurs de base de données qui fonctionnent avec Amazon RDS n'imposent pas de limites de tentatives d'authentification par seconde. Néanmoins, lorsque vous utilisez l'authentification de base de données IAM, votre application doit générer un jeton d'authentification. Votre application emploie ensuite ce jeton pour la connexion au de l'instance de base de données. Si vous dépassez la limite maximale de nouvelles connexions par seconde, le traitement supplémentaire d'authentification de base de données IAM peut entraîner une limitation de la connexion. Il peut même provoquer l'abandon de connexions existantes. Pour de plus amples informations sur le nombre total maximal de connexions pour MySQL, veuillez consulter Maximum de connexions MySQL et MariaDB (p. 1646).

Activation et désactivation de l'authentification de base de données IAM

Par défaut, l'authentification de base de données IAM est désactivée sur les instances et de bases de données. Vous pouvez activer l'authentification de base de données IAM à l'aide d'AWS Management Console, de l'AWS CLI ou de l'API.

Vous pouvez activer l'authentification de base de données IAM lorsque vous effectuez une des actions suivantes :

- Pour créer une nouvelle instance de base de données avec l'authentification de base de données IAM activée, veuillez consulter Création d'une instance de base de données Amazon RDS (p. 146).
- Pour modifier une instance de base de données afin d'activer l'authentification de base de données IAM, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).
- Pour restaurer une instance de base de données à partir d'un instantané avec l'authentification de base de données IAM activée, veuillez consulter Restauration à partir d'un instantané de base de données (p. 329).
- Pour restaurer une instance de base de données à un instant dans le passé avec l'authentification de base de données IAM activée, veuillez consulter Restauration d'une instance de base de données à une date spécifiée (p. 365).

L'authentification IAM pour les des instances de base de données PostgreSQL nécessite que la valeur SSL soit égale à 1. Vous ne pouvez pas activer l'authentification IAM pour une instance de base de données PostgreSQL si la valeur SSL est égale à 0. Vous ne pouvez pas modifier et définir la valeur SSL sur 0 si l'authentification IAM est activée pour une instance de base de données PostgreSQL.

Console

Chaque flux de travail de création ou de modification comporte une section Authentification de base de données dans laquelle vous pouvez activer ou désactiver l'authentification de base de données IAM. Dans cette section, choisissez Authentification de base de données par mot de passe et IAM pour activer l'authentification de base de données IAM.

Pour activer ou désactiver l'authentification de base de données IAM pour une instance de base de données

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez instance de base de données que vous souhaitez modifier.

> **Note**
>
> Assurez-vous que l'instance de base de données est compatible avec l'authentification IAM. Consultez les exigences de compatibilité présentées dans Disponibilité de l'authentification de base de données IAM (p. 1555).

4. Sélectionnez Modify.
5. Dans la section Authentification de base de données, choisissez Authentification de base de données par mot de passe et IAM pour activer l'authentification de base de données IAM, ou choisissez une autre option pour la désactiver.
6. Choisissez Continue.
7. Pour appliquer immédiatement les modifications, choisissez Immédiatement dans la section Planification des modifications.
8. Choisissez Modifier l'instance de base de données ou .

AWS CLI

Pour créer une nouvelle instance de base de données avec authentification IAM par l'intermédiaire de l'AWS CLI, utilisez la commande `create-db-instance` Spécifiez l'option `--enable-iam-database-authentication`, comme indiqué dans l'exemple suivant.

```
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
```

Pour mettre à jour une instance de bases de données existante de manière à activer ou non l'authentification IAM, utilisez la commande de l'AWS CLI `modify-db-instance`. Spécifiez l'option `--enable-iam-database-authentication` ou `--no-enable-iam-database-authentication`, selon le cas.

> **Note**
>
> Assurez-vous que l'instance de base de données est compatible avec l'authentification IAM. Consultez les exigences de compatibilité présentées dans Disponibilité de l'authentification de base de données IAM (p. 1555).

Par défaut, Amazon RDS procède à la modification pendant la fenêtre de maintenance suivante. Si vous souhaitez ignorer ceci et activer l'authentification de bases de données IAM dès que possible, utilisez le paramètre `--apply-immediately`.

L'exemple suivant montre comment activer immédiatement l'authentification IAM pour une instance de base de données existante.

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --apply-immediately \
    --enable-iam-database-authentication
```

Si vous restaurez un ou une instance de base de données, utilisez l'une des commandes AWS CLI suivantes :

- `restore-db-instance-to-point-in-time`
- `restore-db-instance-from-db-snapshot`

Le paramètre d'authentification de base de données IAM par défaut est celui de l'instantané source. Pour le modifier, spécifiez l'option `--enable-iam-database-authentication` ou `--no-enable-iam-database-authentication`, selon le cas.

API RDS

Pour créer une nouvelle instance de base de données avec authentification IAM par l'intermédiaire de l'API, utilisez l'opération d'API `CreateDBInstance`. Définissez le paramètre `EnableIAMDatabaseAuthentication` sur `true`.

Pour mettre à jour une instance de base de données existante de manière à activer l'authentification IAM, utilisez l'opération d'API `ModifyDBInstance`. Définissez le paramètre `EnableIAMDatabaseAuthentication` sur `true` pour activer l'authentification IAM ou sur `false` pour la désactiver.

> **Note**
>
> Assurez-vous que l'instance de base de données est compatible avec l'authentification IAM. Consultez les exigences de compatibilité présentées dans Disponibilité de l'authentification de base de données IAM (p. 1555).

Si vous restaurez un ou une instance de base de données, utilisez l'une des opérations d'API suivantes :

- `RestoreDBInstanceFromDBSnapshot`
- `RestoreDBInstanceToPointInTime`

Le paramètre d'authentification de base de données IAM par défaut est celui de l'instantané source. Pour modifier ce paramètre, définissez le paramètre `EnableIAMDatabaseAuthentication` sur `true` pour activer l'authentification IAM ou sur `false` pour la désactiver.

Création et utilisation d'une stratégie IAM pour l'accès à une base de données IAM

Pour autoriser un utilisateur ou un rôle IAM à se connecter à votre instance ou de base de données, vous devez créer une stratégie IAM. Il suffit ensuite de lier cette stratégie à un rôle ou à un utilisateur IAM.

> **Note**
>
> Pour en savoir plus sur les stratégies IAM, consultez Identity and Access Management dans Amazon RDS (p. 1536).

L'exemple de stratégie suivant autorise l'utilisateur IAM à se connecter au d'une instance de base de données à l'aide de l'authentification de base de données IAM.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
             "rds-db:connect"
         ],
         "Resource": [
             "arn:aws:rds-db:us-east-2:1234567890:dbuser:db-ABCDEFGHIJKL01234/db_user"
         ]
      }
   ]
}
```

> **Important**
>
> Un utilisateur administrateur IAM peut accéder aux instances et aux de base de données sans autorisations explicites dans une stratégie IAM. L'exemple dans Création d'un utilisateur IAM (p. 62) crée un utilisateur administrateur IAM. Si vous souhaitez restreindre l'accès de l'administrateur aux instances et aux de base de données, vous pouvez créer un rôle IAM avec les autorisations appropriées accordant moins de privilèges, puis les assigner à l'administrateur.
>
> **Note**
>
> Ne confondez pas le préfixe `rds-db:` avec d'autres préfixes d'opération d'API RDS; qui commencent par `rds:`. Vous utilisez le préfixe `rds-db:` et l'action `rds-db:connect` uniquement pour l'authentification de base de données IAM. Ils ne sont valides que dans ce contexte.
> Actuellement, la console IAM affiche une erreur pour les stratégies avec l'action `rds-db:connect`. Vous pouvez ignorer cette erreur.

L'exemple de stratégie inclut une instruction unique avec les éléments suivants :

- `Effect` – Spécifiez `Allow` pour octroyer l'accès à l'instance de base de données. Si vous n'autorisez pas explicitement l'accès, celui-ci est refusé par défaut.
- `Action` – Spécifiez `rds-db:connect` pour autoriser les connexions à l'instance de base de données.
- `Resource` – Spécifiez un ARN (Amazon Resource Name) qui décrit un compte de base de données dans une instance de base de données. Le format de l'ARN est le suivant.

```
arn:aws:rds-db:region:account-id:dbuser:DbiResourceId/db-user-name
```

Dans ce format, remplacez les variables suivantes :

- *`region`* correspond à la région AWS pour l'instance de base de données. Dans l'exemple de stratégie, la région AWS est `us-east-2`.
- *`account-id`* correspond au numéro de compte AWS pour l'instance de base de données. Dans l'exemple de stratégie, le numéro de compte est `1234567890`.
- *`DbiResourceId`* correspond à l'identifiant de l'instance de base de données. Cet identifiant est propre à une région AWS et ne change jamais. Dans cet exemple de stratégie, l'identifiant est `db-ABCDEFGHIJKL01234`.

  Pour trouver un identifiant de ressource de d'instance de base de données dans AWS Management Console pour Amazon RDS, choisissez le d'instance de base de données pour en afficher les détails. Choisissez ensuite l'onglet Configuration. L'ID de ressource est indiqué dans la section Configuration.

  Il est également possible d'utiliser la commande AWS CLI pour répertorier les identifiants et les ID de ressource pour la totalité du de votre instance de base de données de la région AWS actuelle, comme illustré ci-dessous.

```
aws rds describe-db-instances --query "DBInstances[*].
[DBInstanceIdentifier,DbiResourceId]"
```

> **Note**
>
> Si vous vous connectez à une base de données via le proxy RDS, spécifiez l'ID de ressource de proxy, par exemple `prx-ABCDEFGHIJKL01234`. Pour plus d'informations sur l'utilisation

de l'authentification de base de données IAM avec le proxy RDS, consultez Connexion à un proxy à l'aide de l'authentification IAM (p. 186).

- *db-user-name* correspond au nom du compte de base de données à associer à l'authentification IAM. Dans cet exemple de stratégie, le compte de la base de données est `db_user`.

Vous pouvez construire d'autres ARN pour prendre en charge différents modèles d'accès. La stratégie suivante permet d'accéder à deux comptes de base de données différents dans une instance de base de données.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
             "rds-db:connect"
         ],
         "Resource": [
             "arn:aws:rds-db:us-east-2:123456789012:dbuser:db-ABCDEFGHIJKL01234/jane_doe",
             "arn:aws:rds-db:us-east-2:123456789012:dbuser:db-ABCDEFGHIJKL01234/mary_roe"
         ]
      }
   ]
}
```

La stratégie suivante utilise le caractère « * » pour faire correspondre l'ensemble des instances de base de données et l'ensemble des comptes de base de données pour un compte AWS et une région AWS spécifiques.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "rds-db:connect"
            ],
            "Resource": [
                "arn:aws:rds-db:us-east-2:1234567890:dbuser:*/*"
            ]
        }
    ]
}
```

La stratégie suivante met en correspondance l'ensemble des instances de base de données pour un compte AWS et une région AWS spécifiques. Néanmoins, cette stratégie n'octroie l'accès qu'aux instances et de bases de données qui ont un compte de base de données `jane_doe`.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
             "rds-db:connect"
```

```
            ],
            "Resource": [
                "arn:aws:rds-db:us-east-2:123456789012:dbuser:*/jane_doe"
            ]
        }
    ]
}
```

L'utilisateur ou le rôle IAM a uniquement accès aux bases de données auxquelles l'utilisateur de base de données a accès. Supposons par exemple que votre instance de base de donnés possède une base de données nommée dev et une autre base de données nommée test. Si l'utilisateur de base de données `jane_doe` a uniquement accès à dev, tous les rôles ou utilisateurs IAM qui accèdent à cette instance de bases de données avec l'utilisateur `jane_doe` ont aussi uniquement accès à dev. Cette restriction d'accès s'applique également aux autres objets de bases de données, tels que les tables, les vues, etc.

Un administrateur IAM doit créer des stratégies IAM autorisant les utilisateurs et les rôles à exécuter des opérations d'API spécifiques sur les ressources spécifiées dont ils ont besoin. Il doit ensuite attacher ces stratégies aux utilisateurs ou aux groupes IAM ayant besoin de ces autorisations. Pour obtenir des exemples de stratégies, consultez la section Exemples de stratégies basées sur l'identité Amazon RDS (p. 1544).

Attachement d'une stratégie IAM à un rôle ou à un utilisateur IAM

Après avoir créé une stratégie IAM pour permettre l'authentification de base de données, il convient d'attacher la stratégie à un rôle ou à un utilisateur IAM. Pour accéder à un didacticiel sur ce sujet, veuillez consulter Créer et attacher votre première stratégie gérée par le client dans le Guide de l'utilisateur IAM.

Tandis que vous parcourez ce didacticiel, vous pouvez utiliser un exemple de stratégie illustré dans cette section comme point de départ afin de le personnaliser en fonction de vos besoins. À la fin de ce didacticiel, vous obtenez un utilisateur IAM avec une stratégie attachée qui peut utiliser l'action `rds-db:connect`.

> **Note**
>
> Vous pouvez mapper plusieurs utilisateurs ou rôles IAM au même compte d'utilisateur de base de données. Supposons par exemple que votre stratégie IAM a spécifié l'ARN de ressource suivant.
>
> ```
> arn:aws:rds-db:us-east-2:123456789012:dbuser:db-12ABC34DEFG5HIJ6KLMNOP78QR/jane_doe
> ```
>
> Si vous attachez la stratégie aux utilisateurs IAM Jane, Bob et Diego, chacun de ces utilisateurs peut alors se connecter à l'instance de base de données spécifié(e) par l'intermédiaire du compte de base de données `jane_doe`.

Création d'un compte de base de données à l'aide de l'authentification IAM

Avec l'authentification de base de données IAM, vous n'avez pas besoin d'associer de mots de passe de base de données aux comptes d'utilisateurs que vous créez. Si vous supprimez un utilisateur IAM qui est mappé à un compte de base de données, vous devez également supprimer le compte de base de données avec l'instruction `DROP USER`.

Utilisation de l'authentification IAM avec PostgreSQL

Pour utiliser l'authentification IAM avec PostgreSQL, connectez-vous à l'instance de base de données, créez des utilisateurs de base de données, puis accordez-leur le rôle `rds_iam`, comme indiqué dans l'exemple suivant.

```
CREATE USER db_userx;
GRANT rds_iam TO db_userx;
```

Utilisation de l'authentification IAM avec MySQL

Avec MySQL, l'authentification est gérée par `AWSAuthenticationPlugin`, un plug-in fourni par AWS qui agit de manière transparente avec IAM pour authentifier vos utilisateurs IAM. Connectez-vous à l'instance de base de données et exécutez l'instruction `CREATE USER`, comme indiqué dans l'exemple suivant.

```
CREATE USER jane_doe IDENTIFIED WITH AWSAuthenticationPlugin AS 'RDS';
```

La clause `IDENTIFIED WITH` permet à MySQL d'utiliser le `AWSAuthenticationPlugin` pour authentifier le compte de base de données (`jane_doe`). La clause `AS 'RDS'` fait référence à la méthode d'authentification, et le compte de base de données spécifié doit avoir le même nom que l'utilisateur ou le rôle IAM. Dans cet exemple, le compte de base de données et l'utilisateur ou le rôle IAM se nomment `jane_doe`.

> **Note**
>
> Si vous voyez le message suivant, cela signifie que le plug-in fourni par AWS n'est pas disponible pour l'instance de base de données.
> `ERROR 1524 (HY000): Plugin 'AWSAuthenticationPlugin' is not loaded`
> Pour remédier à cette erreur, vérifiez si vous utilisez une configuration prise en charge et si vous avez activé l'authentification de base de données IAM sur votre instance de base de données. Pour plus d'informations, consultez Disponibilité de l'authentification de base de données IAM (p. 1555) et Activation et désactivation de l'authentification de base de données IAM (p. 1556).

Après avoir créé un compte à l'aide de `AWSAuthenticationPlugin`, vous pouvez le gérer de la même manière que les autres comptes de base de données. Vous pouvez par exemple modifier les privilèges de compte avec `GRANT` et `REVOKE`, ou changer divers attributs de compte avec l'instruction `ALTER USER`.

Connexion à votre instance de base de données à l'aide de l'authentification IAM.

Avec l'authentification de base de données IAM, vous utilisez un jeton d'identification lors de la connexion à votre instance de base de données. Un jeton d'authentification constitue une chaîne de caractères unique qui remplace un mot de passe. Après avoir été créé, un jeton d'authentification est valable pendant 15 minutes avant d'expirer. Si vous tentez de vous connecter alors que le jeton expiré, la demande de connexion est rejetée.

Chaque jeton d'authentification doit être accompagné d'une signature valide, en utilisant AWS Signature Version 4. (Pour plus d'informations, consultez Processus de signature Signature Version 4 dans le document AWS General Reference.) L'AWS CLI et un kit SDK AWS, comme le AWS SDK for Java ou Kit SDK AWS pour Python (Boto3) peuvent automatiquement signer chaque jeton que vous créez.

Vous pouvez utiliser un jeton d'authentification lorsque vous vous connectez à Amazon RDS pour un autre service AWS, comme AWS Lambda. L'utilisation d'un jeton vous évite d'avoir à placer un mot de passe dans votre code. Vous pouvez aussi utiliser un kit SDK AWS pour créer et signer un jeton d'authentification par programmation.

Après avoir obtenu un jeton d'authentification IAM signé, vous pouvez vous connecter à une instance de base de données Amazon RDS. Utilisez les liens ci-dessous pour savoir comment procéder avec un outil de ligne de commande ou un kit SDK AWS, comme le AWS SDK for Java ou Kit SDK AWS pour Python (Boto3).

Pour plus d'informations, consultez les billets de blog suivants :

- Utiliser l'authentification IAM pour se connecter avec SQL Workbench/J à Amazon Aurora MySQL ou Amazon RDS for MySQL.
- Utilisation de l'authentification IAM pour se connecter à PgAdmin Amazon Aurora PostgreSQL ou Amazon RDS for PostgreSQL

Les conditions préalables à la connexion à votre instance de base de données à l'aide de l'authentification IAM sont les suivantes :

- Activation et désactivation de l'authentification de base de données IAM (p. 1556)
- Création et utilisation d'une stratégie IAM pour l'accès à une base de données IAM (p. 1558)
- Création d'un compte de base de données à l'aide de l'authentification IAM (p. 1561)

Rubriques

- Connexion à votre cluster de base de données à l'aide de l'authentification IAM à partir de la ligne de commande : AWS CLI et MySQL Client (p. 1563)
- Connexion à votre cluster de base de données à l'aide de l'authentification IAM à partir de la ligne de commande : AWS CLI et client psql (p. 1565)
- Connexion à votre d'instances de base de données à l'aide de l'authentification IAM et de Kit AWS SDK pour .NET (p. 1566)
- Connexion à votre d'instances de base de données à l'aide de l'authentification IAM et de Kit SDK AWS pour Go (p. 1568)
- Connexion à votre d'instances de base de données à l'aide de l'authentification IAM et de AWS SDK for Java (p. 1571)
- Connexion à votre d'instances de base de données à l'aide de l'authentification IAM et de Kit SDK AWS pour Python (Boto3) (p. 1579)

Connexion à votre cluster de base de données à l'aide de l'authentification IAM à partir de la ligne de commande : AWS CLI et MySQL Client

À partir de la ligne de commande, vous pouvez vous connecter à une instance de base de données Amazon RDS ou à un avec l'AWS CLI et l'outil de ligne de commande `mysql` en suivant les instructions des liens suivants.

Les conditions préalables à la connexion à votre instance de base de données à l'aide de l'authentification IAM sont les suivantes :

- Activation et désactivation de l'authentification de base de données IAM (p. 1556)
- Création et utilisation d'une stratégie IAM pour l'accès à une base de données IAM (p. 1558)
- Création d'un compte de base de données à l'aide de l'authentification IAM (p. 1561)

Rubriques

- Création d'un jeton d'authentification IAM (p. 1563)
- Connexion à votre instance de base de données (p. 1564)

Création d'un jeton d'authentification IAM

L'exemple suivant illustre comment obtenir un jeton d'identification signé à l'aide d'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
```

Dans cet exemple, les paramètres sont les suivants :

- `--hostname` – Le nom d'hôte de l'instance de base de données auquel vous souhaitez accéder.
- `--port` – Le numéro du port utilisé lors de la connexion au d'instances de base de données.
- `--region` – La région AWS où le d'instances de base de données s'exécute.
- `--username` – Le compte de base de données auquel vous souhaitez accéder.

Les premiers caractères du jeton ressemblent à l'exemple suivant.

```
rdsmysql.123456789012.us-west-2.rds.amazonaws.com:3306/?Action=connect&DBUser=jane_doe&X-
Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Expires=900...
```

Connexion à votre instance de base de données

Le format général de connexion est illustré ci-dessous.

```
mysql --host=hostName --port=portNumber --ssl-ca=[full path]rds-combined-ca-bundle.pem --
enable-cleartext-plugin --user=userName --password=authToken
```

Les paramètres sont les suivants :

- `--host` – Le nom d'hôte de l'instance de base de données auquel vous souhaitez accéder.
- `--port` – Le numéro du port utilisé lors de la connexion au d'instances de base de données.
- `--ssl-ca` – Le fichier de certificat SSL contenant la clé publique.

  Pour plus d'informations, consultez Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).
- `--enable-cleartext-plugin` – Une valeur qui spécifie que `AWSAuthenticationPlugin` doit être utilisé pour cette connexion.
- `--user` – Le compte de base de données auquel vous souhaitez accéder.
- `--password` – Un jeton d'authentification IAM signé.

Le jeton d'authentification est composé de plusieurs centaines de caractères. Il peut être encombrant sur la ligne de commande. Pour contourner ce problème, vous pouvez enregistrer le jeton dans une variable d'environnement, puis utiliser cette variable pour la connexion. L'exemple suivant illustre une manière de contourner ce problème.

```
RDSHOST="rdsmysql.123456789012.us-west-2.rds.amazonaws.com"
TOKEN="$(aws rds generate-db-auth-token --hostname $RDSHOST --port 3306 --region us-west-2
 --username jane_doe )"

mysql --host=$RDSHOST --port=3306 --ssl-ca=/sample_dir/rds-combined-ca-bundle.pem --enable-
cleartext-plugin --user=jane_doe --password=$TOKEN
```

Lorsque vous vous connectez avec `AWSAuthenticationPlugin`, la connexion est sécurisée par SSL. Pour le vérifier, tapez la commande suivante à l'invite de commande `mysql>`.

```
show status like 'Ssl%';
```

Les lignes suivantes de l'affichage obtenu fournissent plus de détails.

```
+---------------+-------------+
| Variable_name | Value

                                                                  |
+---------------+-------------+
| ...           | ...
| Ssl_cipher    | AES256-SHA

                                                                  |
| ...           | ...
| Ssl_version   | TLSv1.1

                                                                  |
| ...           | ...
+-----------------------------+
```

Connexion à votre cluster de base de données à l'aide de l'authentification IAM à partir de la ligne de commande : AWS CLI et client psql

À partir de la ligne de commande, vous pouvez vous connecter à Amazon RDS pour une instance de base de données PostgreSQL avec l'AWS CLI et l'outil de ligne de commande psql comme décrit ci-après.

Les conditions préalables à la connexion à votre instance de base de données à l'aide de l'authentification IAM sont les suivantes :

- Activation et désactivation de l'authentification de base de données IAM (p. 1556)
- Création et utilisation d'une stratégie IAM pour l'accès à une base de données IAM (p. 1558)
- Création d'un compte de base de données à l'aide de l'authentification IAM (p. 1561)

Rubriques

- Création d'un jeton d'authentification IAM (p. 1565)
- Connexion à une instance PostgreSQL Amazon RDS (p. 1566)

Création d'un jeton d'authentification IAM

Le jeton d'authentification se compose de plusieurs centaines de caractères ; il peut donc être complexe à manipuler sur la ligne de commande. Pour contourner ce problème, vous pouvez enregistrer le jeton dans une variable d'environnement, puis utiliser cette variable pour la connexion. L'exemple de code suivant montre comment utiliser l'AWS CLI pour obtenir un jeton d'authentification signé à l'aide de la commande `generated-db-auth-token` et le stocker dans une variable d'environnement `PGPASSWORD`.

```
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 )"
```

Dans cet exemple, les paramètres de la commande `generate-db-auth-token` sont les suivants :

- `--hostname` – Nom d'hôte de l'instance de base de données auquel vous souhaitez accéder.
- `--port` – Le numéro du port utilisé lors de la connexion au d'instances de base de données.
- `--region` – La région AWS où le d'instances de base de données s'exécute.
- `--username` – Le compte de base de données auquel vous souhaitez accéder.

Les premiers caractères du jeton généré ressemblent à l'exemple suivant.

```
rdspostgres.123456789012.us-west-2.rds.amazonaws.com:5432/?
Action=connect&DBUser=jane_doe&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Expires=900...
```

Connexion à une instance PostgreSQL Amazon RDS

Le format général pour utiliser psql pour la connexion est illustré ci-dessous.

```
psql "host=hostName port=portNumber sslmode=verify-full sslrootcert=certificateFile
 dbname=DBName user=userName password=authToken"
```

Les paramètres sont les suivants :

- `host` – Nom d'hôte de l'instance de base de données auquel vous souhaitez accéder.
- `port` – Le numéro du port utilisé lors de la connexion au d'instances de base de données.
- `sslmode` – Le mode SSL à utiliser.

  Lorsque vous utilisez `sslmode=verify-full`, la connexion SSL vérifie le point de terminaison de l'instance de base de données par rapport au point de terminaison dans le certificat SSL.
- `sslrootcert` – Le fichier de certificat SSL contenant la clé publique.

  Pour plus d'informations, consultez la section Utilisation de SSL avec une instance de base de données PostgreSQL.
- `dbname` – La base de données à laquelle vous souhaitez accéder.
- `user` – Le compte de base de données auquel vous souhaitez accéder.
- `password` – Un jeton d'authentification IAM signé.

L'exemple suivant montre l'utilisation de psql pour se connecter. Dans l'exemple, psql utilise la variable d'environnement `PGPASSWORD` définie lors de la génération du jeton dans la section précédente.

```
psql "host=$RDSHOST port=5432 sslmode=verify-full sslrootcert=/sample_dir/rds-combined-ca-
bundle.pem dbname=DBName user=jane_doe password=$PGPASSWORD"
```

Connexion à votre d'instances de base de données à l'aide de l'authentification IAM et de Kit AWS SDK pour .NET

Vous pouvez vous connecter à une instance de base de données Amazon RDS MySQL ou PostgreSQL avec Kit AWS SDK pour .NET comme décrit ci-après.

Les conditions préalables à la connexion à votre instance de base de données à l'aide de l'authentification IAM sont les suivantes :

- Activation et désactivation de l'authentification de base de données IAM (p. 1556)
- Création et utilisation d'une stratégie IAM pour l'accès à une base de données IAM (p. 1558)
- Création d'un compte de base de données à l'aide de l'authentification IAM (p. 1561)

L'exemple de code suivant montre comment créer un jeton d'authentification, puis l'utiliser pour se connecter à un d'instances de base de données.

Pour exécuter cet exemple de code, vous avez besoin de Kit AWS SDK pour .NET, disponible sur le site AWS. Les paquets `AWSSDK.CORE` et `AWSSDK.RDS` sont requis. Pour vous connecter à une instance de

base de données, utilisez le connecteur de base de données .NET pour le moteur de base de données, tel que MySQLConnector pour MySQL ou Npgsql pour PostgreSQL.

Modifiez la valeur des variables suivantes selon les besoins :

- `server` – Le point de terminaison du d'instances de base de données auquel vous souhaitez accéder.
- `port` – Le numéro du port utilisé lors de la connexion au d'instances de base de données.
- `user` – Le compte de base de données auquel vous souhaitez accéder.

Ce code se connecte à une instance de base de données MySQL.

```
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.RDSAuthTokenGenerator.GenerateAuthToken(RegionEndpoint.USEast1,
 "mysqldb.123456789012.us-east-1.rds.amazonaws.com", 3306, "jane_doe");
      // for debug only Console.Write("{0}\n", pwd);  //this verifies the token is
 generated

      MySqlConnection conn = new MySqlConnection("server=mysqldb.123456789012.us-
east-1.rds.amazonaws.com;user=jane_doe;database=mydB;port=3306;password={pwd};SslMode=Required;SslCa=..
rds-ca-2019-root.pem");
      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();
    }
  }
}
```

Ce code se connecte à une instance de base de données PostgreSQL.

```
using System;
using Npgsql;
using Amazon.RDS.Util;

namespace ConsoleApp1
{
    class Program
    {
        static void Main(string[] args)
```

```
        {
            var pwd =
 RDSAuthTokenGenerator.GenerateAuthToken("postgresqldb.123456789012.us-
east-1.rds.amazonaws.com", 5432, "jane_doe");
// for debug only Console.Write("{0}\n", pwd);  //this verifies the token is generated

            NpgsqlConnection conn = new
 NpgsqlConnection($"Server=postgresqldb.123456789012.us-east-1.rds.amazonaws.com;User
 Id=jane_doe;Password={pwd};Database=mydb;SSL Mode=Require;Trust Server
 Certificate=true;");
            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.Write("{0}\n", dr[0]);

            // Close connection
            conn.Close();
        }
    }
}
```

Connexion à votre d'instances de base de données à l'aide de l'authentification IAM et de Kit SDK AWS pour Go

À partir de la ligne de commande, vous pouvez vous connecter à une instance de base de données Amazon RDS MySQL ou PostgreSQL avec Kit SDK AWS pour Go comme décrit ci-après.

Les conditions préalables à la connexion à votre instance de base de données à l'aide de l'authentification IAM sont les suivantes :

- Activation et désactivation de l'authentification de base de données IAM (p. 1556)
- Création et utilisation d'une stratégie IAM pour l'accès à une base de données IAM (p. 1558)
- Création d'un compte de base de données à l'aide de l'authentification IAM (p. 1561)

Pour exécuter cet exemple de code, vous avez besoin de Kit SDK AWS pour Go, disponible sur le site AWS.

Modifiez la valeur des variables suivantes selon les besoins :

- `dbName` – La base de données à laquelle vous souhaitez accéder.
- `dbUser` – Le compte de base de données auquel vous souhaitez accéder.
- `dbHost` – Le point de terminaison du d'instances de base de données auquel vous souhaitez accéder.
- `dbPort` – Le numéro du port utilisé lors de la connexion au d'instances de base de données.
- `region` – La région AWS où le d'instances de base de données s'exécute.

En outre, assurez-vous que les bibliothèques importées dans l'exemple de code existent sur votre système.

Rubriques

- Création d'un jeton d'authentification IAM (p. 1569)
- Connexion à votre instance de base de données (p. 1570)

Création d'un jeton d'authentification IAM

Vous pouvez utiliser le package `rdsutils` pour générer des jetons utilisés pour vous connecter à und'instances de base de données. Appelez la fonction `BuildAuthToken` pour générer un jeton. Fournissez le point de terminaison d'instance de base de données, la région AWS, le nom d'utilisateur et les informations d'identification IAM pour générer le jeton pour la connexion à un d'instances de bases de données avec les informations d'identification IAM.

L'exemple suivant montre comment utiliser `BuildAuthToken` pour créer un jeton d'authentification pour la connexion à une instance de base de données MySQL.

```
package main

import (
    "database/sql"
    "fmt"
    "log"

    "github.com/aws/aws-sdk-go/aws/credentials"
    "github.com/aws/aws-sdk-go/service/rds/rdsutils"
)

func main() {
    dbName := "app"
    dbUser := "jane_doe"
    dbHost := "mydb.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 {
        log.Fatalf("failed to build auth token %v", err)
    }
}
```

L'exemple suivant montre comment utiliser `BuildAuthToken` pour créer un jeton d'authentification pour la connexion à une instance de base de données PostgreSQL.

```
package main

import (
    "database/sql"
    "fmt"
    "log"

    "github.com/aws/aws-sdk-go/aws/credentials"
    "github.com/aws/aws-sdk-go/service/rds/rdsutils"
)

func main() {
    dbName := "app"
    dbUser := "jane_doe"
    dbHost := "mydb.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 {
        log.Fatalf("failed to build auth token %v", err)
```

```
    }
}
```

Connexion à votre instance de base de données

L'exemple de code suivant montre comment créer un jeton d'authentification, puis l'utiliser pour se connecter à un d'instances de base de données.

Ce code se connecte à une instance de base de données MySQL.

```
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 := "mydb.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)
    }
}
```

Ce code se connecte à une instance de base de données PostgreSQL.

```
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 := "mydb.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)
    }
}
```

Connexion à votre d'instances de base de données à l'aide de l'authentification IAM et de AWS SDK for Java

Vous pouvez vous connecter à une instance de base de données Amazon RDS MySQL ou PostgreSQL avec AWS SDK for Java comme décrit ci-après.

Les conditions préalables à la connexion à votre instance de base de données à l'aide de l'authentification IAM sont les suivantes :

- Activation et désactivation de l'authentification de base de données IAM (p. 1556)
- Création et utilisation d'une stratégie IAM pour l'accès à une base de données IAM (p. 1558)
- Création d'un compte de base de données à l'aide de l'authentification IAM (p. 1561)

Rubriques

- Création d'un jeton d'authentification IAM (p. 1571)
- Construction manuelle d'un jeton d'authentification IAM (p. 1572)
- Connexion à votre instance de base de données (p. 1575)

Création d'un jeton d'authentification IAM

Si vous écrivez des programmes à l'aide de AWS SDK for Java, vous pouvez obtenir un jeton d'authentification signé au moyen de la classe `RdsIamAuthTokenGenerator`. L'usage de cette classe exige que vous fournissiez les informations d'identification AWS. Pour ce faire, vous devez créer une instance de la classe `DefaultAWSCredentialsProviderChain`. `DefaultAWSCredentialsProviderChain` utilise la première clé d'accès AWS et la clé secrète trouvée dans la chaîne de fournisseur d'informations d'identification par défaut. Pour de plus amples informations sur les clés d'accès AWS, veuillez consulter Gestion des clés d'accès pour les utilisateurs IAM.

Après avoir créé une instance de `RdsIamAuthTokenGenerator`, vous pouvez appeler la méthode `getAuthToken` pour obtenir un jeton signé. Fournissez la région AWS, le nom d'hôte, le numéro de port et le nom d'utilisateur. L'exemple de code suivant montre comment procéder.

```
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;
    }

}
```

Construction manuelle d'un jeton d'authentification IAM

Dans Java, la manière la plus facile de créer un jeton d'authentification est d'utiliser `RdsIamAuthTokenGenerator`. Cette classe créé un jeton d'authentification pour vous, puis le signe à l'aide d'AWS Signature Version 4. Pour de plus amples informations, veuillez consulter Processus de signature Signature Version 4 dans le AWS General Reference.

Vous pouvez néanmoins aussi construire et signer un jeton d'authentification manuellement, comme indiqué dans l'exemple de code suivant.

```
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 CreateRDSAuthTokenManually {
    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 dateTime
 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' + dateTime + '\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) throws SdkClientException {
        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) throws SdkClientException {
        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);
        }
    }
}
```

Connexion à votre instance de base de données

L'exemple de code suivant montre comment créer un jeton d'authentification, puis l'utiliser pour se connecter à une instance exécutant MySQL.

Pour exécuter cet exemple de code, vous avez besoin d'AWS SDK for Java, disponible sur le site AWS. En outre, vous avez besoin des éléments suivants :

- MySQL Connector/J. Cet exemple de code a été testé avec `mysql-connector-java-5.1.33-bin.jar`.
- Certificat intermédiaire pour Amazon RDS qui est spécifique à une région AWS. (Pour plus d'informations, consultez Utilisation de SSL/TLS pour chiffrer une connexion à une instance de base de données (p. 1525).) À l'exécution, le chargeur de classe recherche le certificat dans le même annuaire que celui de cet exemple de code Java, afin de pouvoir le trouver.
- Modifiez la valeur des variables suivantes selon les besoins :
  - `RDS_INSTANCE_HOSTNAME` – Le nom d'hôte de l'instance de base de données auquel vous souhaitez accéder.
  - `RDS_INSTANCE_PORT` – Numéro du port utilisé lors de la connexion à votre instance de base de données PostgreSQL.
  - `REGION_NAME` – La région AWS où le cluster de base de données s'exécute.
  - `DB_USER` – Le compte de base de données auquel vous souhaitez accéder.
  - `SSL_CERTIFICATE` – Un certificat SSL pour Amazon RDS qui est spécifique à une région AWS.

Pour télécharger un certificat pour votre région AWS, consultez Certificats intermédiaires (p. 1526). Placez le certificat SSL dans le même annuaire que ce fichier de programme Java, afin que le chargeur de classe puisse le trouver à l'exécution.

Cet exemple de code obtient les informations d'identification AWS à partir de la chaîne de fournisseur d'informations d'identification par défaut.

```
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=AKIAPFXHGVDI5RNFO4AQ%2F20171003%2Fcn-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");
    }

}
```

Connexion à votre d'instances de base de données à l'aide de l'authentification IAM et de Kit SDK AWS pour Python (Boto3)

Vous pouvez vous connecter à une instance de base de données Amazon RDS MySQL ou PostgreSQL avec Kit SDK AWS pour Python (Boto3) comme décrit ci-après.

Les conditions préalables à la connexion à votre instance de base de données à l'aide de l'authentification IAM sont les suivantes :

- Activation et désactivation de l'authentification de base de données IAM (p. 1556)
- Création et utilisation d'une stratégie IAM pour l'accès à une base de données IAM (p. 1558)
- Création d'un compte de base de données à l'aide de l'authentification IAM (p. 1561)

En outre, assurez-vous que les bibliothèques importées dans l'exemple de code existent sur votre système.

Les exemples de code utilisent des profils pour les informations d'identification partagées. Pour de plus amples informations sur les informations d'identification spécifiant, veuillez consulter Informations d'identification dans la documentation Kit SDK AWS pour Python (Boto3).

Rubriques

- Création d'un jeton d'authentification IAM (p. 1579)
- Connexion à votre instance de base de données (p. 1570)

Création d'un jeton d'authentification IAM

Vous pouvez appeler la méthode `generate_db_auth_token` pour obtenir un jeton signé. Fournissez le point de terminaison du d'instance de base de données, le port, le nom d'utilisateur, la région AWS et le moteur de base de données pour générer le jeton pour la connexion à un d'instance de base de données avec des informations d'identification IAM.

Ce code génère un jeton d'authentification IAM pour une instance de base de données MySQL.

```
import sys
import boto3

ENDPOINT="mysqldb.123456789012.us-east-1.rds.amazonaws.com"
PORT="3306"
USR="jane_doe"
REGION="us-east-1"
os.environ['LIBMYSQL_ENABLE_CLEARTEXT_PLUGIN'] = '1'

#gets the credentials from .aws/credentials
session = boto3.Session(profile_name='RDSCreds')
client = boto3.client('rds')

token = client.generate_db_auth_token(DBHostname=ENDPOINT, Port=PORT, DBUsername=USR,
 Region=REGION)
```

Ce code génère un jeton d'authentification IAM pour une instance de base de données PostgreSQL.

```
import sys
import boto3

ENDPOINT="postgresmydb.123456789012.us-east-1.rds.amazonaws.com"
PORT="5432"
```

```
USR="jane_doe"
REGION="us-east-1"

#gets the credentials from .aws/credentials
session = boto3.Session(profile_name='RDSCreds')
client = boto3.client('rds')

token = client.generate_db_auth_token(DBHostname=ENDPOINT, Port=PORT, DBUsername=USR,
 Region=REGION)
```

Connexion à votre instance de base de données

L'exemple de code suivant montre comment créer un jeton d'authentification, puis l'utiliser pour se connecter à un d'instances de base de données.

Pour exécuter cet exemple de code, vous avez besoin de Kit SDK AWS pour Python (Boto3), disponible sur le site AWS.

Modifiez la valeur des variables suivantes selon les besoins :

- `ENDPOINT` – Le point de terminaison du d'instances de base de données auquel vous souhaitez accéder.
- `PORT` – Le numéro du port utilisé lors de la connexion au d'instances de base de données.
- `USER` – Le compte de base de données auquel vous souhaitez accéder.
- `REGION` – La région AWS où le d'instances de base de données s'exécute.
- `DBNAME` – La base de données à laquelle vous souhaitez accéder.

Ce code se connecte à une instance de base de données MySQL.

```
import mysql.connector
import sys
import boto3
import os

ENDPOINT="mysqldb.123456789012.us-east-1.rds.amazonaws.com"
PORT="3306"
USR="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 = boto3.client('rds')

token = client.generate_db_auth_token(DBHostname=ENDPOINT, Port=PORT, DBUsername=USR,
 Region=REGION)

try:
    conn =  mysql.connector.connect(host=ENDPOINT, user=USR, passwd=token, port=PORT,
 database=DBNAME)
    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))
```

Ce code se connecte à une instance de base de données PostgreSQL.

```
import psycopg2
import sys
import boto3

ENDPOINT="postgresmydb.123456789012.us-east-1.rds.amazonaws.com"
PORT="5432"
USR="jane_doe"
REGION="us-east-1"
DBNAME="mydb"

#gets the credentials from .aws/credentials
session = boto3.Session(profile_name='RDSCreds')
client = boto3.client('rds')

token = client.generate_db_auth_token(DBHostname=ENDPOINT, Port=PORT, DBUsername=USR,
 Region=REGION)

try:
    conn = psycopg2.connect(host=ENDPOINT, port=PORT, database=DBNAME, user=USR,
 password=token)
    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))
```

Résolution des problèmes liés à Identity and Access Amazon RDS

Utilisez les informations suivantes pour identifier et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Amazon RDS et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Amazon RDS (p. 1581)
- Je ne suis pas autorisé à exécuter iam:PassRole (p. 1582)
- Je veux afficher mes clés d'accès (p. 1582)
- Je suis un administrateur et je veux autoriser d'autres utilisateurs à accéder à Amazon RDS (p. 1582)
- Je veux permettre à des personnes extérieures à mon compte AWS d'accéder à mes ressources Amazon RDS (p. 1583)

Je ne suis pas autorisé à effectuer une action dans Amazon RDS

Si AWS Management Console indique que vous n'êtes pas autorisé à exécuter une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni votre nom d'utilisateur et votre mot de passe.

L'exemple d'erreur suivant se produit lorsque l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées concernant un *`widget`* mais ne dispose pas d'autorisations `rds:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 rds:GetWidget on resource: my-example-widget
```

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses stratégies pour lui permettre d'accéder à la ressource `my-example-widget` à l'aide de l'action `rds:GetWidget`.

Je ne suis pas autorisé à exécuter iam:PassRole

Si vous recevez un message d'erreur selon lequel vous n'êtes pas autorisé à exécuter l'action `iam:PassRole`, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni votre nom d'utilisateur et votre mot de passe. Demandez à cette personne de mettre à jour vos stratégies pour vous permettre de transmettre un rôle à Amazon RDS.

Certains services AWS vous permettent de transmettre un rôle existant à ce service, au lieu de créer un nouveau rôle de service ou rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour exécuter une action dans Amazon RDS. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

Dans ce cas, Mary demande à son administrateur de mettre à jour ses stratégies pour lui permettre d'exécuter l'action `iam:PassRole`.

Je veux afficher mes clés d'accès

Une fois que vous avez créé vos clés d'accès IAM, vous pouvez afficher votre ID de clé d'accès à tout moment. Toutefois, vous ne pouvez pas afficher à nouveau votre clé d'accès secrète. Si vous perdez votre clé d'accès secrète, vous devez créer une nouvelle paire de clés.

Les clés d'accès se composent de deux parties : un ID de clé d'accès (par exemple, `AKIAIOSFODNN7EXAMPLE`) et une clé d'accès secrète (par exemple, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). À l'instar d'un nom d'utilisateur et un mot de passe, vous devez utiliser à la fois l'ID de clé d'accès et la clé d'accès secrète pour authentifier vos demandes. Gérez vos clés d'accès de manière aussi sécurisée que votre nom d'utilisateur et votre mot de passe.

> **Important**
>
> Ne communiquez pas vos clés d'accès à un tiers, même pour qu'il vous aide à trouver votre ID utilisateur canonique. En effet, vous lui accorderiez ainsi un accès permanent à votre compte.

Lorsque vous créez une paire de clé d'accès, enregistrez l'ID de clé d'accès et la clé d'accès secrète dans un emplacement sécurisé. La clé d'accès secrète est accessible uniquement au moment de sa création. Si vous perdez votre clé d'accès secrète, vous devez ajouter de nouvelles clés d'accès pour votre utilisateur IAM. Vous pouvez avoir un maximum de deux clés d'accès. Si vous en avez déjà deux, vous devez supprimer une paire de clés avant d'en créer une nouvelle. Pour obtenir plus d'informations, consultez Gestion des clés d'accès dans le IAM Guide de l'utilisateur.

Je suis un administrateur et je veux autoriser d'autres utilisateurs à accéder à Amazon RDS

Pour permettre à d'autres utilisateurs d'accéder à Amazon RDS, vous devez créer une entité IAM (utilisateur ou rôle) pour la personne ou l'application qui a besoin de l'accès. Ils utiliseront les informations d'identification de cette entité pour accéder à AWS. Vous devez ensuite associer une stratégie à l'entité qui leur accorde les autorisations appropriées dans Amazon RDS.

Pour démarrer immédiatement, consultez Création de votre premier groupe et utilisateur délégué IAM dans le IAM Guide de l'utilisateur.

Je veux permettre à des personnes extérieures à mon compte AWS d'accéder à mes ressources Amazon RDS

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation peuvent utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est approuvé pour assumer le rôle. Pour les services qui prennent en charge les stratégies basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces stratégies pour accorder aux personnes l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Amazon RDS prend en charge ces fonctionnalités, consultez Comment Amazon RDS fonctionne avec IAM (p. 1540).
- Pour savoir comment fournir un accès à vos ressources sur les comptes AWS que vous détenez, consultez Octroi à un utilisateur IAM de l'autorisation d'accès à un autre compte AWS vous appartenant dans le IAM Guide de l'utilisateur.
- Pour savoir comment fournir l'accès à vos ressources à des comptes AWS tiers, consultez Octroi d'un accès à des comptes AWS appartenant à des tiers dans le IAM Guide de l'utilisateur.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Octroi d'accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le IAM Guide de l'utilisateur.
- Pour en savoir plus sur la différence entre l'utilisation des rôles et des stratégies basées sur les ressources pour l'accès entre comptes, consultez Différence entre les rôles IAM et les stratégies basées sur les ressources dans le IAM Guide de l'utilisateur.

Journalisation et surveillance dans Amazon RDS

La surveillance est un enjeu important pour assurer la fiabilité, la disponibilité et les performances d'Amazon RDS et de vos solutions AWS. Vous devez recueillir les données de surveillance de toutes les parties de votre solution AWS de manière à pouvoir déboguer plus facilement une éventuelle défaillance à plusieurs points. AWS fournit plusieurs outils pour surveiller vos ressources Amazon RDS et répondre aux incidents potentiels :

Alarmes Amazon CloudWatch

À l'aide d'alarmes Amazon CloudWatch, vous surveillez une métrique unique sur une période donnée que vous spécifiez. Si la métrique dépasse un seuil donné, une notification est envoyée à une rubrique Amazon SNS ou à une stratégie AWS Auto Scaling. Les alarmes CloudWatch n'appellent pas d'actions parce qu'elles sont à un état particulier. L'état doit avoir changé et avoir été conservé pendant un nombre de périodes spécifié. Pour plus d'informations, consultez Surveillance avec Amazon CloudWatch (p. 376).

Journaux AWS CloudTrail

CloudTrail fournit un enregistrement des actions réalisées par un utilisateur, un rôle ou un service AWS dans Amazon RDS. CloudTrail capture tous les appels d'API pour Amazon RDS sous la forme d'événements, y compris des appels depuis la console et depuis des appels de code aux opérations d'API Amazon RDS. Les informations collectées par CloudTrail, vous permettent de déterminer quelle demande a été envoyée à Amazon RDS, l'adresse IP source à partir de laquelle la demande a été effectuée, qui a effectué la demande, quand, ainsi que d'autres informations. Pour plus d'informations, consultez Utilisation de AWS CloudTrail et Amazon RDS (p. 526).

Surveillance améliorée

Amazon RDS fournit des métriques en temps réel pour le système d'exploitation sur lequel votre instance de base de données s'exécute. Vous pouvez afficher les métriques pour votre instance de

base de données à l'aide de la console, ou utiliser la sortie JSON de surveillance améliorée d'Amazon CloudWatch Logs dans le système de surveillance de votre choix. Pour plus d'informations, consultez Surveillance améliorée (p. 394).

Amazon RDS Performance Insights

Performance Insights complète les fonctions de surveillance existantes sur Amazon RDS. Ce service illustre les performances de votre base de données et facilite votre analyse des problèmes qui les impactent. Grâce au tableau de bord de Performance Insights, vous pouvez visualiser la charge de la base de données et la filtrer par attentes, instructions SQL, hôtes ou utilisateurs. Pour plus d'informations, consultez Utilisation d'Amazon RDS Performance Insights (p. 410).

Journaux de base de données

Vous pouvez afficher, télécharger et consulter les journaux de base de données à l'aide d'AWS Management Console, de l'AWS CLI ou de l'API RDS. Pour plus d'informations, consultez Amazon RDS Fichiers journaux de base de données (p. 490).

Recommandations Amazon RDS

Amazon RDS fournit des recommandations automatisées pour les ressources de base de données. Ces recommandations offrent des conseils quand aux bonnes pratiques en analysant la configuration de l'instance de base de données, son utilisation et les données relatives à ses performances. Pour plus d'informations, consultez Utilisation des recommandations Amazon RDS (p. 389).

Notification d'événement Amazon RDS

Amazon RDS utilise Amazon Simple Notification Service (Amazon SNS) pour fournir une notification lorsqu'un événement Amazon RDS se produit. Ces notifications peuvent être sous l'une des formes prises en charge par Amazon SNS pour une région AWS, telles qu'un e-mail, un SMS ou un appel à un point de terminaison HTTP. Pour plus d'informations, consultez Utilisation de la notification d'événement Amazon RDS (p. 467).

AWS Trusted Advisor

Trusted Advisor tire profit des bonnes pratiques acquises à travers la satisfaction de centaines de milliers de clients AWS. Trusted Advisor examine votre environnement AWS, puis effectue des recommandations lorsqu'il est possible de faire des économies, d'améliorer la disponibilité et les performances du système, ou de remédier à des failles de sécurité. Tous les clients AWS ont accès à cinq contrôles Trusted Advisor. Les clients avec un plan de support Business ou Enterprise peuvent afficher tous les contrôles Trusted Advisor.

Trusted Advisor dispose des contrôles de sécurité liés à Amazon RDS-suivants :

- Instances de base de données Amazon RDS inactives
- Risque lié à l'accès aux groupes de sécurité Amazon RDS
- Sauvegardes Amazon RDS
- Multi-AZ Amazon RDS

Pour plus d'informations sur ces vérifications, consultez Bonnes pratiques Trusted Advisor (Checks).

Pour plus d'informations sur la surveillance Amazon RDS, consultez Surveillance d'une instance de base de données Amazon RDS (p. 373).

Validation de la conformité pour Amazon RDS

Les auditeurs tiers évaluent la sécurité et la conformité de Amazon RDS dans le cadre de plusieurs programmes de conformité AWS. Il s'agit notamment des certifications SOC, PCI, FedRAMP, HIPAA et autres.

Pour obtenir la liste des services AWS dans le cadre de programmes de conformité spécifiques, consultez Services AWS concernés par le programme de conformité. Pour obtenir des informations générales, veuillez consulter Programmes de conformité AWS.

Vous pouvez télécharger les rapports de l'audit externe avec AWS Artifact. Pour de plus amples informations, veuillez consulter Téléchargement des rapports dans AWS Artifact.

Votre responsabilité de conformité lors de l'utilisation de Amazon RDS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre organisation, ainsi que par la législation et la réglementation applicables. AWS fournit les ressources suivantes pour faciliter la conformité :

- Guides de démarrage rapide de la sécurité et de la conformité – Ces guides de déploiement proposent des considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de référence centrés sur la sécurité et la conformité dans AWS.
- Livre blanc sur l'architecture pour la sécurité et la conformité HIPAA – Le livre blanc décrit comment les entreprises peuvent utiliser AWS pour créer des applications conformes à la loi HIPAA.
- Ressources de conformité AWS – Cet ensemble de manuels et de guides peut s'appliquer à votre secteur et à votre emplacement.
- AWS Config – Ce service AWS permet d'évaluer comment les configurations de vos ressources se conforment aux pratiques internes, aux normes et aux directives industrielles.
- AWS Security Hub – Ce service AWS fournit une vue complète de votre état de sécurité au sein de AWS qui vous permet de vérifier votre conformité aux normes du secteur et aux bonnes pratiques de sécurité.

Résilience dans Amazon RDS

L'infrastructure mondiale d'AWS repose sur les régions et les zones de disponibilité AWS. Les régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour de plus amples informations sur les régions et les zones de disponibilité AWS, veuillez consulter Infrastructure mondiale AWS.

Outre l’infrastructure globale d'AWS, Amazon RDS propose différentes fonctionnalités qui contribuent à la prise en charge des vos besoins en matière de résilience et de sauvegarde de données.

Sauvegarde et restauration

Amazon RDS crée et enregistre les sauvegardes automatisées de votre instance de base de données. Amazon RDS crée un instantané de volume de stockage de votre instance de base de données, sauvegardant ainsi la totalité de l'instance de base de données, et pas seulement les bases de données individuelles.

Amazon RDS crée des sauvegardes automatisées de votre instance de base de données lors du créneau de sauvegarde de votre instance de base de données. Amazon RDS enregistre des sauvegardes automatisées de votre instance de base de données selon la période de rétention des sauvegardes que vous avez spécifié. Le cas échéant, vous pouvez récupérer votre base de données à tout moment pendant la période de rétention des sauvegardes. Vous pouvez également sauvegarder votre instance de base de données manuellement, en créant manuellement un instantané de bases de données.

Vous pouvez créer une instance de base de données en restaurant à partir de cet instantané de base de données comme solution de récupération après sinistre si l'instance de base de données source échoue.

Pour de plus amples informations, veuillez consulter Sauvegarde et restauration d'une instance de base de données Amazon RDS (p. 317).

Réplication

Amazon RDS utilise aussi la fonctionnalité de réplication intégrée des moteurs de base de données PostgreSQL, MySQL et MariaDB pour créer un type particulier d'instance de base de données appelé réplica en lecture à partir d'une instance de base de données source. Les mises à jour apportées à l'instance de base de données source sont copiées de façon asynchrone sur le réplica en lecture. Vous pouvez réduire la charge sur votre instance de base de données source en acheminant les requêtes en lecture depuis vos applications vers le réplica en lecture. Les réplicas en lecture permettent une montée en puissance basée sur Elastic au-delà des contraintes de capacité d'une seule instance de base de données dans le cas de charges de travail de base de données à lecture intensive. Vous pouvez effectuez la promotion d'un réplica en lecture en instance autonome comme plan de reprise après sinistre en cas de défaillance de l'instance de base de données. Pour certains moteurs de base de données, Amazon RDS prend aussi en charge d'autres options de réplication.

Pour plus d'informations, consultez Utilisation des réplicas en lecture (p. 275).

Basculement

Amazon RDS fournit une haute disponibilité et la prise en charge du basculement pour les instances de base de données utilisant les déploiements multi-AZ. Amazon RDS utilise plusieurs technologies différentes pour fournir une prise en charge du basculement. Les déploiements multi-AZ pour les instances de base de données Oracle, PostgreSQL, MySQL et MariaDB utilisent la technologie de basculement d'Amazon. Les instances de base de données SQL Server utilisent la mise en miroir de bases de données SQL Server (DBM).

Pour plus d'informations, consultez Haute disponibilité (multi-AZ) pour Amazon RDS (p. 43).

Sécurité de l'infrastructure dans Amazon RDS

En tant que service géré, Amazon RDS est protégé par les procédures de sécurité du réseau mondial AWS qui sont décrites dans le livre blanc Amazon Web Services : Présentation des procédures de sécurité.

Vous utilisez les appels d'API publiés AWS pour accéder à Amazon RDS via le réseau. Les clients doivent prendre en charge le protocole Transport Layer Security (TLS) 1.0. Nous recommandons TLS 1.2 ou version ultérieure. Les clients doivent également prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) La plupart des systèmes modernes telles que Java 7 et versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un mandataire IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

En outre, Amazon RDS offre des fonctions pour contribuer à prendre en charge la sécurité de l'infrastructure.

Groupes de sécurité

Les groupes de sécurité contrôlent l'accès dont dispose le trafic entrant et sortant d'une instance de base de données. Par défaut, l'accès au réseau est désactivé sur une instance de base de données. Vous pouvez spécifier des règles dans un groupe de sécurité qui autorisent l'accès depuis une plage d'adresses IP, un port ou un groupe de sécurité. Une fois les règles de trafic entrant configurées, les

mêmes règles s'appliquent à toutes les instances de base de données qui sont associées à ce groupe de sécurité.

Pour plus d'informations, consultez Contrôle d'accès par groupe de sécurité (p. 1590).

Accessibilité publique

Lorsque vous lancez une instance de base de données à l'intérieur d'un VPC basé sur le service Amazon VPC, vous pouvez activer ou désactiver l'accessibilité publique pour cette instance. Pour définir si l'instance de base de données que vous créez comporte un nom DNS qui se résout en une adresse IP publique, vous utilisez le paramètre Public accessibility (Accessibilité publique). Ce paramètre vous permet de définir s'il existe un accès publique à l'instance de base de données. Vous pouvez modifier une instance de base de données pour activer ou désactiver l'accessibilité publique en modifiant le paramètre Public accessibility (Accessibilité publique).

Pour plus d'informations, consultez Masquer une instance de base de données dans un VPC depuis Internet (p. 1622).

> Note
>
> Si votre instance de base de données se trouve dans un VPC mais n'est pas accessible publiquement, vous pouvez également utiliser une connexion VPN site à site AWS ou une connexion AWS Direct Connect pour y accéder à partir d'un réseau privé. Pour de plus amples informations, veuillez consulter Confidentialité du trafic inter-réseaux (p. 1535).

Amazon RDS et interface des points de terminaison VPC (AWS PrivateLink)

Vous pouvez établir une connexion privée entre votre VPC et vos points de terminaison d'API Amazon RDS en créant un point de terminaison de VPC d'interface. Les points de terminaison d'interface sont alimentés par AWS PrivateLink.

AWS PrivateLink vous permet d'accéder en privé aux opérations d'API Amazon RDS sans passerelle Internet, périphérique NAT, connexion VPN ou connexion AWS Direct Connect. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec les points de terminaison d'API Amazon RDS pour lancer, modifier ou mettre fin à des instances de base de données. Vos instances n'ont pas non plus besoin d'adresses IP publiques pour utiliser une des opérations d'API RDS disponibles. Le trafic entre votre VPC et Amazon RDS ne quitte pas le réseau Amazon.

Chaque point de terminaison d'interface est représenté par une ou plusieurs interfaces réseau Elastic dans vos sous-réseaux. Pour de plus amples informations sur les interfaces réseau Elastic, veuillez consulter Interfaces réseau Elastic dans le Guide de l'utilisateur Amazon EC2.

Pour de plus amples informations sur les points de terminaison de VPC, veuillez consulter Points de terminaison d'un VPC d'interface (AWS PrivateLink) dans le Guide de l'utilisateur Amazon VPC. Pour de plus amples informations sur les opérations de l'API RDS, veuillez consulter Amazon RDS API Reference.

Considérations relatives aux points de terminaison VPC Amazon RDS

Avant de configurer un point de terminaison d'un VPC d'interface pour les points de terminaison d'API Amazon RDS, assurez-vous de vérifier les propriétés et limitations du point de terminaison d'interface dans le Amazon VPC Guide de l'utilisateur.

Amazon RDS prend en charge l'exécution d'appels en direction de toutes ses actions d'API depuis votre VPC.

Les stratégies de point de terminaison d'un VPC sont prises en charge pour Amazon RDS. Par défaut, l'accès complet à Amazon RDS est autorisé via le point de terminaison. Pour de plus amples informations, veuillez consulter Contrôle de l'accès aux services avec des points de terminaison d'un VPC dans le Amazon VPC Guide de l'utilisateur.

Disponibilité

Amazon RDS prend actuellement en charge les points de terminaison d'un VPC dans les régions AWS suivantes :

- USA Est (Ohio)
- USA Est (Virginie du Nord)
- USA Ouest (Californie du Nord)
- USA Ouest (Oregon)
- Asie-Pacifique (Hong Kong)
- Asie-Pacifique (Mumbai)
- Asie-Pacifique (Séoul)
- Asie-Pacifique (Singapour)
- Asie-Pacifique (Sydney)
- Asie-Pacifique (Tokyo)
- Canada (Centre)
- Europe (Francfort)
- Europe (Irlande)
- Europe (Londres)
- Europe (Paris)
- Europe (Stockholm)
- Moyen-Orient (Bahreïn)
- Amérique du Sud (São Paulo)
- Chine (Pékin)
- Chine (Ningxia)
- AWS GovCloud (US-East)
- AWS GovCloud (USA Ouest)

Création d'un point de terminaison de VPC d'interface pour Amazon RDS

Vous pouvez créer un point de terminaison d'un VPC pour l'API Amazon RDS à l'aide de la console Amazon VPC ou de l'AWS Command Line Interface (AWS CLI). Pour de plus amples informations, veuillez consulter Création d'un point de terminaison d'interface dans le Amazon VPC Guide de l'utilisateur.

Créez un point de terminaison d'un VPC pour Amazon RDS à l'aide du nom de service `com.amazonaws.`*`region`*`.rds`.

À l'exception des régions AWS en Chine, si vous activez le DNS privé pour le point de terminaison, vous pouvez faire des demandes d'API à Amazon RDS avec son point de terminaison de VPC en utilisant son nom DNS par défaut pour la région AWS, par exemple `rds.us-east-1.amazonaws.com`. Pour les

régions AWS Chine (Ningxia) et Chine (Pékin), vous pouvez effectuer des demandes d'API avec le point de terminaison de VPC en utilisant respectivement `rds-api.cn-north-1.amazonaws.com.cn` et `rds-api.cn-northwest-1.amazonaws.com.cn`.

Pour de plus amples informations, veuillez consulter Accès à un service via un point de terminaison d'interface dans le Amazon VPC Guide de l'utilisateur.

Création d'une stratégie de point de terminaison d'un VPC pour Amazon RDS

Vous pouvez attacher une stratégie de point de terminaison à votre point de terminaison d'un VPC qui contrôle l'accès à Amazon RDS. La stratégie spécifie les informations suivantes :

- Le mandataire qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être exécutées.

Pour de plus amples informations, veuillez consulter Contrôle de l'accès aux services avec des points de terminaison d'un VPC dans le Guide de l'utilisateur Amazon VPC.

Exemple : stratégie de point de terminaison d'un VPC pour les actions Amazon RDS

Voici un exemple de stratégie de point de terminaison pour Amazon RDS. Lorsqu'elle est attachée à un point de terminaison, cette stratégie accorde l'accès aux actions Amazon RDS répertoriées pour tous les mandataires sur toutes les ressources.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "rds:CreateDBInstance",
            "rds:ModifyDBInstance",
            "rds:CreateDBSnapshot"
         ],
         "Resource":"*"
      }
   ]
}
```

Exemple : stratégie de point de terminaison d'un VPC qui refuse tout accès à partir d'un compte AWS spécifié

La stratégie de point de terminaison d'un VPC suivante refuse au compte AWS `123456789012` tout accès aux ressources utilisant le point de terminaison. La stratégie autorise toutes les actions provenant d'autres comptes.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    },
    {
```

```
      "Action": "*",
      "Effect": "Deny",
      "Resource": "*",
      "Principal": {
        "AWS": [
          "123456789012"
        ]
      }
    ]
}
```

Bonnes pratiques de sécurité pour Amazon RDS

Utilisez des comptes AWS Identity and Access Management (IAM) pour contrôler l'accès aux opérations d'API Amazon RDS, particulièrement les opérations qui créent, modifient ou suppriment des ressources Amazon RDS. Les ressources de ce type incluent les instances de base de données, les groupes de sécurité et les groupes de paramètres. Utilisez également IAM pour contrôler les actions qui effectuent des tâches administratives courantes telles que la sauvegarde et la restauration d'instances de base de données.

- Créez un utilisateur IAM pour chaque personne qui gère les ressources Amazon RDS, y compris vous-même. N'utilisez pas d'informations d'identification AWS pour gérer les ressources Amazon RDS.
- Accordez à chaque utilisateur un ensemble minimum d'autorisations requises pour exécuter ses tâches.
- Utilisez des groupes IAM pour gérer efficacement des autorisations pour plusieurs utilisateurs.
- Effectuer une rotation régulière des informations d'identification IAM.
- Configurez AWS Secrets Manager pour effectuer une rotation automatique des secrets pour Amazon RDS. Pour plus d'informations, consultez Rotation de vos secrets AWS Secrets Manager dans le Guide de l'utilisateur AWS Secrets Manager. Vous pouvez également récupérer les informations d'identification auprès d'AWS Secrets Manager par programmation. Pour de plus amples informations, veuillez consulter Récupération de la valeur du secret dans le Guide de l'utilisateur AWS Secrets Manager.

Pour plus d'informations sur IAM, consultez AWS Identity and Access Management. Pour plus d'informations sur les bonnes pratiques IAM, consultez Bonnes pratiques IAM.

Utilisez l'AWS Management Console l'AWS CLI ou l'API RDS pour modifier le mot de passe de l'utilisateur principal. Si vous utilisez un autre outil, comme SQL client, pour modifier le mot de passe de l'utilisateur principal, cela pourrait finir par la révocation involontaire des privilèges de l'utilisateur.

Contrôle d'accès par groupe de sécurité

Les groupes de sécurité contrôlent l'accès dont dispose le trafic entrant et sortant d'une instance de base de données. Trois types de groupes de sécurité sont utilisés avec Amazon RDS : les groupes de sécurité VPC, les groupes de sécurité de base de données et les groupes de sécurité EC2-Classic. En termes simples, le fonctionnement est le suivant :

- Un groupe de sécurité VPC contrôle l'accès aux instances de base de données et aux instances EC2 dans un VPC.
- Un groupe de sécurité de base de données contrôle l'accès réseau aux instances de base de données EC2-Classic qui ne sont pas dans un VPC.
- Un groupe de sécurité EC2-Classic contrôle l'accès à une instance EC2. Pour de plus amples informations sur les groupes de sécurité EC2-Classic, veuillez consulter EC2-Classic dans la documentation Amazon EC2.

Par défaut, l'accès réseau est désactivé pour une instance de base de données. Vous pouvez spécifier des règles dans un groupe de sécurité qui autorisent l'accès depuis une plage d'adresses IP, un port ou un groupe de sécurité. Une fois les règles de trafic entrant configurées, les mêmes règles s'appliquent à toutes les instances de base de données qui sont associées à ce groupe de sécurité. Vous pouvez spécifier jusqu'à 20 règles dans un groupe de sécurité.

Groupes de sécurité VPC

Chaque règle de groupe de sécurité VPC permet à une source spécifique d'accéder à une instance de base de données dans un VPC associée à ce groupe de sécurité VPC. Cette source peut être une plage d'adresses (par exemple, 203.0.113.0/24) ou un autre groupe de sécurité VPC. En spécifiant un groupe de sécurité VPC en tant que source, vous autorisez le trafic entrant provenant de toutes les instances (généralement les serveurs d'application) qui utilisent le groupe de sécurité VPC source. Les groupes de sécurité VPC peuvent avoir des règles qui régissent à la fois le trafic entrant et sortant, même si les règles de trafic sortant ne s'appliquent généralement pas aux instances de base de données. Des règles de trafic sortant s'appliquent uniquement si l'instance de base de données fonctionne comme un client. Par exemple, dès règles de trafic sortant s'appliquent à une instance de base de données Oracle DB avec des liens de base de données sortants. Vous devez utiliser l'API Amazon EC2 ou l'option Groupe de sécurité de la console VPC pour créer des groupes de sécurité VPC.

Lorsque vous créez des règles pour votre groupe de sécurité VPC pour permettre d'accéder aux instances dans votre VPC, vous devez spécifier un port pour chaque plage d'adresses à laquelle la règle autorise l'accès. Par exemple, si vous souhaitez activer l'accès SSH vers les instances du VPC, vous créez une règle qui autorise l'accès au port TCP 22 pour la plage d'adresses spécifiée.

Vous pouvez configurer plusieurs groupes de sécurité VPC qui permettent d'accéder à des ports différents pour différentes instances dans votre VPC. Par exemple, vous pouvez créer un groupe de sécurité VPC qui autorise l'accès au port TCP 80 pour les serveurs Web de votre VPC. Vous pouvez ensuite créer un autre groupe de sécurité VPC qui autorise l'accès au port TCP 3306 pour les instances de base de données RDS MySQL de votre VPC.

Pour plus d'informations sur les groupes de sécurité VPC, consultez Groupes de sécurité dans le Guide de l'utilisateur Amazon Virtual Private Cloud.

> Note
>
> Si votre instance de base de données se trouve dans un VPC mais n'est pas accessible publiquement, vous pouvez également utiliser une connexion VPN site à site AWS ou une connexion AWS Direct Connect pour y accéder à partir d'un réseau privé. Pour de plus amples informations, veuillez consulter Confidentialité du trafic inter-réseaux (p. 1535).

Groupes de sécurité DB

Les groupes de sécurité de base de données sont utilisés avec des instances de base de données qui ne se trouvent pas dans un VPC, ni dans la plateforme EC2-Classic. Chaque règle de groupe de sécurité DB permet à une source spécifique d'accéder à une instance de base de données associée à ce groupe de sécurité DB. Cette source peut être une plage d'adresses (par exemple, 203.0.113.0/24) ou un groupe de sécurité EC2-Classic. Lorsque vous spécifiez un groupe de sécurité EC2-Classic en tant que source, vous autorisez le trafic entrant provenant de toutes les instances EC2 qui utilisent ce groupe de sécurité EC2-Classic. Les règles d'un groupe de sécurité de base de données s'appliquent uniquement au trafic entrant. Le trafic sortant n'est actuellement pas autorisé pour les instances de base de données.

Vous n'avez pas besoin de spécifier un numéro de port de destination lorsque vous créez des règles de groupe de sécurité de base de données. Le numéro de port défini pour l'instance de base de données est utilisé comme numéro de port de destination pour toutes les règles définies pour le groupe de sécurité de base de données. Les ensembles de sécurité de base de données peuvent être créés à l'aide des opérations d'API Amazon RDS ou de la page Amazon RDS de la AWS Management Console.

Pour plus d'informations sur l'utilisation des groupes de sécurité DB, consultez Utilisation des groupes de sécurité DB (plateforme EC2-Classic) (p. 1596).

Groupes de sécurité de base de données vs. Groupes de sécurité VPC

Le tableau ci-dessous montre les différences clés entre les groupes de sécurité DB et les groupes de sécurité VPC.

Groupe de sécurité DB	Groupe de sécurité VPC
Contrôle l'accès aux instances de base de données situées hors d'un VPC.	Contrôle l'accès aux instances de base de données situées dans un VPC.
Utilise les opérations d'API Amazon RDS ou la page Amazon RDS de la AWS Management Console pour créer et gérer un groupe et des règles.	Utilise les opérations d'API Amazon EC2 ou la page Amazon VPC de la AWS Management Console pour créer et gérer un groupe et des règles.
Lorsque vous ajoutez une règle à un groupe, vous n'avez pas besoin de spécifier de numéro de port ni de protocole.	Lorsque vous ajoutez une règle à un groupe, indiquez le protocole TCP. En outre, spécifiez le même numéro de port que celui que vous avez utilisé pour créer les instances de base de données (ou options) que vous envisagez d'ajouter au groupe en tant que membres.
Les groupes autorisent l'accès à partir des groupes de sécurité EC2-Classic dans votre compte AWS ou dans d'autres comptes.	Les groupes autorisent l'accès à partir des autres groupes de sécurité VPC dans votre VPC uniquement.

Scénario de groupes de sécurité

Une utilisation courante d'une instance de base de données dans un VPC consiste à partager les données avec un serveur d'application qui s'exécute dans une instance Amazon EC2 dans le même VPC et auquel accède une application cliente située hors du VPC. Dans ce scénario, vous utilisez les pages RDS et VPC sur la AWS Management Console ou les opérations d'API RDS et EC2 pour créer les instances et les groupes de sécurité nécessaires :

1. Créez un groupe de sécurité VPC (par exemple, `sg-appsrv1`) et définissez des règles entrantes qui utilisent les adresses IP de l'application cliente comme source. Ce groupe de sécurité autorise votre application cliente à se connecter aux instances EC2 dans un VPC qui utilise ce groupe de sécurité.
2. Créez une instance EC2 pour l'application et ajoutez l'instance EC2 au groupe de sécurité VPC (`sg-appsrv1`) que vous avez créé à l'étape précédente. L'instance EC2 dans le VPC partage le groupe de sécurité VPC avec l'instance de base de données.
3. Créez un second groupe de sécurité VPC (par exemple, `sg-dbsrv1`) et créez une nouvelle règle en spécifiant le groupe de sécurité VPC que vous avez créé à l'étape 1 (`sg-appsrv1`) en tant que source.
4. Créez une instance de base de données et ajoutez-la au groupe de sécurité VPC (`sg-dbsrv1`) que vous avez créé à l'étape précédente. Lorsque vous créez l'instance de base de données, utilisez le même numéro de port que celui spécifié pour la règle du groupe de sécurité VPC (`sg-dbsrv1`) que vous avez créée à l'étape 3.

Le schéma suivant illustre ce scénario.

Pour plus d'informations sur l'utilisation d'un VPC, consultez VPC Amazon Virtual Private Cloud et Amazon RDS (p. 1610).

Création d'un groupe de sécurité VPC

Vous pouvez créer un groupe de sécurité VPC pour une instance de base de données à l'aide de la console VPC. Pour plus d'informations sur la création d'un groupe de sécurité, consultez Créer un groupe de sécurité qui autorise l'accès à votre instance de base de données dans votre VPC (p. 66) et Groupes de sécurité dans le Guide de l'utilisateur Amazon Virtual Private Cloud.

Association d'un groupe de sécurité à une instance de base de données

Vous pouvez associer un groupe de sécurité de base de données à une instance de base de données à l'aide de l'option Modifier sur la console RDS, de l'API `ModifyDBInstance` Amazon RDS ou de la commande `modify-db-instance` de l'AWS CLI.

Pour plus d'informations sur la modification d'une instance de base de données , consultez Modification d'une instance de base de données Amazon RDS (p. 243). Pour plus de détails sur les groupes de sécurité lors de la restauration d'une instance de base de données à partir d'un instantané de base de données, consultez Considérations relatives aux groupes de sécurité (p. 330).

Suppression de Security Group DB VPC

Les groupes de sécurité DB VPC sont un mécanisme RDS permettant de synchroniser les informations de sécurité avec un groupe de sécurité VPC. Toutefois, cette synchronisation n'est plus requise car RDS a été mis à jour pour utiliser directement les informations des groupes de sécurité VPC.

> Note
>
> Les groupes de sécurité VPC de base de données sont obsolètes et diffèrent des groupes de sécurité de base de données, des groupes de sécurité VPC et des groupes de sécurité EC2-Classic.

Nous vous recommandons vivement de supprimer tous les groupes de sécurité de base de données VPC que vous utilisez actuellement. Si vous ne supprimez pas vos groupes de sécurité de base de données VPC, vous pouvez rencontrer des comportements inattendus avec vos instances de base de données qui peuvent poser de graves problèmes, tels que la perte de l'accès à une instance de base de données. Les comportements inattendus peuvent résulter d'une action telle qu'une mise à jour apportée à une instance de base de données, à un groupe de paramètres, etc. De tells mises à jour entraînent la resynchronisation par RDS du groupe de sécurité de base de données VPC avec le groupe de sécurité VPC. Cette resynchronisation peut entraîner le remplacement de vos informations de sécurité par des informations de sécurité incorrectes et obsolètes. Cela peut affecter gravement votre accès à vos instances de base de données.

Comment déterminer si vous possédez un groupe de sécurité DB VPC ?

Comme les groupes de sécurité de base de données VPC sont désormais obsolètes, ils n'apparaissent pas dans la console RDS. Toutefois, vous pouvez appeler la commande describe-db-security-groups de l'interface AWS CLI ou l'opération d'API DescribeDBSecurityGroups pour déterminer si vous avez des groupes de sécurité de base de données VPC.

Dans ce cas, vous pouvez appeler la commande d'AWS CLI `describe-db-security-groups` avec JSON indiqué comme format de sortie. Ce faisant, vous pouvez identifier les groupes de sécurité VPC de base de données grâce à l'identifiant VPC figurant sur la deuxième ligne de la sortie pour le groupe de sécurité, comme illustré dans l'exemple suivant.

```
{
    "DBSecurityGroups": [
        {
            "VpcId": "vpc-abcd1234",
            "DBSecurityGroupDescription": "default:vpc-abcd1234",
            "IPRanges": [
                {
                    "Status": "authorized",
                    "CIDRIP": "xxx.xxx.xxx.xxx/n"
                },
                {
                    "Status": "authorized",
                    "CIDRIP": "xxx.xxx.xxx.xxx/n "
                }
            ],
            "OwnerId": "123456789012",
            "EC2SecurityGroups": [],
            "DBSecurityGroupName": "default:vpc-abcd1234"
        }
    ]
}
```

Si vous exécutez l'opération d'API `DescribeDBSecurityGroups`, vous pouvez identifier les groupes de sécurité de base de données VPC à l'aide de l'élément de réponse `<VpcId>`, tel qu'illustré dans l'exemple suivant.

```
<DBSecurityGroup>
  <EC2SecurityGroups/>
  <DBSecurityGroupDescription>default:vpc-abcd1234</DBSecurityGroupDescription>
  <IPRanges>
    <IPRange>
      <CIDRIP>xxx.xxx.xxx.xxx/n</CIDRIP>
      <Status>authorized</Status>
    </IPRange>
    <IPRange>
```

```
      <CIDRIP>xxx.xxx.xxx.xxx/n</CIDRIP>
      <Status>authorized</Status>
    </IPRange>
  </IPRanges>
  <VpcId>vpc-abcd1234</VpcId>
  <OwnerId>123456789012</OwnerId>
  <DBSecurityGroupName>default:vpc-abcd1234</DBSecurityGroupName>
</DBSecurityGroup>
```

Comment supprimer un groupe de sécurité DB VPC ?

Étant donné que les groupes de sécurité VPC de base de données n'apparaissent pas dans la console RDS, vous devez appeler la commande delete-db-security-group de l'interface AWS CLI ou l'opération d'API DeleteDBSecurityGroup pour supprimer un groupe de sécurité VPC de base de données.

Après avoir supprimé un groupe de sécurité de base de données VPC, vos instances de base de données de votre VPC continuent à être sécurisées par le groupe de sécurité pour ce VPC. Le groupe de sécurité DB VPC qui a été supprimé n'était qu'une copie des informations des groupes de sécurité VPC.

Passer en revue vos modèles AWS CloudFormation

Les versions antérieures des modèles AWS CloudFormation peuvent contenir des instructions permettant de créer un groupe de sécurité DB VPC. Comme les groupes de sécurité VPC de base de données ne sont pas encore complètement abandonnés, il est encore possible d'en créer. Assurez-vous que les modèles AWS CloudFormation que vous utilisez pour fournir des paramètres de sécurité à une instance de base de données ne créent pas également un groupe de sécurité VPC de base de données. N'utilisez pas de modèles AWS CloudFormation qui créent un groupe RDS `DBSecurityGroup` avec un identifiant `EC2VpcId` comme illustré dans l'exemple suivant.

```
{
  "DbSecurityByEC2SecurityGroup" : {
    "Type" : "AWS::RDS::DBSecurityGroup",
    "Properties" : {
       "GroupDescription" : "Ingress for security group",
       "EC2VpcId" : "MyVPC",
       "DBSecurityGroupIngress" : [ {
          "EC2SecurityGroupId" : "sg-b0ff1111",
          "EC2SecurityGroupOwnerId" : "111122223333"
       }, {
          "EC2SecurityGroupId" : "sg-ffd722222",
          "EC2SecurityGroupOwnerId" : "111122223333"
       } ]
    }
  }
}
```

A la place, ajoutez des informations de sécurité pour vos instances de base de données dans un VPC à l'aide de groupes de sécurité VPC, comme illustré dans l'exemple suivant.

```
{
  "DBInstance" : {
    "Type": "AWS::RDS::DBInstance",
    "Properties": {
      "DBName"            : { "Ref" : "DBName" },
      "Engine"            : "MySQL",
      "MultiAZ"           : { "Ref": "MultiAZDatabase" },
      "MasterUsername"    : { "Ref" : "<master_username>" },
      "DBInstanceClass"   : { "Ref" : "DBClass" },
```

```
      "AllocatedStorage"  : { "Ref" : "DBAllocatedStorage" },
      "MasterUserPassword": { "Ref" : "<master_password>" },
      "VPCSecurityGroups" : [ { "Fn::GetAtt": [ "VPCSecurityGroup", "GroupId" ] } ]
    }
  }
}
```

Utilisation des groupes de sécurité DB (plateforme EC2-Classic)

Par défaut, l'accès au réseau est désactivé sur une instance de base de données. Vous pouvez spécifier des règles dans un groupe de sécurité qui autorise l'accès depuis une plage d'adresses IP, un port ou un groupe de sécurité. Une fois les règles de trafic entrant configurées, les mêmes règles s'appliquent à toutes les instances de base de données qui sont associées à ce groupe de sécurité. Vous pouvez spécifier jusqu'à 20 règles dans un groupe de sécurité.

Amazon RDS prend en charge deux types différents de groupes de sécurité. Celui que vous utilisez dépend de la plateforme Amazon RDS sur laquelle vous êtes :

- Groupes de sécurité VPC – pour la plateforme EC2-VPC.
- Groupes de sécurité de base de données – pour la plateforme EC2-Classic.

Il est fort probable que vous soyez sur la plateforme EC2-VPC (et que vous devrez utiliser les groupes de sécurité VPC) si l'une des conditions suivantes est vraie :

- Si vous êtes un nouveau client Amazon RDS.
- Si vous n'avez jamais créé d'instance de base de données auparavant.
- Si vous créez une instance de base de données dans une région AWS que vous n'avez pas encore utilisée.

Sinon, si vous vous trouvez sur la plateforme EC2-Classic, vous utilisez les groupes de sécurité de base de données pour gérer l'accès à vos instances de base de données Amazon RDS. Pour plus d'informations sur les différences entre les groupes de sécurité de base de données et les groupes de sécurité VPC, consultez Contrôle d'accès par groupe de sécurité (p. 1590).

> **Note**
>
> Pour déterminer la plateforme sur laquelle vous êtes, consultez Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611).
> Si vous êtes sur la plateforme EC2-VPC, vous pouvez utiliser les groupes de sécurité VPC au lieu des groupes de sécurité DB. Pour plus d'informations sur l'utilisation d'un VPC, consultez VPC Amazon Virtual Private Cloud et Amazon RDS (p. 1610).

Rubriques

- Création d'un groupe de sécurité de base de données (p. 1597)
- Liste des groupes de sécurité de base de données disponibles (p. 1598)
- Affichage d'un groupe de sécurité DB (p. 1599)
- Association d'un groupe de sécurité de base de données à une instance de base de données (p. 1600)
- Autorisation de l'accès réseau à un groupe de sécurité DB depuis une plage IP (p. 1600)
- Autorisation de l'accès réseau à une instance de base de données depuis une instance Amazon EC2 (p. 1602)
- Révocation de l'accès réseau à une instance de base de données depuis une plage IP (p. 1604)

Création d'un groupe de sécurité de base de données

Pour créer un groupe de sécurité DB, vous devez fournir un nom et une description.

Console

Pour créer un groupe de sécurité DB

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Depuis le volet de navigation, sélectionnez Groupes de sécurité.

   Note

   Si vous utilisez la plateforme EC2-VPC, l'option Groupes de sécurité n'apparaît pas dans le volet de navigation. Dans ce cas, vous pouvez utiliser les groupes de sécurité VPC au lieu des groupes de sécurité DB. Pour plus d'informations sur l'utilisation d'un VPC, consultez VPC Amazon Virtual Private Cloud et Amazon RDS (p. 1610).
3. Choisissez Create DB Security Group.
4. Saisissez le nom et la description du nouveau groupe de sécurité de base de données dans les zones de texte Nom et Description. Le nom du groupe de sécurité ne peut pas contenir d'espaces et ne peut pas commencer par un chiffre.
5. Choisissez Yes, Create.

   Le groupe de sécurité de base de données est créé.

   Un groupe de sécurité de base de données nouvellement créé ne fournit pas un accès à une instance de base de données par défaut. Vous devez spécifier une plage d'adresses IP ou un groupe de sécurité EC2-Classic pouvant avoir accès à l'instance de base de données. Pour spécifier des adresses IP ou un groupe de sécurité EC2-Classic pour un groupe de sécurité de base de données, veuillez consulter Autorisation de l'accès réseau à un groupe de sécurité DB depuis une plage IP (p. 1600).

AWS CLI

Pour créer un groupe de sécurité de base de données, utilisez la commande `create-db-security-group` de l'AWS CLI.

Example

Pour Linux, macOS ou Unix :

```
aws rds create-db-security-group \
    --db-security-group-name mydbsecuritygroup \
    --db-security-group-description "My new security group"
```

Pour Windows :

```
aws rds create-db-security-group ^
    --db-security-group-name mydbsecuritygroup ^
    --db-security-group-description "My new security group"
```

Un groupe de sécurité de base de données nouvellement créé ne fournit pas un accès à une instance de base de données par défaut. Vous devez spécifier une plage d'adresses IP ou un groupe de sécurité EC2-Classic pouvant avoir accès à l'instance de base de données. Pour spécifier des adresses IP ou un groupe de sécurité EC2-Classic pour un groupe de sécurité de base de données, veuillez consulter Autorisation de l'accès réseau à un groupe de sécurité DB depuis une plage IP (p. 1600).

API

Pour créer un groupe de sécurité de base de données, appelez la fonction Amazon RDS `CreateDBSecurityGroup` avec les paramètres suivants :

- `DBSecurityGroupName = mydbsecuritygroup`
- `Description = "My new security group"`

Example

```
https://rds.amazonaws.com/
    ?Action=CreateDBSecurityGroup
    &DBSecurityGroupName=mydbsecuritygroup
    &Description=My%20new%20db%20security%20group
    &Version=2012-01-15
    &SignatureVersion=2
    &SignatureMethod=HmacSHA256
    &Timestamp=2012-01-20T22%3A06%3A23.624Z
    &AWSAccessKeyId=<AWS Access Key ID>
    &Signature=<Signature>
```

Un groupe de sécurité de base de données nouvellement créé ne fournit pas un accès à une instance de base de données par défaut. Vous devez spécifier une plage d'adresses IP ou un groupe de sécurité EC2-Classic pouvant avoir accès à l'instance de base de données. Pour spécifier des adresses IP ou un groupe de sécurité EC2-Classic pour un groupe de sécurité de base de données, veuillez consulter Autorisation de l'accès réseau à un groupe de sécurité DB depuis une plage IP (p. 1600).

Liste des groupes de sécurité de base de données disponibles

Vous pouvez répertorier les groupes de sécurité DB qui ont été créés pour votre compte AWS.

Console

Pour répertorier tous les groupes de sécurité DB disponibles pour un compte AWS

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Depuis le volet de navigation, sélectionnez Groupes de sécurité.

   Les groupes de sécurité de base de données disponibles s'affichent dans la liste Groupes de sécurité de base de données.

   > **Note**
   >
   > Si vous utilisez la plateforme EC2-VPC, l'option Groupes de sécurité n'apparaît pas dans le volet de navigation. Dans ce cas, vous pouvez utiliser les groupes de sécurité VPC au lieu des groupes de sécurité DB. Pour plus d'informations sur l'utilisation d'un VPC, consultez VPC Amazon Virtual Private Cloud et Amazon RDS (p. 1610).

AWS CLI

Pour répertorier tous les groupes de sécurité de base de données disponibles pour un compte AWS, utilisez la commande `describe-db-security-groups` de l'AWS CLI sans paramètres.

Example

```
aws rds describe-db-security-groups
```

API

Pour répertorier tous les groupes de sécurité de base de données disponibles pour un compte AWS, appelez `DescribeDBSecurityGroups` sans paramètres.

Example

```
https://rds.amazonaws.com/
    ?Action=DescribeDBSecurityGroups
    &MaxRecords=100
    &Version=2009-10-16
    &SignatureVersion=2
    &SignatureMethod=HmacSHA256
    &AWSAccessKeyId=<AWS Access Key ID>
    &Signature=<Signature>
```

Affichage d'un groupe de sécurité DB

Vous pouvez affichez des informations détaillées sur votre groupe de sécurité DB pour voir les plages IP qui ont été autorisées.

Console

Pour afficher des propriétés d'un groupe de sécurité DB spécifique

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Depuis le volet de navigation, sélectionnez Groupes de sécurité.

   Note

   Si vous utilisez la plateforme EC2-VPC, l'option Groupes de sécurité n'apparaît pas dans le volet de navigation. Dans ce cas, vous pouvez utiliser les groupes de sécurité VPC au lieu des groupes de sécurité DB. Pour plus d'informations sur l'utilisation d'un VPC, consultez VPC Amazon Virtual Private Cloud et Amazon RDS (p. 1610).
3. Sélectionnez l'icône de détails pour le groupe de sécurité DB que vous souhaitez visualiser. Les informations détaillées pour le groupe de sécurité DB sont affichées.

AWS CLI

Pour afficher les propriétés d'un groupe de sécurité de base de données spécifique, utilisez l'AWS CLI `describe-db-security-groups`. Spécifiez le groupe de sécurité DB que vous souhaitez afficher.

Example

Pour Linux, macOS ou Unix :

```
aws rds describe-db-security-groups \
    --db-security-group-name mydbsecuritygroup
```

Pour Windows :

```
aws rds describe-db-security-groups ^
    --db-security-group-name mydbsecuritygroup
```

API

Pour afficher les propriétés d'un groupe de sécurité de base de données, appelez `DescribeDBSecurityGroups` avec les paramètres suivants :

- `DBSecurityGroupName=mydbsecuritygroup`

Example

```
https://rds.amazonaws.com/
    ?Action=DescribeDBSecurityGroups
    &DBSecurityGroupName=mydbsecuritygroup
    &Version=2009-10-16
    &SignatureVersion=2
    &SignatureMethod=HmacSHA256
    &Timestamp=2009-10-16T22%3A23%3A07.107Z
    &AWSAccessKeyId=<AWS Access Key ID>
    &Signature=<Signature>
```

Association d'un groupe de sécurité de base de données à une instance de base de données

Vous pouvez associer un groupe de sécurité de base de données à une instance de base de données à l'aide de l'option Modifier de la console RDS, de l'API Amazon RDS `ModifyDBInstance` ou de la commande `modify-db-instance` de l'AWS CLI.

Pour plus d'informations sur la modification d'une instance de base de données , consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Autorisation de l'accès réseau à un groupe de sécurité DB depuis une plage IP

Par défaut, l'accès au réseau est désactivé sur une instance de base de données. Si vous souhaitez accéder à une instance de base de données qui ne soit pas dans un VPC, vous devez définir des règles d'accès pour un groupe de sécurité de base de données afin d'autoriser l'accès depuis certains groupes de sécurité EC2-Classic ou certaines plages IP CIDR. Vous devez alors associer cette instance de base de données à ce groupe de sécurité DB. Ce processus est appelé entrée. Une fois que l'entrée est configurée pour un groupe de sécurité DB, les mêmes règles d'entrée sont appliquées à toutes les instances de base de données associées à ce groupe de sécurité DB.

> **Warning**
>
> Si vous prévoyez d'accéder à une instance de base de données derrière un pare-feu afin de déterminer les adresses IP que vous devez utiliser, adressez-vous à votre administrateur réseau.

Dans l'exemple suivant, vous configurez un groupe de sécurité DB avec une règle d'entrée pour une plage IP CIDR.

Console

Pour configurer un groupe de sécurité DB avec une règle d'entrée pour une plage IP CIDR

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Depuis le volet de navigation, sélectionnez Groupes de sécurité.

   > **Note**
   >
   > Si vous utilisez la plateforme EC2-VPC, l'option Groupes de sécurité n'apparaît pas dans le volet de navigation. Dans ce cas, vous pouvez utiliser les groupes de sécurité VPC au lieu des groupes de sécurité DB. Pour plus d'informations sur l'utilisation d'un VPC, consultez VPC Amazon Virtual Private Cloud et Amazon RDS (p. 1610).

3. Sélectionnez l'icône de détails pour le groupe de sécurité DB que vous souhaitez autoriser.
4. Dans la page de détails de votre groupe de sécurité, sélectionnez CIDR/IP dans la liste déroulante Type de connexion, saisissez la plage CIDR pour la règle d'entrée que vous souhaitez ajouter à ce groupe de sécurité de base de données dans la zone de texte CIDR, puis choisissez Authorize (Autoriser).

   Tip

   La AWS Management Console affiche une IP CIDR basée sur votre connexion sous le champ de texte CIDR. Si vous n'accédez pas à l'instance de base de données depuis derrière un pare-feu, vous pouvez utiliser cette adresse IP CIDR.
5. Le statut de la règle d'entrée est autorisation en cours jusqu'à application de la nouvelle règle d'entrée à toutes les instances de base de données qui sont associées au groupe de sécurité de base de données que vous avez modifié. Après que la règle d'entrée a été appliquée avec succès, le statut passe à autorisé.

AWS CLI

Pour configurer un groupe de sécurité de base de données avec une règle d'entrée pour une plage IP CIDR, utilisez la commande `authorize-db-security-group-ingress` de l'AWS CLI.

Example

Pour Linux, macOS ou Unix :

```
aws rds authorize-db-security-group-ingress \
    --db-security-group-name mydbsecuritygroup \
    --cidrip 192.168.1.10/27
```

Pour Windows :

```
aws rds authorize-db-security-group-ingress ^
    --db-security-group-name mydbsecuritygroup ^
    --cidrip 192.168.1.10/27
```

La commande doit produire un résultat similaire à ce qui suit.

```
SECGROUP  mydbsecuritygroup  My new DBSecurityGroup
IP-RANGE  192.168.1.10/27  authorizing
```

API

Pour configurer un groupe de sécurité de base de données avec une règle d'entrée pour une plage IP CIDR, appelez l'API Amazon RDS `AuthorizeDBSecurityGroupIngress` avec les paramètres suivants :

- `DBSecurityGroupName = mydbsecuritygroup`
- `CIDRIP = 192.168.1.10/27`

Example

```
https://rds.amazonaws.com/
 ?Action=AuthorizeDBSecurityGroupIngress
 &CIDRIP=192.168.1.10%2F27
```

```
&DBSecurityGroupName=mydbsecuritygroup
&Version=2009-10-16
&Action=AuthorizeDBSecurityGroupIngress
&SignatureVersion=2
&SignatureMethod=HmacSHA256
&Timestamp=2009-10-22T17%3A10%3A50.274Z
&AWSAccessKeyId=<AWS Access Key ID>
&Signature=<Signature>
```

Autorisation de l'accès réseau à une instance de base de données depuis une instance Amazon EC2

Si vous souhaitez accéder à votre instance de base de données depuis une instance Amazon EC2, vous devez tout d'abord déterminer si votre instance EC2 et votre instance de base de données sont dans un VPC. Si vous utilisez un VPC par défaut, vous pouvez affecter le même groupe de sécurité EC2 ou VPC que celui que vous avez utilisé pour votre instance EC2 lorsque vous avez créé ou modifié l'instance de base de données à laquelle l'instance EC2 accède.

Si votre instance de base de données et votre instance EC2 ne sont pas dans un VPC, vous devez configurer le groupe de sécurité de l'instance de base de données avec une règle d'entrée qui permet le trafic depuis l'instance Amazon EC2. Pour cela, vous ajoutez le groupe de sécurité EC2-Classic pour l'instance EC2 au groupe de sécurité de base de données pour l'instance de base de données. Dans cet exemple, vous ajoutez une règle d'entrée à un groupe de sécurité de base de données pour un groupe de sécurité EC2-Classic.

> **Important**
>
> - L'ajout d'une règle d'entrée à un groupe de sécurité de base de données pour un groupe de sécurité EC2-Classic accorde uniquement l'accès à vos instances de base de données depuis les instances Amazon EC2 associées à ce groupe de sécurité EC2-Classic.
> - Vous ne pouvez pas autoriser un groupe de sécurité EC2-Classic qui se trouve dans une région AWS autre que celle de votre instance de base de données. Vous pouvez autoriser une plage d'adresses IP, ou spécifier un groupe de sécurité EC2-Classic dans la même région AWS qui se rapporte à l'adresse IP d'une autre région AWS. Si vous spécifiez une plage IP, nous vous recommandons d'utiliser l'adresse IP privée de votre instance Amazon EC2, qui fournit un itinéraire réseau plus direct depuis votre instance Amazon EC2 vers votre instance de base de données Amazon RDS et n'implique pas de charge réseau pour les données envoyées en dehors du réseau Amazon.

Console

Pour ajouter un groupe de sécurité EC2-Classic à un groupe de sécurité de base de données

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Depuis le volet de navigation, sélectionnez Groupes de sécurité.

   > **Note**
   >
   > Si vous utilisez la plateforme EC2-VPC, l'option Groupes de sécurité n'apparaît pas dans le volet de navigation. Dans ce cas, vous pouvez utiliser les groupes de sécurité VPC au lieu des groupes de sécurité DB. Pour plus d'informations sur l'utilisation d'un VPC, consultez VPC Amazon Virtual Private Cloud et Amazon RDS (p. 1610).
3. Sélectionnez l'icône de détails pour le groupe de sécurité DB que vous souhaitez autoriser l'accès.
4. Sur la page des détails de votre groupe de sécurité, choisissez Groupe de sécurité EC2 en regard de Type de connexion, puis sélectionnez le groupe de sécurité EC2-Classic que vous souhaitez utiliser. Choisissez ensuite Authorize (Autoriser).

5. Le statut de la règle d'entrée est autorisation en cours jusqu'à application de la nouvelle règle d'entrée à toutes les instances de base de données qui sont associées au groupe de sécurité de base de données que vous avez modifié. Après que la règle d'entrée a été appliquée avec succès, le statut passe à autorisé.

AWS CLI

Pour accorder l'accès à un groupe de sécurité EC2-Classic, utilisez la commande AWS CLI `authorize-db-security-group-ingress`.

Example

Pour Linux, macOS ou Unix :

```
aws rds authorize-db-security-group-ingress \
    --db-security-group-name default  \
    --ec2-security-group-name myec2group \
    --ec2-security-group-owner-id 987654321021
```

Pour Windows :

```
aws rds authorize-db-security-group-ingress ^
    --db-security-group-name default  ^
    --ec2-security-group-name myec2group ^
    --ec2-security-group-owner-id 987654321021
```

La commande doit produire un résultat similaire à ce qui suit :

```
SECGROUP  Name     Description
SECGROUP  default  default
      EC2-SECGROUP  myec2group  987654321021  authorizing
```

API

Pour autoriser l'accès réseau à un groupe de sécurité EC2-Classic, appelez la fonction d'API Amazon RDS https://docs.aws.amazon.com/AmazonRDS/latest/APIReference/API_AuthorizeDBSecurityGroupIngress.html`AuthorizeDBSecurityGroupIngress` avec les paramètres suivants :

- `EC2SecurityGroupName = myec2group`
- `EC2SecurityGroupOwnerId = 987654321021`

Example

```
https://rds.amazonaws.com/
    ?Action=AuthorizeDBSecurityGroupIngress
    &EC2SecurityGroupOwnerId=987654321021
    &EC2SecurityGroupName=myec2group
    &Version=2009-10-16
    &SignatureVersion=2
    &SignatureMethod=HmacSHA256
    &Timestamp=2009-10-22T17%3A10%3A50.274Z
    &AWSAccessKeyId=<AWS Access Key ID>
    &Signature=<Signature>
```

Révocation de l'accès réseau à une instance de base de données depuis une plage IP

Vous pouvez facilement révoquer l'accès réseau depuis une plage IP CIDR à des instances de base de données appartenant à un groupe de sécurité de base de données en révoquant la règle d'entrée IP CIDR associée.

Dans cet exemple, vous révoquez une règle d'entrée pour une plage IP CDR sur un groupe de sécurité de base de données.

Console

Pour révoquer une règle d'entrée pour une plage IP CIDR sur un groupe de sécurité DB

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Depuis le volet de navigation, sélectionnez Groupes de sécurité.

   Note

   Si vous utilisez la plateforme EC2-VPC, l'option Groupes de sécurité n'apparaît pas dans le volet de navigation. Dans ce cas, vous pouvez utiliser les groupes de sécurité VPC au lieu des groupes de sécurité DB. Pour plus d'informations sur l'utilisation d'un VPC, consultez VPC Amazon Virtual Private Cloud et Amazon RDS (p. 1610).
3. Sélectionnez l'icône de détails pour le groupe de sécurité DB associé à la règle d'entrée que vous souhaitez révoquer.
4. Dans la page de détails pour votre groupe de sécurité, choisissez Supprimer à côté de la règle d'entrée que vous voulez révoquer.
5. Le statut de la règle d'entrée est révocation jusqu'à suppression de la règle d'entrée de toutes les instances de base de données qui sont associées au groupe de sécurité de base de données que vous avez modifié. Après la suppression réussie de la règle d'entrée, cette dernière est supprimée du groupe de sécurité de base de données.

AWS CLI

Pour révoquer une règle d'entrée pour une plage IP CIDR sur un groupe de sécurité de base de données, utilisez la commande `revoke-db-security-group-ingress` de l'AWS CLI.

Example

Pour Linux, macOS ou Unix :

```
aws rds revoke-db-security-group-ingress \
    --db-security-group-name mydbsecuritygroup \
    --cidrip 192.168.1.1/27
```

Pour Windows :

```
aws rds revoke-db-security-group-ingress ^
    --db-security-group-name mydbsecuritygroup ^
    --cidrip 192.168.1.1/27
```

La commande doit produire un résultat similaire à ce qui suit.

```
SECGROUP  mydbsecuritygroup  My new DBSecurityGroup
  IP-RANGE  192.168.1.1/27  revoking
```

API

Pour révoquer une règle d'entrée pour une plage IP CIDR sur un groupe de sécurité de base de données, appelez l'opération d'API Amazon RDShttps://docs.aws.amazon.com/AmazonRDS/latest/APIReference/API_RevokeDBSecurityGroupIngress.html`RevokeDBSecurityGroupIngress` avec les paramètres suivants :

- `DBSecurityGroupName = mydbsecuritygroup`
- `CIDRIP = 192.168.1.10/27`

Example

```
https://rds.amazonaws.com/
    ?Action=RevokeDBSecurityGroupIngress
    &DBSecurityGroupName=mydbsecuritygroup
    &CIDRIP=192.168.1.10%2F27
    &Version=2009-10-16
    &SignatureVersion=2&SignatureMethod=HmacSHA256
    &Timestamp=2009-10-22T22%3A32%3A12.515Z
    &AWSAccessKeyId=<AWS Access Key ID>
    &Signature=<Signature>
```

Privilèges du compte utilisateur principal

Lorsque vous créez un nouveau d'instance de base de données, l'utilisateur principal par défaut que vous utilisez obtient certains privilèges pour ce d'instance de base de données. Le tableau suivant montre les privilèges et les rôles de base de données que l'utilisateur principal obtient pour chacun des moteurs de base de données.

> **Important**
>
> Nous vous recommandons vivement de ne pas avoir recours au rôle d'utilisateur principal directement dans vos applications. Au lieu de cela, respectez la bonne pratique qui consiste à avoir recours à un utilisateur de base de données doté des privilèges minimum requis pour votre application.

> **Note**
>
> Si vous supprimez par mégarde les autorisations de l'utilisateur principal, vous pouvez les restaurer en modifiant l'instance de base de données et définissant un nouveau mot de passe d'utilisateur principal. Pour plus d'informations sur la modification d'une instance de base de données, consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Moteur de base de données	Privilège système	Rôle de base de données
MySQL et 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` (uniquement pour Amazon RDS MySQL versions 5.6, 5.7 et 8.0, Amazon RDS MariaDB)	—

Moteur de base de données	Privilège système	Rôle de base de données
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
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
Microsoft SQL Server	ADMINISTER BULK OPERATIONS, ALTER ANY CONNECTION, ALTER ANY LINKED SERVER, ALTER ANY LOGIN, ALTER SERVER STATE, ALTER TRACE, CONNECT SQL, CREATE ANY DATABASE, VIEW ANY DATABASE, VIEW ANY DEFINITION, VIEW SERVER STATE, ALTER ANY SERVER ROLE, ALTER ANY USER, ALTER ON ROLE SQLAgentOperatorRole	DB_OWNER (rôle au niveau de la base de données), PROCESSADMIN (rôle au niveau du serveur), SETUADMIN (rôle au niveau du serveur), SQLAgentUserRole (rôle au niveau de la base de données)

Utilisation des rôles liés à un service pour Amazon RDS

Amazon RDS utilise les rôles liés à un service AWS Identity and Access Management (IAM). Un rôle lié à un service est un type unique de rôle IAM lié directement à Amazon RDS. Les rôles liés à un service sont prédéfinis par Amazon RDS et comprennent toutes les autorisations nécessaires au service pour appeler d'autres services AWS en votre nom.

Un rôle lié à un service permet d'utiliser Amazon RDS plus facilement, car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. Amazon RDS définit les autorisations de ses rôles liés à un service et, sauf définition contraire, seul Amazon RDS peut endosser ses rôles. Les autorisations définies comprennent la stratégie d'approbation et la stratégie d'autorisation. De plus, cette stratégie d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer les rôles uniquement après la suppression préalable de leurs ressources connexes. Vos ressources Amazon RDS sont ainsi protégées, car vous ne pouvez pas involontairement supprimer l'autorisation d'accéder aux ressources.

Pour de plus amples informations sur les autres services qui prennent en charge les rôles liés à un service, veuillez consulter Services AWS qui fonctionnent avec IAM et recherchez les services qui comportent Oui dans la colonne Rôle lié à un service. Choisissez un Oui ayant un lien permettant de consulter la documentation du rôle lié à un service, pour ce service.

Autorisations des rôles liés à un service pour Amazon RDS

Amazon RDS utilise le rôle lié à un service nommé AWSServiceRoleForRDS – to allow Amazon RDS to call AWS services on behalf of your DB instances.

Le rôle lié à un service AWSServiceRoleForRDS approuve les services suivants pour endosser le rôle :

- `rds.amazonaws.com`

La stratégie d'autorisations liée au rôle permet à Amazon RDS d'exécuter les actions suivantes sur les ressources spécifiées :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcs",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:ModifyVpcEndpoint",
                "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:*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kinesis:CreateStream",
                "kinesis:PutRecord",
                "kinesis:PutRecords",
                "kinesis:DescribeStream",
                "kinesis:SplitShard",
                "kinesis:MergeShards",
                "kinesis:DeleteStream",
                "kinesis:UpdateShardCount"
            ],
            "Resource": [
                "arn:aws:kinesis:*:*:stream/aws-rds-das-*"
            ]
        }
    ]
}
```

Note

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, groupe ou rôle) de créer, modifier ou supprimer un rôle lié à un service. Si vous rencontrez le message d'erreur suivant :
Impossible de créer la ressource. Vérifiez que vous détenez l'autorisation de créer un rôle lié au service. Dans le cas contraire, attendez et réessayez ultérieurement.
Vérifiez que les autorisations suivantes sont activées :

```
{
    "Action": "iam:CreateServiceLinkedRole",
    "Effect": "Allow",
    "Resource": "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
    "Condition": {
        "StringLike": {
            "iam:AWSServiceName":"rds.amazonaws.com"
        }
    }
}
```

Pour de plus amples informations, veuillez consulter Autorisations de rôles liés à un service dans le IAM Guide de l'utilisateur.

Création d'un rôle lié à un service pour Amazon RDS

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous create a DB instance, Amazon RDS crée automatiquement le rôle lié au service.

> **Important**
>
> Si vous utilisiez le service Amazon RDS avant December 1, 2017, quand il commençait à prendre en charge les rôles liés à un service, Amazon RDS créait le rôle AWSServiceRoleForRDS dans votre compte. Pour en savoir plus, consultez Un nouveau rôle est apparu dans mon compte AWS.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous create a DB instance, Amazon RDS crée automatiquement le rôle lié au service.

Modification d'un rôle lié à un service pour Amazon RDS

Amazon RDS ne vous permet pas de modifier le rôle lié à un service AWSServiceRoleForRDS. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas modifier le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide de IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le IAM Guide de l'utilisateur.

Suppression d'un rôle lié à un service pour Amazon RDS

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez supprimer toutes vos instances et de bases de données avant de pouvoir supprimer le rôle lié à un service.

Nettoyage d'un rôle lié à un service

Avant de pouvoir utiliser IAM pour supprimer un rôle lié à un service, vous devez d'abord vérifier qu'aucune session n'est active pour le rôle et supprimer toutes les ressources utilisées par le rôle.

Pour vérifier si une session est active pour le rôle lié à un service dans la console IAM

1. Connectez-vous à la AWS Management Console et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation de la console IAM, choisissez Rôles. Ensuite, sélectionnez le nom (et non la case à cocher) du rôle AWSServiceRoleForRDS.
3. Sur la page Summary (Récapitulatif) du rôle sélectionné, choisissez l'onglet Access Advisor.
4. Dans l'onglet Access Advisor, consultez l'activité récente pour le rôle lié à un service.

   > **Note**
   >
   > Si vous n'êtes pas certain que Amazon RDS utilise le rôle AWSServiceRoleForRDS, vous pouvez essayer de supprimer le rôle. Si le service utilise ce rôle, la suppression échoue et vous avez accès aux régions AWS dans lesquelles le rôle est utilisé. Si le rôle est utilisé, vous devez attendre que la session se termine avant de pouvoir le supprimer. Vous ne pouvez pas révoquer la session d'un rôle lié à un service.

Si vous souhaitez supprimer le rôle AWSServiceRoleForRDS, vous devez d'abord supprimer toutes vos instances et de bases de données.

Suppression de toutes vos instances

Utilisez l'une des procédures suivantes pour supprimer chacune de vos instances.

Pour supprimer une instance (console)

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans la panneau de navigation, choisissez Databases (Bases de données).
3. Choisissez l'instance que vous voulez supprimer.
4. Pour Actions, choisissez Supprimer.
5. Si vous on vous demande de Créer un aperçu final ?, sélectionnez Oui ou Non.
6. Si vous avez choisi Oui à l'étape précédente, dans le champ Nom de l'instantané final, saisissez le nom de votre instantané final.
7. Sélectionnez Delete.

Pour supprimer une instance (CLI)

Voir `delete-db-instance` dans le AWS CLI Command Reference.

Pour supprimer une instance (API)

Voir `DeleteDBInstance` dans le Amazon RDS API Reference.

Vous pouvez utiliser la console IAM, le CLI IAM ou l'API IAM pour supprimer le rôle lié à un service AWSServiceRoleForRDS. Pour de plus amples informations, veuillez consulter Suppression d'un rôle lié à un service dans le IAM Guide de l'utilisateur.

VPC Amazon Virtual Private Cloud et Amazon RDS

Il existe deux plateformes Amazon Elastic Compute Cloud (EC2) qui hébergent des instances de base de données Amazon RDS EC2-VPC et EC2-Classic. Amazon Virtual Private Cloud (Amazon VPC) vous permet de lancer des ressources AWS, telles que des instances de base de données Amazon RDS, dans un virtual private cloud (VPC).

Lorsque vous utilisez un Amazon VPC, vous avez le contrôle sur votre environnement de réseau virtuel : vous pouvez sélectionner votre propre plage d'adresses IP, créer des sous-réseaux et configurer le routage et les listes de contrôle d'accès. Les fonctionnalités de base de Amazon RDS sont les mêmes, que votre instance de base de données s'exécute ou non dans un Amazon VPC : Amazon RDS gère les sauvegardes, les correctifs logiciels, la détection automatique de pannes et la récupération. Il n'y a pas de frais supplémentaires pour exécuter votre instance de base de données dans un Amazon VPC.

Les comptes qui prennent en charge uniquement la plateforme EC2-VPC disposent d'un VPC par défaut. Toutes les nouvelles instances de base de données sont créées dans le VPC par défaut, à moins que vous ne spécifiez une autre option. Si vous êtes un nouveau client Amazon RDS, si vous n'avez jamais créé

d'instance de base de données ou si vous créez une instance de base de données dans une région AWS que vous n'avez pas encore utilisée, il est fort probable que vous soyez sur la plateforme EC2-VPC et que vous ayez un VPC par défaut.

Certaines instances de base de données héritées de la plateforme EC2-Classic ne sont pas dans un VPC. La plateforme EC2-Classic existante n'a pas de VPC par défaut, mais comme pour l'une ou l'autre plateforme, vous pouvez créer votre propre VPC et spécifier qu'une instance de base de données se trouve dans ce VPC.

Rubriques

- Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611)
- Scénarios d'accès à une instance de base de données d'un VPC (p. 1613)
- Utilisation d'une instance de base de données dans un VPC (p. 1620)
- Mise à jour du VPC pour une instance de base de données (p. 1627)
- Didacticiel : créer un Amazon VPC à utiliser avec une instance de base de données (p. 1629)

Cette documentation ne présente que les fonctionnalités VPC relatives aux instances de base de données Amazon RDS. Pour plus d'informations sur Amazon VPC, consultez Amazon VPC Guide de mise en route et Amazon VPC Guide de l'utilisateur. Pour obtenir des informations sur l'utilisation d'une passerelle NAT (Network Address Translation), veuillez consulter Passerelles NAT dans le Guide de l'utilisateur Amazon Virtual Private Cloud.

Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic

Votre compte AWS et la région AWS que vous choisissez déterminent sur laquelle des deux plateformes RDS votre instance de base de données est créée : EC2-VPC ou EC2-Classic. Le type de plateforme détermine si vous avez un VPC par défaut et le type de groupe de sécurité que vous utilisez pour fournir l'accès à votre instance de base de données.

La plateforme EC2-Classic héritée est la plateforme d'origine utilisée par Amazon RDS. Si vous êtes sur cette plateforme et que vous souhaitez utiliser un VPC, vous devez créer le VPC à l'aide de la console Amazon VPC ou de l'API Amazon VPC. Les comptes qui prennent en charge uniquement la plateforme EC2-VPC disposent d'un VPC par défaut où toutes les instances de base de données sont créées et vous devez utiliser un groupe de sécurité EC2 ou VPC pour fournir l'accès à l'instance de base de données.

> **Important**
>
> Si vous êtes un nouveau client Amazon RDS, si vous n'avez jamais créé d'instance de base de données auparavant ou si vous créez une instance de base de données dans une région AWS que vous n'avez pas encore utilisée, il est fort probable que vous soyez sur la plateforme EC2-VPC et que vous ayez un VPC par défaut.

Vous pouvez savoir sur quelle plateforme votre compte AWS dans une région AWS donnée se trouve en examinant le tableau de bord de la console RDS ou de la console EC2. Si vous êtes un nouveau client Amazon RDS, si vous n'avez jamais créé d'instance de base de données auparavant ou si vous créez une instance de base de données dans une région AWS que vous n'avez pas encore utilisée, il se peut que vous soyez redirigé vers la page de la console de la première utilisation et que vous ne puissiez pas voir la page d'accueil suivante.

Plateforme EC2-VPC dans la console

Si Supported platforms (Plateformes prises en charge) indique `VPC`, comme illustré ci-après dans la console RSDS, votre compte AWS de la région AWS actuelle utilise la plateforme EC2-VPC, ainsi qu'un VPC par défaut.

Si Supported platforms (Plateformes prises en charge) indique `VPC`, comme illustré ci-après dans la console EC2, votre compte AWS de la région AWS actuelle utilise la plateforme EC2-VPC, ainsi qu'un VPC par défaut.

Dans la console RDS et la console EC2, le nom du VPC par défaut est affiché sous la plateforme prise en charge. Pour fournir l'accès à une instance de base de données créée sur la plateforme EC2-VPC, vous devez créer un groupe de sécurité VPC. Pour obtenir des informations sur la création d'un groupe de sécurité VPC, consultez Didacticiel : créer un Amazon VPC à utiliser avec une instance de base de données (p. 1629).

Plateforme EC2-Classic dans la console

Dans la console RDS et la console EC2, si Supported platforms (Plateformes prises en charge) indique `EC2,VPC`, votre compte AWS de la région AWS actuelle utilise la plateforme EC2-Classic et vous n'avez pas de VPC par défaut. Pour fournir l'accès à une instance de base de données créée sur la plateforme EC2-Classic, vous devez créer un groupe de sécurité de base de données. Pour obtenir des informations

sur la création d'un groupe de sécurité DB, consultez Création d'un groupe de sécurité de base de données (p. 1597).

Note

- Vous pouvez créer un VPC sur la plateforme EC2-Classic, mais il n'en sera pas créé par défaut, car il se trouve sur les comptes qui prennent en charge la plateforme EC2-VPC.
- Vous pouvez facilement déplacer une instance de base de données existante dans un VPC avec AWS Management Console. Pour plus d'informations, consultez Déplacement vers un VPC d'une instance de base de données n'appartenant pas à un VPC (p. 1627).

Scénarios d'accès à une instance de base de données d'un VPC

Amazon RDS prend en charge les scénarios suivants pour accéder à une instance de base de données :

instance de base de données	Accédée par
Dans un VPC	Une instance EC2 du même VPC (p. 1613)
	Une instance EC2 d'un autre VPC (p. 1615)
	Une instance EC2 ne figurant pas dans un VPC (p. 1616)
	Une application cliente via Internet (p. 1617)
Pas dans un VPC	Une instance EC2 d'un VPC (p. 1617)
	Une instance EC2 ne figurant pas dans un VPC (p. 1618)
	Une application cliente via Internet (p. 1619)

Note

Si votre instance de base de données se trouve dans un VPC mais n'est pas accessible publiquement, vous pouvez également utiliser une connexion VPN site à site AWS ou une connexion AWS Direct Connect pour y accéder à partir d'un réseau privé. Pour de plus amples informations, veuillez consulter Confidentialité du trafic inter-réseaux (p. 1535).

Une instance de base de données d'un VPC accédée par une instance EC2 du même VPC

Une utilisation courante d'une instance de base de données d'un VPC consiste à partager les données avec un serveur d'application qui s'exécute dans une instance EC2 du même VPC. Il s'agit du scénario utilisateur créé si vous utilisez AWS Elastic Beanstalk pour créer une instance EC2 et une instance de base de données dans le même VPC.

Le schéma suivant illustre ce scénario.

La solution la plus simple pour gérer l'accès entre les instances EC2 et les instances de base de données du même VPC consiste à agir ainsi :

- Créez un groupe de sécurité VPC dans lequel seront placées vos instances de base de données. Ce groupe de sécurité peut être utilisé pour restreindre l'accès aux instances de base de données. Par exemple, vous pouvez créer une règle personnalisée pour ce groupe de sécurité, qui autorise l'accès TCP à l'aide du port que vous avez attribué à l'instance de base de données lorsque vous l'avez créée et une adresse IP que vous utilisez pour accéder à l'instance de base de données à des fins de développement ou autre.
- Créez un groupe de sécurité VPC dans lequel seront placées vos instances EC2 (serveurs web et clients). Ce groupe de sécurité peut, si nécessaire, autoriser l'accès à l'instance EC2 à partir d'Internet à l'aide de la table de routage du VPC. Par exemple, vous pouvez définir des règles sur ce groupe de sécurité pour autoriser l'accès TCP à l'instance EC2 sur le port 22.
- Créez des règles personnalisées dans le groupe de sécurité pour vos instances de base de données qui autorisent les connexions depuis le groupe de sécurité que vous avez créé pour vos instances EC2. N'importe quel membre du groupe de sécurité peut ainsi accéder aux instances de base de données.

Pour obtenir un didacticiel qui explique comment créer un VPC avec des sous-réseaux publics et privés pour ce scénario, consultez Didacticiel : créer un Amazon VPC à utiliser avec une instance de base de données (p. 1629).

Pour créer une règle dans un groupe de sécurité VPC qui autorise les connexions à partir d'un autre groupe de sécurité, procédez comme suit :

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sélectionnez Groupes de sécurité.
3. Choisissez ou créez un groupe de sécurité auquel vous voulez autoriser les membres d'un autre groupe de sécurité à accéder. Dans le scénario précédent, il s'agit du groupe de sécurité que vous utilisez pour vos instances de base de données. Sélectionnez l'onglet Inbound Rules (Règles entrantes), puis Edit rule (Modifier la règle).
4. Sur la page Edit inbound rules (Modifier les règles entrantes), choisissez Add Rule (Ajouter une règle).
5. Dans Type, choisissez l'entrée qui correspond au port que vous avez utilisé lors de la création de votre instance de base de données, telle que MYSQL/Aurora.

6. Dans la zone Source, commencez à taper l'ID du groupe de sécurité, qui répertorie les groupes de sécurité correspondants. Choisissez le groupe de sécurité dont vous voulez autoriser les membres à accéder aux ressources protégées par ce groupe de sécurité. Dans le scénario précédent, il s'agit du groupe de sécurité que vous utilisez pour votre instance EC2.
7. Si nécessaire, répétez les étapes pour le protocole TCP en créant une règle avec Tous TCP comme Type et votre groupe de sécurité dans la zone Source. Si vous prévoyez d'utiliser le protocole UDP, créez une règle avec Tous UDP comme Type et votre groupe de sécurité dans la zone Source.
8. Choisissez Enregistrer lorsque vous avez terminé.

L'écran suivant affiche plusieurs règles entrantes.

Une instance de base de données d'un VPC accédée par une instance EC2 d'un autre VPC

Quand votre instance de base de données se trouve dans un VPC différent de l'instance EC2 que vous utilisez pour y accéder, vous pouvez utiliser l'appairage de VPC pour accéder à l'instance de base de données.

Le schéma suivant illustre ce scénario.

Une connexion d'appairage de VPC est une connexion de mise en réseau entre deux VPC qui permet de router le trafic entre ces derniers à l'aide d'adresses IP privées. Les instances des deux VPC peuvent communiquer entre elles comme si elles se trouvaient dans le même réseau. Vous pouvez créer une connexion d'appairage de VPC entre vos propres VPC, avec un VPC situé dans un autre compte AWS ou avec un VPC au sein d'une autre région AWS. Pour plus d'informations sur l'appairage de VPC, consultez Appairage de VPC dans le Guide de l'utilisateur Amazon Virtual Private Cloud.

Une instance de base de données ne figurant pas dans un VPC accédée par une instance EC2 d'un VPC

Vous pouvez communiquer entre une instance de base de données Amazon RDS qui se trouve dans un VPC et une instance EC2 qui ne se trouve pas dans un Amazon VPC à l'aide de ClassicLink. Lorsque vous utilisez ClassicLink, une application sur l'instance EC2 peut se connecter à l'instance de base de données à l'aide du point de terminaison pour l'instance de base de données. ClassicLink est disponible gratuitement.

Le schéma suivant illustre ce scénario.

Avec ClassicLink, vous pouvez connecter une instance EC2 à une base de données isolée logiquement où vous définissez la plage d'adresses IP et contrôlez les listes de contrôle d'accès (ACL) pour gérer le trafic réseau. Vous n'avez pas à utiliser les adresses IP publiques ou le tunneling pour communiquer avec l'instance de base de données du VPC. Cette disposition vous fournit la connexion au débit le plus élevé et à la latence la plus faible pour les communications inter-instance.

Pour activer ClassicLink entre une instance de base de données d'un VPC et une instance EC2 ne figurant pas dans un VPC

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, sélectionnez Vos VPC.
3. Choisissez le VPC utilisé par l'instance de base de données.
4. Dans Actions, choisissez Enable ClassicLink (Activer ClassicLink). Dans la boîte de dialogue de confirmation, sélectionnez Oui, activer.
5. Dans la console EC2, choisissez l'instance EC2 que vous voulez connecter à l'instance de base de données du VPC.
6. Dans Actions, choisissez ClassicLink, puis Link to VPC (Liens vers VPC).
7. Dans la page Link to VPC (Lien vers VPC), choisissez le groupe de sécurité que vous voulez utiliser, puis choisissez Link to VPC (Lier au VPC).

   Note

   Les fonctions de ClassicLink sont visibles uniquement sur les consoles pour les comptes et les régions prenant en charge EC2-Classic. Pour plus d'informations, consultez ClassicLink dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux.

Une instance de base de données d'un VPC accessible par une application cliente via Internet

Pour accéder à une instance de base de données d'un VPC à partir d'une application cliente via Internet, vous configurez un VPC avec un seul sous-réseau public et une passerelle Internet pour activer la communication sur Internet.

Le schéma suivant illustre ce scénario.

Nous recommandons la configuration suivante :

- Un VPC de taille /16 (par exemple, CIDR : 10.0.0.0/16). Cette taille fournit 65 536 adresses IP privées.
- Un sous-réseau de taille /24 (par exemple, CIDR : 10.0.0.0/24). Cette taille fournit 256 adresses IP privées.
- Une instance de base de données Amazon RDS associée au VPC et au sous-réseau. Amazon RDS affecte à votre instance de base de données une adresse IP au sein du sous-réseau.
- Une passerelle Internet qui connecte le VPC à Internet et à d'autres produits AWS.
- Groupe de sécurité associé à l'instance de base de données. Les règles de trafic entrant de votre groupe de sécurité permettent à votre application client d'accéder à votre instance de base de données.

Pour plus d'informations sur la création d'une instance de base de données dans un VPC, consultez Création d'une instance de base de données dans un VPC (p. 1624).

Une instance de base de données ne figurant pas dans un VPC accédée par une instance EC2 d'un VPC

Dans le cas où vous avez une instance EC2 dans un VPC et une instance de base de données RDS ne figurant pas dans un VPC, vous pouvez les connecter via l'Internet public.

Le schéma suivant illustre ce scénario.

> **Note**
>
> ClassicLink n'est pas disponible pour ce scénario, tel qu'indiqué dans Une instance de base de données ne figurant pas dans un VPC accédée par une instance EC2 d'un VPC (p. 1616).

Pour connecter votre instance de base de données et votre instance EC2 sur Internet, procédez comme suit :

- Assurez-vous que l'instance EC2 se trouve dans un sous-réseau public du VPC.
- Assurez-vous que l'instance de base de données RDS a été marquée comme publiquement accessible.
- Une remarque à propos des ACL réseau. Une liste ACL réseau est semblable à un pare-feu pour la totalité de votre sous-réseau. Par conséquent, toutes les instances de ce sous-réseau sont soumises aux règles des listes ACL réseau. Par défaut, les listes ACL réseau autorisent la totalité du trafic et vous n'avez généralement pas à vous en préoccuper, à moins que vous souhaitiez particulièrement ajouter des règles comme couche de sécurité supplémentaire. Un groupe de sécurité, d'autre part, est associé à des instances individuelles et vous n'avez pas à vous préoccuper des règles de groupe de sécurité.
- Ajoutez les règles d'entrée nécessaires au groupe de sécurité DB pour l'instance de base de données RDS.

  Une règle d'entrée spécifie un port réseau et une plage CIDR/IP. Par exemple, vous pouvez ajouter une règle d'entrée qui autorise le port 3306 à se connecter à une instance de base de données MySQL RDS et une plage CIDR/IP `203.0.113.25/32`. Pour plus d'informations, consultez Autorisation de l'accès réseau à un groupe de sécurité DB depuis une plage IP (p. 1600).

> **Note**
>
> Si vous souhaitez déplacer une instance de base de données existante vers un VPC, vous pouvez utiliser AWS Management Console pour faire facilement. Pour plus d'informations, consultez Déplacement vers un VPC d'une instance de base de données n'appartenant pas à un VPC (p. 1627).

Une instance de base de données ne figurant pas dans un VPC accédée par une instance EC2 ne figurant pas dans un VPC

Quand ni votre instance de base de données ni une application d'une instance EC2 ne se trouvent dans un VPC, vous pouvez accéder à l'instance de base de données en utilisant son point de terminaison et son port.

Le schéma suivant illustre ce scénario.

Vous devez créer un groupe de sécurité pour l'instance de base de données qui autorise l'accès à partir du port que vous avez spécifié lors de la création de l'instance de base de données. Par exemple, vous pouvez utiliser une chaîne de connexion similaire à celle utilisée avec sqlplus pour accéder à une instance de base de données Oracle :

```
PROMPT>sqlplus 'mydbusr@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=<endpoint>)
    (PORT=<port number>))(CONNECT_DATA=(SID=<database name>)))'
```

Pour plus d'informations, consultez la documentation suivante.

Moteur de base de données	Documentation
MariaDB	Connexion à une instance de base de données exécutant le moteur de base de données MariaDB (p. 556)
Microsoft SQL Server	Connexion à une instance de base de données exécutant le moteur de base de données Microsoft SQL Server (p. 618)
MySQL	Connexion à une instance de base de données exécutant le moteur de base de données MySQL (p. 793)
Oracle	Connexion à une instance de base de données Oracle (p. 961)
PostgreSQL	Connexion à une instance de base de données exécutant le moteur de base de données PostgreSQL (p. 1364)

Note

Si vous souhaitez déplacer une instance de base de données existante vers un VPC, vous pouvez utiliser AWS Management Console pour faire facilement. Pour plus d'informations, consultez Déplacement vers un VPC d'une instance de base de données n'appartenant pas à un VPC (p. 1627).

Une instance de base de données ne figurant pas dans un VPC accédée par une application cliente via Internet

Les nouveaux clients Amazon RDS peuvent uniquement créer une instance de base de données dans un VPC. Cependant, il se peut que vous ayez besoin de vous connecter à une instance de base de données Amazon RDS qui ne figure pas dans un VPC à partir d'une application cliente via Internet.

Le schéma suivant illustre ce scénario.

Dans ce scénario, vous devez vous assurer que le groupe de sécurité DB de l'instance de base de données RDS inclut les règles d'entrée nécessaires pour que votre application cliente puisse se connecter. Une règle d'entrée spécifie un port réseau et une plage CIDR/IP. Par exemple, vous pouvez ajouter une règle d'entrée qui autorise le port 3306 à se connecter à une instance de base de données MySQL RDS et une plage CIDR/IP `203.0.113.25/32`. Pour plus d'informations, consultez Autorisation de l'accès réseau à un groupe de sécurité DB depuis une plage IP (p. 1600).

> **Warning**
>
> Si vous prévoyez d'accéder à une instance de base de données derrière un pare-feu, parlez avec votre administrateur réseau pour déterminer les adresses IP à utiliser.

> **Note**
>
> Si vous souhaitez déplacer une instance de base de données existante vers un VPC, vous pouvez utiliser AWS Management Console pour faire facilement. Pour plus d'informations, consultez Déplacement vers un VPC d'une instance de base de données n'appartenant pas à un VPC (p. 1627).

Utilisation d'une instance de base de données dans un VPC

À moins que vous n'utilisiez une instance de base de données héritée, votre instance de base de données se trouve dans un Virtual Private Cloud (VPC). Un VPC est un réseau virtuel isolé de manière logique des autres réseaux virtuels du cloud AWS. Amazon VPC vous permet de lancer des ressources AWS, telles qu'une instance de base de données Amazon RDS ou une instance Amazon EC2 dans un VPC. Le VPC peut être un VPC par défaut fourni avec votre compte ou un VPC que vous créez. Tous les VPC sont associés à votre compte AWS.

Votre VPC par défaut a trois sous-réseaux que vous pouvez utiliser pour isoler les ressources à l'intérieur du VPC. Le VPC par défaut possède aussi une passerelle Internet qui peut être utilisée pour fournir l'accès aux ressources à l'intérieur du VPC depuis l'extérieur du VPC.

Pour la liste des scénarios impliquant des instances de base de données Amazon RDS dans un VPC et en dehors d'un VPC, consultez Scénarios d'accès à une instance de base de données d'un VPC (p. 1613).

Pour un didacticiel qui explique comment créer un VPC que vous pouvez utiliser avec un scénario Amazon RDS courant, consultez Didacticiel : créer un Amazon VPC à utiliser avec une instance de base de données (p. 1629).

Pour apprendre à utiliser des instances de base de données à l'intérieur d'un VPC, consultez les éléments suivants :

Rubriques

- Utilisation d'une instance de base de données dans un VPC (p. 1621)
- Utilisation de groupes de sous-réseaux DB (p. 1622)
- Masquer une instance de base de données dans un VPC depuis Internet (p. 1622)
- Création d'une instance de base de données dans un VPC (p. 1624)

Utilisation d'une instance de base de données dans un VPC

Voici quelques conseils d'utilisation d'une instance de base de données dans un VPC :

- Votre VPC doit avoir au moins deux sous-réseaux. Ces sous-réseaux doivent se trouver dans deux zones de disponibilité différentes de la région AWS où vous voulez déployer votre instance de base de données. Un sous-réseau est un segment d'une plage d'adresses IP d'un VPC que vous pouvez spécifier et qui vous permet de regrouper les instances en fonction de vos besoins de sécurité et de fonctionnement.

  > **Note**
  >
  > Le groupe de sous-réseaux de base de données d'une zone locale ne peut avoir qu'un seul sous-réseau.

- Si vous voulez que votre instance de base de données du VPC soit publiquement accessible, vous devez activer les noms d'hôte DNS des attributs du VPC, ainsi que la résolution DNS.
- Votre VPC doit avoir un groupe de sous-réseaux DB que vous créez (pour plus d'informations, consultez la section suivante). Vous créez un groupe de sous-réseaux de base de données en précisant les sous-réseaux que vous avez créé. Amazon RDS utilise ce groupe de sous-réseaux de base de données ainsi que votre zone de disponibilité pour choisir un sous-réseau et une adresse IP au sein de ce sous-réseau afin de l'attitrer à votre instance de base de données.
- Votre VPC doit avoir un groupe de sécurité VPC qui autorise l'accès à l'instance de base de données.
- Les blocs d'adresse CIDR de chacun de vos sous-réseaux doivent être assez grands pour accueillir les adresses IP de rechange utilisées par Amazon RDS pendant les activités de maintenance, y compris le basculement et le dimensionnement du calcul.
- Un VPC peut avoir un attribut instance tenancy (location d'instance) ayant la valeur par défaut ou dédiée. Tous les VPC par défaut ont l'attribut de location d'instance défini à la valeur par défaut et un VPC par défaut peut prendre en charge n'importe quelle classe d'instance de base de données.

  Si vous choisissez que votre instance de base de données se trouve dans un VPC dédié où l'attribut « instance tenancy » a la valeur « dedicated », la classe d'instance de base de données de votre instance de base de données doit être de l'un des types d'instance dédiée Amazon EC2 approuvés. Par exemple, l'instance dédiée EC2 m3.medium correspond à la classe d'instance de base de données db.m3.medium. Pour plus d'informations sur la location d'instance dans un VPC, consultez Instances dédiées dans le Guide de l'utilisateur Amazon Elastic Compute Cloud.

  Pour plus d'informations sur les types d'instance qui peuvent se trouver dans une instance dédiée, consultez Instances dédiées Amazon EC2 sur la page de tarification EC2.

  > **Note**
  >
  > Lorsque vous définissez l'attribut de location d'instance à dédier pour une instance de base de données Amazon RDS, cela ne garantit pas que l'instance de base de données s'exécute sur un hôte dédié.

- Lorsqu'un groupe d'options est affecté à une instance de base de données, il est lié à la plateforme prise en charge sur laquelle se trouve l'instance de base de données, VPC ou EC2-Classic (non-VPC). De plus, si une instance de base de données est dans un VPC, le groupe d'options associé à l'instance de base de données est lié à ce VPC. Cette liaison signifie que vous ne pouvez pas utiliser le groupe d'options assigné à une instance de base de données si vous tentez de restaurer l'instance de base de données dans un VPC différent ou sur une autre plateforme.

- Si vous restaurez une instance de base de données dans un autre VPC ou sur une autre plateforme, vous devez attribuer le groupe d'options par défaut à l'instance de base de données, assigner un groupe d'options lié à ce VPC ou à cette plateforme, ou créer un groupe d'options et l'affecter à l'instance de base de données. Avec les options permanentes ou persistantes, telles qu'Oracle TDE, vous devez créer un nouveau groupe d'options incluant l'option persistante ou permanente lorsque vous restaurez une instance de base de données dans un VPC différent.

Utilisation de groupes de sous-réseaux DB

Un sous-réseau est un segment d'une plage d'adresses IP d'un VPC que vous définissez pour regrouper vos ressources en fonction de vos besoins de sécurité et de fonctionnement. Un groupe de sous-réseaux DB est une collection de sous-réseaux (généralement privés) que vous créez dans un VPC et que vous spécifiez alors pour vos instances de base de données. Un groupe de sous-réseaux DB vous permet de spécifier un VPC particulier lors de la création d'instances de base de données à l'aide de l'interface de ligne de commande ou de l'API ; si vous utilisez la console, vous pouvez simplement choisir le VPC et les sous-réseaux que vous voulez utiliser.

Chaque groupe de sous-réseaux DB doit avoir des sous-réseaux dans au moins deux zones de disponibilité d'une région AWS donnée. Vous devez choisir un groupe de sous-réseaux de base de données lorsque vous créez une instance de base de données dans un VPC. Amazon RDS utilise ce groupe de sous-réseaux de base de données, ainsi que votre zone de disponibilité privilégiée, pour choisir un sous-réseau et une adresse IP au sein de ce sous-réseau, afin de l'attribuer à votre instance de base de données. Si l'instance de base de données principale d'un déploiement multi-AZ échoue, Amazon RDS peut promouvoir l'instance de secours et par la suite créer une nouvelle instance de secours à l'aide d'une adresse IP du sous-réseau dans l'une des autres zones de disponibilité.

Les sous-réseaux d'un groupe de sous-réseaux de base de données sont publics ou privés. Ils ne peuvent pas être un mélange de sous-réseaux publics et privés. Les sous-réseaux sont publics ou privés, selon la configuration que vous définissez pour leurs listes de contrôle d'accès réseau (ACL réseau) et leurs tables de routage.

> Note
>
> Le groupe de sous-réseaux de base de données d'une zone locale ne peut avoir qu'un seul sous-réseau.

Quand Amazon RDS crée une instance de base de données dans un VPC, il affecte une interface réseau à votre instance de base de données en utilisant une adresse IP de votre groupe de sous-réseaux de base de données. Cependant, nous vous recommandons fortement d'utiliser le nom DNS pour vous connecter à votre instance de base de données parce que l'adresse IP sous-jacente change pendant le basculement.

> Note
>
> Pour chaque instance de base de données que vous exécutez dans un VPC, assurez-vous de réserver au moins une adresse dans chaque sous-réseau du groupe de sous-réseaux de base de données qui sera utilisée par Amazon RDS pour les actions de récupération.

Masquer une instance de base de données dans un VPC depuis Internet

Un scénario Amazon RDS courant consiste à avoir un VPC dans lequel vous avez une instance EC2 avec une application web publique et une instance de base de données avec une base de données qui n'est pas accessible publiquement. Par exemple, vous pouvez créer un VPC qui dispose d'un sous-réseau public et d'un sous-réseau privé. Les instances Amazon EC2 qui fonctionnent comme serveurs web peuvent être déployés dans le sous-réseau public et les instances de base de données sont déployées dans le sous-réseau privé. Dans un tel déploiement, seuls les serveurs web ont accès aux instances de base de

données. Pour obtenir une illustration de ce scénario, consultez Une instance de base de données d'un VPC accédée par une instance EC2 du même VPC (p. 1613).

Lorsque vous lancez une instance de base de données dans un VPC, l'instance de base de données possède une adresse IP privée pour le trafic à l'intérieur du VPC. Cette adresse IP privée n'est pas accessible au public. Vous pouvez utiliser l'option Public access (Accès public) pour indiquer si l'instance de base de données possède également une adresse IP publique en plus de l'adresse IP privée. Si l'instance de base de données est désignée comme étant accessible au public, son point de terminaison DNS se résout à l'adresse IP privée à partir du VPC de l'instance de base de données, et à l'adresse IP publique à partir de l'extérieur du VPC de l'instance de base de données. L'accès à l'instance de base de données est finalement contrôlé par le groupe de sécurité qu'elle utilise, et cet accès public n'est pas autorisé si le groupe de sécurité attribué à l'instance de base de données ne l'autorise pas.

Vous pouvez modifier une instance de base de données pour activer ou désactiver l'accessibilité publique en modifiant l'option Public access (Accès public). Pour plus d'informations, consultez la section sur la modification de votre moteur de base de données.

L'illustration suivante présente l'option Public Access (Accès public) dans la section Additional connectivity configuration (Configuration de connectivité supplémentaire). Pour définir cette option, ouvrez la section Additional connectivity configuration (Configuration de connectivité supplémentaire) dans la section Connectivity (Connectivité).

Pour de plus amples informations sur la modification d'une instance de base de données afin de définir l'option Public access (Accès public), veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

> **Note**
>
> Si votre instance de base de données n'est pas accessible publiquement, vous pouvez également utiliser une connexion VPN site à site AWS ou une connexion AWS Direct Connect pour y accéder

à partir d'un réseau privé. Pour de plus amples informations, veuillez consulter Confidentialité du trafic inter-réseaux (p. 1535).

Création d'une instance de base de données dans un VPC

Les procédure suivantes vous aident à créer une instance de base de données dans un VPC. Si votre compte comporte un VPC par défaut, vous pouvez commencer par l'étape 3, car le VPC et le groupe de sous-réseaux DB ont déjà été créés pour vous. Si votre compte AWS n'a pas de VPC par défaut, ou si vous souhaitez créer un VPC supplémentaire, vous pouvez créer un nouveau VPC.

Si vous ignorez si vous avez un VPC par défaut, consultez Déterminer si vous utilisez une plateforme EC2-VPC ou EC2-Classic (p. 1611).

> Note
>
> Si vous voulez que votre instance de base de données du VPC soit publiquement accessible, vous devez mettre à jour les informations DNS pour le VPC en activant les attributs VPC noms d'hôtes DNS et résolution DNS. Pour plus d'informations sur la mise à jour des informations DNS pour une instance VPC, consultez Mise à jour de la prise en charge DNS pour votre VPC.

Suivez les étapes ci-après pour créer une instance de base de données dans un VPC:

- Étape 1 : Création d'un VPC (p. 1624)
- Étape 2 : Ajouter des sous-réseaux au VPC (p. 1624)
- Étape 3 : Créer un groupe de sous-réseaux DB (p. 1624)
- Étape 4 : Créer un groupe de sécurité VPC (p. 1626)
- Étape 5 : Créer une instance de base de données dans le VPC (p. 1627)

Étape 1 : Création d'un VPC

Si votre compte AWS ne comporte pas de VPC par défaut, ou si vous voulez créer un VPC supplémentaire, suivez les instructions de la création d'un VPC. Consultez Créer un VPC avec des sous-réseaux publics et privés (p. 1630) ou Étape 1 : Créer un VPC dans la documentation Amazon VPC.

Étape 2 : Ajouter des sous-réseaux au VPC

Une fois que vous avez créé un VPC, vous devez créer des sous-réseaux dans au moins deux zones de disponibilité. Vous utilisez ces sous-réseaux lorsque vous créerez un groupe de sous-réseaux de base de données. Si vous avez un VPC par défaut, un sous-réseau est automatiquement créé pour vous dans chaque zone de disponibilité de la région AWS.

Pour des instructions sur la façon de créer des sous-réseaux dans un VPC, consultez Créer un VPC avec des sous-réseaux publics et privés (p. 1630).

Étape 3 : Créer un groupe de sous-réseaux DB

Un groupe de sous-réseaux DB est une collection de sous-réseaux (généralement privés) que vous créez pour un VPC et que vous spécifiez alors pour vos instances de base de données. Un groupe de sous-réseaux DB vous permet de spécifier un VPC particulier lors de la création d'instances de base de données à l'aide de l'interface de ligne de commande ou de l'API. Si vous utilisez la console, vous pouvez simplement choisir le VPC et les sous-réseaux que vous voulez utiliser. Chaque groupe de sous-réseaux DB doit avoir au moins un sous-réseau dans au moins deux zones de disponibilité de la région AWS.

Pour qu'une instance de base de données soit publiquement accessible, les sous-réseaux du groupe de sous-réseaux DB doivent avoir une passerelle Internet. Pour de plus amples informations sur les

passerelles Internet pour les sous-réseaux, veuillez consulter Passerelles Internet dans la documentation relative à Amazon VPC.

> **Note**
>
> Le groupe de sous-réseaux de base de données d'une zone locale ne peut avoir qu'un seul sous-réseau.

Vous devez choisir un groupe de sous-réseaux de base de données lorsque vous créez une instance de base de données dans un VPC. Amazon RDS utilise ensuite ce groupe de sous-réseaux de base de données, ainsi que votre zone de disponibilité privilégiée, pour choisir un sous-réseau et une adresse IP au sein de ce sous-réseau. Amazon RDS crée et associe une interface réseau Elastic à votre instance de base de données avec cette adresse IP. Pour les déploiements multi-AZ, la définition d'un sous-réseau pour deux zones de disponibilité ou plus d'une région permet à Amazon RDS de créer une copie de secours dans une autre zone de disponibilité, le cas échéant. Vous devez procéder de la sorte même pour les déploiements Single-AZ, au cas où vous souhaitiez les convertir en déploiements multi-AZ par la suite.

Dans cette étape, vous créez un groupe de sous-réseaux de base de données et ajoutez les sous-réseaux que vous avez créés pour votre VPC.

Pour créer un groupe de sous-réseaux

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
2. Dans le volet de navigation, choisissez Subnet groups (Groupes de sous-réseaux).
3. Choisissez Create DB Subnet Group (Créer groupe de sous-réseaux de base de données).
4. Dans Nom, saisissez le nom de votre nouveau groupe de sous-réseaux de base de données.
5. Dans le champ Description, saisissez une description de votre groupe de sous-réseaux de base de données.
6. Pour VPC, choisissez le VPC que vous avez créé.
7. Dans la section Ajouter des sous-réseaux, choisissez les zones de disponibilité qui incluent les sous-réseaux à partir de Zones de disponibilité, puis choisissez les sous-réseaux à partir de Sous-réseaux.

Note

Si vous avez activé une zone locale, vous pouvez choisir un groupe de zone de disponibilité sur la page Créer un groupe de sous-réseaux DB. Dans ce cas, choisissez Groupe de zone de disponibilité, Zones de disponibilité et Sous-réseaux.

8. Sélectionnez Create.

   Votre nouveau groupe de sous-réseaux DB apparaît dans la liste des groupes de sous-réseaux sur la console RDS. Vous pouvez choisir le groupe de sous-réseaux DB pour afficher les détails, y compris l'ensemble des sous-réseaux associés au groupe, dans le volet des détails en bas de la fenêtre.

Étape 4 : Créer un groupe de sécurité VPC

Avant de créer votre instance de base de données, vous devez créer un groupe de sécurité VPC à associer à votre instance de base de données. Pour des instructions sur la création d'un groupe de sécurité pour votre instance de base de données, consultez Créer un groupe de sécurité VPC pour une instance de base de données privée (p. 1632) ou Groupes de sécurité pour votre VPC dans la documentation Amazon VPC.

Étape 5 : Créer une instance de base de données dans le VPC

Dans cette étape, vous créez une instance de base de données et utilisez le nom du VPC, le groupe de sous-réseaux DB et le groupe de sécurité VPC que vous avez créés dans les étapes précédentes.

> Note
>
> Si vous voulez que votre instance de base de données du VPC soit publiquement accessible, vous devez activer les noms d'hôte DNS des attributs du VPC, ainsi que la résolution DNS. Pour plus d'informations sur la mise à jour des informations DNS pour une instance VPC, consultez Mise à jour de la prise en charge DNS pour votre VPC.

Pour de plus amples informations sur la création d'une instance de base de données, veuillez consulter Création d'une instance de base de données Amazon RDS (p. 146).

Lorsque vous y êtes invité dans la section Réseau et sécurité, entrez le nom du VPC, le groupe de sous-réseaux de base de données et le groupe de sécurité VPC que vous avez créés aux étapes précédentes.

Mise à jour du VPC pour une instance de base de données

Vous pouvez utiliser AWS Management Console afin de déplacer votre instance de base de données vers un autre VPC.

Pour plus d'informations sur la modification d'une instance de base de données , consultez Modification d'une instance de base de données Amazon RDS (p. 243). Dans la section Réseau et sécurité de la page de modification illustrée ci-après, pour Groupe de sous-réseaux, saisissez le nouveau groupe de sous-réseaux. Le nouveau groupe de sous-réseaux doit être un groupe de sous-réseaux dans un nouveau VPC.

Déplacement vers un VPC d'une instance de base de données n'appartenant pas à un VPC

Certaines instances de base de données héritées de la plateforme EC2-Classic ne sont pas dans un VPC. Si votre instance de base de données n'est pas dans un VPC, vous pouvez utiliser AWS Management Console pour déplacer facilement votre instance de base de données vers un VPC. Avant de déplacer une instance de base de données, qui n'est pas dans un VPC, vers un VPC, vous devez créer le VPC.

Suivez les étapes ci-après pour créer un VPC pour votre instance de base de données.

- Étape 1 : Création d'un VPC (p. 1624)
- Étape 2 : Ajouter des sous-réseaux au VPC (p. 1624)

- Étape 3 : Créer un groupe de sous-réseaux DB (p. 1624)
- Étape 4 : Créer un groupe de sécurité VPC (p. 1626)

Chaque groupe de sous-réseaux de base de données doit inclure au moins les zones de disponibilité dans lesquelles se trouve l'instance de base de données.

Une fois que vous avez créé le VPC, procédez comme suit pour déplacer votre instance de base de données vers le VPC.

- Mise à jour du VPC pour une instance de base de données (p. 1627)

Nous vous recommandons vivement de créer une sauvegarde de votre instance de base de données immédiatement avant la migration. Cela garantit que vous serez en mesure de restaurer les données en cas d'échec de la migration. Pour plus d'informations, consultez Sauvegarde et restauration d'une instance de base de données Amazon RDS (p. 317).

Voici quelques limitations pour le déplacement de votre instance de base de données vers le VPC.

- Classes d'instance de base de données de génération précédente – Les classes d'instance de base de données de génération précédente peuvent ne pas être prises en charge sur la plateforme de VPC. Lorsque vous déplacez une instance de base de données vers un VPC, choisissez une classe d'instance de base de données db.m3 ou db.r3. Après avoir déplacé l'instance de base de données vers un VPC, vous pouvez mettre à l'échelle l'instance de base de données pour utiliser une classe d'instance de base de données ultérieure. Pour obtenir la liste complète des classes d'instance prises en charge par les VPC, veuillez consulter Types d'instance Amazon RDS.
- Multi-AZ – Le déplacement vers un VPC d'une instance de base de données à plusieurs zones de disponibilité (multi-AZ) ne se trouvant pas dans un VPC n'est pas pris en charge actuellement. Pour déplacer votre instance de base de données vers un VPC, modifiez d'abord l'instance de base de données de sorte qu'il s'agisse d'un déploiement mono-AZ. Modifiez le paramètre Déploiement multi-AZ sur Non. Après avoir déplacé l'instance de base de données vers un VPC, modifiez-la à nouveau de manière à en faire un déploiement multi-AZ. Pour de plus amples informations, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).
- Réplicas en lecture – Le déplacement vers un VPC d'une instance de base de données avec des réplicas en lecture ne se trouvant pas dans un VPC n'est pas pris en charge actuellement. Pour déplacer votre instance de base de données vers un VPC, supprimez d'abord tous ses réplicas de lecture. Après avoir déplacé l'instance de base de données vers un VPC, recréez les réplicas en lecture. Pour plus d'informations, consultez Utilisation des réplicas en lecture (p. 275).
- Groupes d'options – Si vous déplacez votre instance de base de données vers un VPC et que l'instance de base de données utilise un groupe d'options personnalisé, modifiez le groupe d'options associé à votre instance de base de données. Les groupes d'options sont propres à la plateforme, et le déplacement vers un VPC est une modification de plateforme. Pour utiliser un groupe d'options personnalisé dans ce cas, attribuez le groupe d'options VPC par défaut à l'instance de base de données, assignez à l'instance de base de données un groupe d'options utilisé par d'autres instances de base de données dans le VPC vers lequel vous effectuez le déplacement, ou créez un groupe d'options et assignez-le à l'instance de base de données. Pour de plus amples informations, veuillez consulter Utilisation de groupes d'options (p. 209).

Alternatives pour le déplacement vers un VPC d'une instance de base de données ne se trouvant pas dans un VPC avec un temps d'arrêt minimal

Les alternatives suivantes permettent de déplacer vers un VPC une instance de base de données ne se trouvant pas dans un VPC avec un temps d'arrêt minimal. Ces alternatives entraînent une perturbation minimale de l'instance de base de données source et lui permettent de servir le trafic utilisateur pendant la migration. Toutefois, le temps nécessaire à la migration vers un VPC varie en fonction de la taille de la base de données et des caractéristiques de la charge de travail active.

- AWS Database Migration Service(AWS DMS) – AWS DMS permet la migration dynamique des données tout en maintenant l'instance de base de données source pleinement opérationnelle, mais réplique uniquement un ensemble limité d'instructions DDL. AWS DMS ne propage pas les éléments tels que les index, les utilisateurs, les privilèges, les procédures stockées et d'autres modifications de base de données qui ne sont pas directement liées aux données de table. En outre, AWS DMS n'utilise pas automatiquement les instantanés RDS pour la création de l'instance de base de données initiale, ce qui peut augmenter le temps de migration. Pour de plus amples informations, veuillez consulter AWS Database Migration Service.
- Restauration d'instantanés de base de données ou restauration ponctuelle – Vous pouvez déplacer vers un VPC une instance de base de données en restaurant un instantané de l'instance de base de données ou en restaurant une instance de base de données à un moment donné. Pour plus d'informations, consultez Restauration à partir d'un instantané de base de données (p. 329) et Restauration d'une instance de base de données à une date spécifiée (p. 365).

Didacticiel : créer un Amazon VPC à utiliser avec une instance de base de données

Un scénario fréquent inclut une instance de base de données dans un Amazon VPC, qui partage les données avec un serveur web s'exécutant dans le même VPC. Dans ce didacticiel, vous créez le VPC pour ce scénario.

Le schéma suivant illustre ce scénario. Pour plus d'informations sur d'autres scénarios, consultez Scénarios d'accès à une instance de base de données d'un VPC (p. 1613).

Comme votre instance de base de données a uniquement besoin d'être accessible par votre serveur web, et non par Internet, vous créez un VPC avec les sous-réseaux publics et privés. Le serveur web étant hébergé dans le sous-réseau public, il peut atteindre Internet. L'instance de base de données est hébergée dans un sous-réseau privé. Le serveur web peut se connecter à l'instance de base de données, car il est hébergé au sein du même VPC, mais l'instance de base de données n'est pas accessible par Internet, ce qui offre une plus grande sécurité.

Ce didacticiel décrit la configuration d'un VPC pour les instances de base de données Amazon RDS. Pour plus d'informations sur Amazon VPC, consultez Amazon VPC Guide de mise en route et Amazon VPC Guide de l'utilisateur.

Note

Pour obtenir un didacticiel qui vous montre comment créer un serveur Web pour ce scénario VPC, consultez Didacticiel : Créer un serveur web et une instance de base de données Amazon RDS (p. 109).

Créer un VPC avec des sous-réseaux publics et privés

Utilisez la procédure suivante pour créer un VPC avec des sous-réseaux publics et privés.

Pour créer un VPC et des sous-réseaux

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le coin supérieur droit d'AWS Management Console, choisissez la région où vous voulez créer le VPC. Cet exemple utilise la région USA Ouest (Oregon).
3. Dans le coin supérieur gauche, choisissez VPC Dashboard (Tableau de bord VPC). Pour démarrer la création d'un VPC, choisissez Launch VPC Wizard (Lancer l'assistant VPC).
4. Sur la page Step 1: Select a VPC Configuration (Étape 1 : Sélectionner une configuration de VPC), choisissez VPC with Public and Private Subnets (VPC avec sous-réseaux publics et privés), puis Sélectionner.
5. Sur la page Step 2: VPC with Public and Private Subnets (Étape 2 : VPC avec sous-réseaux publics et privés), définissez ces valeurs :
   - Bloc d'adresse CIDR IPv4 : `10.0.0.0/16`
   - Bloc d'adresse CIDR IPv6 : Pas de bloc d'adresse CIDR IPv6
   - Nom VPC : `tutorial-vpc`
   - Bloc d'adresse CIDR IPv4 du sous-réseau public : `10.0.0.0/24`
   - Zone de disponibilité : `us-west-2a`
   - Nom du sous-réseau public : `Tutorial public`
   - CIDR IPv4 du sous-réseau privé : `10.0.1.0/24`
   - Zone de disponibilité : `us-west-2a`
   - Nom de sous-réseau privé : `Tutorial Private 1`
   - Type d'instance : `t2.small`

     Important

     Si la zone Instance type (Type d'instance) n'apparaît pas dans la console, choisissez Use a NAT instance instead (Utiliser à la place une instance NAT). Ce lien se trouve à droite.

     Note

     Si le type d'instance t2.small n'est pas répertorié, vous pouvez choisir une instance d'un type différent.
   - Nom de paire de clés : `No key pair`
   - Points de terminaison de service : Ignorez ce champ.
   - Activez les nom d'hôtes DNS : `Yes`
   - Location matérielle : `Default`
6. Lorsque vous avez terminé, choisissez Créer un VPC.

Création de sous-réseaux supplémentaires

Vous devez avoir deux sous-réseaux privés ou deux sous-réseaux publics pour créer un groupe de sous-réseaux de base de données qu'une instance de base de données puisse utiliser dans un VPC. Comme l'instance de base de données de ce didacticiel est privée, ajoutez un deuxième sous-réseau privé au VPC.

Pour créer un sous-réseau supplémentaire

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Pour ajouter le deuxième sous-réseau privé à votre VPC, choisissez successivement VPC Dashboard (Tableau de bord VPC), Subnets (Sous-réseaux) et Create Subnet (Créer un sous-réseau).
3. Sur la page Create subnet (Créer un sous-réseau), définissez les valeurs suivantes :
   - Balise de nom : `Tutorial private 2`
   - VPC : choisissez le VPC que vous avez créé lors de l'étape précédente : par exemple, `vpc-`*`identifier`* `tutorial-vpc`.
   - Zone de disponibilité : `us-west-2b`

     Note

     Choisissez une zone de disponibilité différente de celle que vous avez choisie pour le premier sous-réseau privé.
   - Bloc d'adresse CIDR IPv4 : `10.0.2.0/24`
4. Lorsque vous avez terminé, choisissez Create (Créer). Ensuite, choisissez Fermer sur la page de confirmation.
5. Pour vous assurer que le deuxième sous-réseau privé que vous avez créé utilise la même table de routage que le premier sous-réseau privé, procédez comme suit :
   a. Choisissez Tableau de bord du VPC, sélectionnez Sous-réseaux, puis choisissez le premier sous-réseau privé que vous avez créé pour le VPC, `Tutorial private 1`.
   b. Sous la liste des sous-réseaux, choisissez l'onglet Table de routage, et notez la valeur de Table de routage—, par exemple : `rtb-98b613fd`.
   c. Dans la liste des sous-réseaux, désélectionnez le premier sous-réseau privé.
   d. Dans la liste des sous-réseaux, choisissez le deuxième sous-réseau privé, `Tutorial private 2`, puis l'onglet Table de routage.
   e. Si la table de routage active n'est pas la même que la table de routage du premier sous-réseau privé, choisissez Edit route table association (Modifier l'association de la table de routage). Pour Route Table ID (ID de la table de routage), choisissez la table de routage que vous avez notée précédemment (par exemple : `rtb-98b613fd`). Ensuite, pour enregistrer votre sélection, choisissez Save (Enregistrer).

Créer un groupe de sécurité VPC pour un serveur web public

Ensuite, vous créez un groupe de sécurité pour l'accès public. Pour vous connecter aux instance publiques de votre VPC, vous ajoutez des règles entrantes à votre groupe de sécurité VPC qui autorisent le trafic à se connecter depuis Internet.

Pour créer un groupe de sécurité VPC

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Choisissez successivement VPC Dashboard (Tableau de bord VPC), Security Groups (Groupes de sécurité) et Create Security Group (Créer un groupe de sécurité).
3. Sur la page Create Security Group (Créer un groupe de sécurité), définissez les valeurs suivantes :

- Nom du groupe de sécurité : `tutorial-securitygroup`
- Description : `Tutorial Security Group`
- VPC : choisissez le VPC que vous avez créé précédemment : par exemple, `vpc-`*`identifier`* `(tutorial-vpc)`.

4. Ajoutez des règles entrantes au groupe de sécurité.

   a. Déterminez l'adresse IP que vous utiliserez pour la connexion aux instances de votre VPC. Pour déterminer votre adresse IP publique, dans une fenêtre ou un onglet de navigateur différent, vous pouvez utiliser le service à l'adresse https://checkip.amazonaws.com. Exemple d'adresse IP : `203.0.113.25/32`.

      Si votre connexion s'effectue via un fournisseur de services Internet (ISP) ou derrière votre pare-feu sans adresse IP statique, vous devez déterminer la plage d'adresses IP utilisée par les ordinateurs clients.

      > **Warning**
      >
      > Si vous utilisez `0.0.0.0/0`, vous permettez à toutes les adresses IP d'accéder à vos instances publiques. Cette approche est acceptable pour une brève durée dans un environnement de test, mais n'est pas sécurisée pour les environnements de production. Dans un environnement de production, vous autoriserez uniquement l'accès à vos instances pour une adresse IP ou une plage d'adresses spécifiques.

   b. Dans la section Règles entrantes, choisissez Ajouter une règle.

   c. Définissez les valeurs suivantes pour que votre nouvelle règle entrante autorise l'accès Secure Shell (SSH) à votre instance EC2. Pour ce faire, vous pouvez vous connecter à votre instance EC2 pour installer le serveur web et autres utilitaires, et pour charger le contenu de votre serveur web.

      - Type : `SSH`
      - Source : l'adresse IP ou la plage d'adresses IP de l'étape a ; par exemple : `203.0.113.25/32`.

   d. Choisissez Add rule.

   e. Définissez les valeurs suivantes pour que votre nouvelle règle entrante autorise HTTP à accéder à votre serveur Web.

      - Type : `HTTP`
      - Source : `0.0.0.0/0`.

5. Pour créer le groupe de sécurité, choisissez Créer un groupe de sécurité.

   Notez l'ID du groupe de sécurité, car vous en aurez besoin ultérieurement dans ce didacticiel.

Créer un groupe de sécurité VPC pour une instance de base de données privée

Pour que votre instance de base de données demeure privée, créez un deuxième groupe de sécurité pour l'accès privé. Pour vous connecter aux instance privées de votre VPC, vous ajoutez des règles entrantes à votre groupe de sécurité VPC qui autorisent le trafic depuis votre serveur web uniquement.

Pour créer un groupe de sécurité VPC

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Choisissez successivement VPC Dashboard (Tableau de bord VPC), Security Groups (Groupes de sécurité) et Create Security Group (Créer un groupe de sécurité).
3. Sur la page Create Security Group (Créer un groupe de sécurité), définissez les valeurs suivantes :

- Nom du groupe de sécurité : `tutorial-db-securitygroup`
- Description : `Tutorial DB Instance Security Group`
- VPC : choisissez le VPC que vous avez créé précédemment : par exemple, `vpc-`*`identifier`* `(tutorial-vpc)`.

4. Ajoutez des règles entrantes au groupe de sécurité.

   a. Dans la section Règles entrantes, choisissez Ajouter une règle.

   b. Définissez les valeurs suivantes pour que votre nouvelle règle entrante autorise le trafic MySQL sur le port 3306 à partir de votre instance EC2. Pour ce faire, vous pouvez vous connecter à partir de votre serveur web à votre instance de base de données afin de stocker et d'extraire les données entre votre application web et votre base de données.

      - Type : `MySQL/Aurora`
      - Source : identifiant du groupe de sécurité `tutorial-securitygroup` que vous avez créé précédemment dans ce didacticiel, par exemple : `sg-9edd5cfb`.

5. Pour créer le groupe de sécurité, choisissez Créer un groupe de sécurité.

Création d'un groupe de sous-réseaux DB

Un groupe de sous-réseaux DB est une collection de sous-réseaux que vous créez dans un VPC et que vous spécifiez alors pour vos instances de bases de données. Un groupe de sous-réseaux DB vous permet de spécifier un VPC particulier lors de la création d'instances de bases de données.

Pour créer un groupe de sous-réseaux

1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.

   > **Note**
   >
   > Assurez-vous de vous connecter à la console Amazon RDS et non à la console Amazon VPC.

2. Dans le volet de navigation, choisissez Subnet groups (Groupes de sous-réseaux).
3. Choisissez Create DB Subnet Group (Créer groupe de sous-réseaux de base de données).
4. Sur la page Create DB subnet group (Créer groupe de sous-réseaux de base de données), définissez ces valeurs dans Subnet group details (Détails de groupe de sous-réseaux) :

   - Nom : `tutorial-db-subnet-group`
   - Description : `Tutorial DB Subnet Group`
   - VPC : `tutorial-vpc (vpc-`*`identifier`*`)`

5. Dans la section Ajouter des sous-réseaux, choisissez les zones de disponibilité et les sous-réseaux.

   Pour ce didacticiel, choisissez `us-west-2a` et `us-west-2b` pour Zones de disponibilité. Ensuite, pour Subnets (Sous-réseaux), choisissez les sous-réseaux du bloc CIDR IPv4 10.0.0.0/24, 10.0.1.0/24 et 10.0.2.0/24.

   > **Note**
   >
   > Si vous avez activé une zone locale, vous pouvez choisir un groupe de zone de disponibilité sur la page Créer un groupe de sous-réseaux DB. Dans ce cas, choisissez Groupe de zone de disponibilité, Zones de disponibilité et Sous-réseaux.

6. Sélectionnez Create.

   Votre nouveau groupe de sous-réseaux DB apparaît dans la liste des groupes de sous-réseaux sur la console RDS. Vous pouvez cliquer sur le groupe de sous-réseaux DB pour afficher les détails,

y compris l'ensemble des sous-réseaux associés au groupe, dans le volet des détails en bas de la fenêtre.

Note

Si vous avez créé ce VPC pour effectuer Didacticiel : Créer un serveur web et une instance de base de données Amazon RDS (p. 109), créez l'instance de base de données en suivant les instructions fournies dans Créez une instance de base de données. (p. 110) .

Quotas et contraintes pour Amazon RDS

Vous trouverez ci-après une description des quotas de ressources et des contraintes d'attribution de noms pour Amazon RDS.

Rubriques

- Quotas dans Amazon RDS (p. 1635)
- Contraintes d'affectation de noms dans Amazon RDS (p. 1636)
- Nombre maximal de connexions à une base de données (p. 1637)
- Limites de taille des fichiers dans Amazon RDS (p. 1638)

Quotas dans Amazon RDS

Chaque compte AWS a des quotas pour chaque région AWS sur le nombre de ressources Amazon RDS pouvant être créées. Une fois qu'un quota de ressource a été atteint, les appels supplémentaires pour créer cette ressource échouent avec une exception.

Le tableau suivant répertorie les ressources et leurs quotas par région AWS.

Ressource	Quota par défaut
Autorisations par groupe de sécurité de base de données	20
Solde de la rafale pour les instances < 1 tébioctet (TiO)	3 000 IOPS
Demandes de copie d'instantané entre régions	5
Instances DB	40
Groupes de sécurité DB	25
Groupes de sous-réseaux DB	50
Abonnements aux événements	20
Rôles IAM par instance de base de données	5
Instantané de base de données manuel	100
Groupes d'options	20
Groupes de paramètres	50
Proxies	20
Réplicas en lecture par principale	5
Instances DB réservées	40
Règles par groupe de sécurité	20
Règles par groupe de sécurité Virtual Private Cloud (VPC)	50 entrants, 50 sortants

Ressource	Quota par défaut
Sous-réseaux par groupe de sous-réseaux	20
Balises par ressource	50
Stockage total pour toutes les instances de base de données	100 téraoctets (To)
Groupes de sécurité VPC	5

Note

Par défaut, vous pouvez avoir jusqu'à 40 instances de bases de données. Les instances de base de données RDS, les instances de base de données Aurora, les instances Amazon Neptune et les instances Amazon DocumentDB sont concernées par ce quota.
Les limitations suivantes s'appliquent aux instances de bases de données Amazon RDS :

- 10 instances de chaque édition SQL Server (Enterprise, Standard, Web et Express) sous le modèle « license-included (licence incluse) »
- 10 instances pour Oracle sous le modèle « license-included (licence incluse) »
- 40 instances pour MySQL, MariaDB ou PostgreSQL
- 40 instances pour Oracle sous le modèle « Réutilisez vos licences »

Si votre application nécessite plus d'instances de base de données, vous pouvez demander des instances de base de données supplémentaires en ouvrant la console Quotas de service. Dans le volet de navigation, choisissez AWS services (Services AWS). Choisissez Amazon Relational Database Service (Amazon RDS), choisissez un quota et suivez les instructions pour demander une augmentation de quota. Pour de plus amples informations, veuillez consulter Demande d'augmentation de quota dans le Guide de l'utilisateur Quotas de service.
Les sauvegardes gérées par AWS Backup sont considérées comme des instantanés de de base de données manuels, mais ne sont pas prises en compte dans le quota d'instantanés de manuels. Pour de plus amples informations sur AWS Backup, veuillez consulter le Manuel du développeur AWS Backup.

Contraintes d'affectation de noms dans Amazon RDS

Le tableau ci-dessous décrit les contraintes d'affectation de noms dans Amazon RDS.

Ressource ou élément	Contraintes
Identificateur d'instance de base de données	L'identificateur a les contraintes de dénomination suivantes : • Doit contenir entre 1 et 63 caractères alphanumériques ou traits d'union. • Le premier caractère doit être une lettre. • Il ne peut pas se terminer par un trait d'union ou contenir deux traits d'union consécutifs. • Doit être unique pour toutes les instance de base de données par compte AWS et par région AWS.

Ressource ou élément	Contraintes
Nom de base de données	Les contraintes de nom des bases de données diffèrent pour chaque moteur de base de données . Pour de plus amples informations, veuillez consulter les paramètres disponibles lors de la création de chaque instance. Note Cette approche ne s'applique pas à SQL Server. Pour SQL Server, vous créez vos bases de données après avoir créé votre instance de base de données.
Nom d'utilisateur principal	Les contraintes relatives à un nom utilisateur maître diffèrent pour chaque moteur de base de données. Pour de plus amples informations, veuillez consulter les paramètres disponibles lors de la création de chaque instance.
Mot de passe principal	Le mot de passe de l'utilisateur principal de la base de données peut contenir tout caractère ASCII imprimable à l'exception de `/`, `"`, `@` ou d'un espace. Les contraintes de longueur du mot de passe principal diffèrent pour chaque moteur de base de données. Pour de plus amples informations, veuillez consulter les paramètres disponibles lors de la création de chaque instance.
Nom de groupe de paramètres de base de données	Ces noms ont les contraintes suivantes : • Ils doivent contenir entre 1 et 255 caractères alphanumériques. • Le premier caractère doit être une lettre. • Les traits d'union sont autorisés, mais le nom ne peut pas se terminer par un trait d'union ni contenir deux traits d'union consécutifs.
Nom du groupe de sous-réseaux DB	Ces noms ont les contraintes suivantes : • Il doivent contenir entre 1 et 255 caractères. • Les caractères alphanumériques, les espaces, les traits d'union, les traits de soulignement et les points sont autorisés.

Nombre maximal de connexions à une base de données

Le nombre maximal de connexions simultanées à une base de données varie selon le type de moteur de base de données et l'allocation de mémoire pour la classe d'instance de base de données. Le nombre maximal de connexions est défini dans le groupe de paramètres associé à l'instance de base de données, à l'exception de Microsoft SQL Server, pour lequel il est défini dans les propriétés du serveur de l'instance de base de données dans SQL Server Management Studio (SSMS).

> **Note**
>
> Pour Oracle, vous définissez le nombre maximal de processus utilisateur, et de sessions utilisateur et système.

Nombre maximal de connexions à la base de données

Moteur de base de données	Paramètre	Valeurs autorisées	Valeur par défaut	Description
MariaDB et MySQL	`max_connections`	1–100000	{DBInstanceClassMemory/12582880}	Nombre de connexions client simultanées autorisées
Oracle	`processes`	80–20000	LEAST({DBInstanceClassMemory/9868951}, 20000)	Processus utilisateur
	`sessions`	100–65535	–	Sessions utilisateur et système
PostgreSQL	`max_connections`	6–8388607	LEAST({DBInstanceClassMemory/9531392}, 5000)	Nombre maximal de connexions simultanées
SQL Server	Nombre maximal de connexions simultanées	0–32767	0 (illimité)	Nombre maximal de connexions simultanées

Note

Il se peut que vous voyiez moins de connexions que le nombre maximal connexions de base de données. Il s'agit ainsi s'éviter les problèmes potentiels de mémoire insuffisante.

Limites de taille des fichiers dans Amazon RDS

Des limites de taille de fichier s'appliquent à certaines instances de base de données Amazon RDS. Pour de plus amples informations, veuillez consulter les limites spécifiques aux moteurs suivantes :

- Limites de taille des fichiers MariaDB dans Amazon RDS (p. 549)
- Limites de taille des fichiers MySQL dans Amazon RDS (p. 898)
- Limites de taille des fichiers Oracle dans Amazon RDS (p. 937)

Dépannage d’Amazon RDS

Utilisez les sections suivantes pour résoudre les problèmes que vous rencontrez avec les instances de base de données Amazon RDS et Aurora.

Rubriques

- Impossible de se connecter à l'instance de base de données Amazon RDS (p. 1639)
- Problèmes de sécurité Amazon RDS (p. 1641)
- Réinitialisation du mot de passe du propriétaire de l'instance de base de données (p. 1642)
- Panne ou redémarrage d'une instance de base de donnéesAmazon RDS (p. 1642)
- Modifications de paramètre de base de données Amazon RDS n'entrant pas en vigueur (p. 1643)
- Manque d'espace de stockage de l'instance de base de données Amazon RDS (p. 1643)
- Capacité d'instance de base de données insuffisante Amazon RDS (p. 1645)
- Amazon RDS Problèmes MySQL et MariaDB (p. 1645)
- Impossible de définir la période de rétention des sauvegardes sur 0 (p. 1652)

Pour de plus amples informations sur le débogage des problèmes à l’aide de l’API Amazon RDS, veuillez consulter Applications de dépannage sur Amazon RDS (p. 1654).

Impossible de se connecter à l'instance de base de données Amazon RDS

Voici des causes courantes empêchant la connexion à une instance de base de données :

- Règles entrantes – Les règles d'accès appliquées par votre pare-feu local et les adresses IP autorisées à accéder à votre instance de base de données peuvent ne pas correspondre. Le problème est probablement lié aux règles entrantes de votre groupe de sécurité.

  Par défaut, les instances de base de données n'autorisent pas l'accès. L'accès est accordé via un groupe de sécurité associé au VPC qui autorise le trafic entrant et sortant de l'instance de base de données. Si nécessaire, ajoutez au groupe de sécurité des règles entrantes et sortantes pour votre situation. Vous pouvez indiquer une adresse IP, une plage d'adresses IP ou un autre groupe de sécurité VPC.

  > **Note**
  >
  > Lorsque vous ajoutez une nouvelle règle entrante, vous pouvez choisir Mon adresse IP pour Source afin d'autoriser l'accès à l'instance de base de données à partir de l'adresse IP détectée dans votre navigateur.

  Pour de plus amples informations sur la configuration des groupes de sécurité, veuillez consulter Créer un groupe de sécurité qui autorise l'accès à votre instance de base de données dans votre VPC (p. 66).

  > **Note**
  >
  > Les connexions client à partir d'adresses IP dans la plage 169.254.0.0/16 ne sont pas autorisées. Il s'agit d'une plage d'adresses IP privées automatiques (APIPA, Automatic Private IP Addressing Range), qui est utilisée pour l'adressage de liens locaux.
- Accessibilité publique – Pour vous connecter à votre instance de base de données depuis l'extérieur du VPC, par exemple en utilisant une application cliente, une adresse IP publique doit lui être attribuée.

Pour rendre l'instance accessible au public, modifiez-la et choisissez Oui sous Public accessibility (Accessibilité publique). Pour de plus amples informations, veuillez consulter Masquer une instance de base de données dans un VPC depuis Internet (p. 1622).

- Port – Le port que vous avez spécifié quand vous avez créé l'instance de base de données ne peut pas être utilisé pour envoyer ou recevoir des communications en raison des restrictions de votre pare-feu local. Pour déterminer si votre réseau autorise l'utilisation du port spécifié pour les communications entrantes et sortantes, vérifiez auprès de votre administrateur réseau.
- Disponibilité – Pour une instance de base de données récemment créée, celle-ci a un état `creating` (création) jusqu'à ce qu'elle soit prête à l'emploi. Lorsque l'état devient `available` (disponible), vous pouvez vous connecter à l'instance de base de données. Selon la taille de votre instance de base de données, vous devez parfois patienter une vingtaine de minutes avant qu'elle ne soit disponible.
- Passerelle Internet – Pour qu'une instance de base de données soit publiquement accessible, les sous-réseaux de son groupe de sous-réseaux de base de données doivent avoir une passerelle Internet.

  Pour configurer une passerelle Internet pour un sous-réseau

  1. Connectez-vous au AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/.
  2. Dans le panneau de navigation, sélectionnez Bases de données, puis sélectionnez le nom de l'instance de base de données.
  3. Dans l'onglet Connectivity & security (Connectivité et sécurité), notez les valeurs de l'ID du VPC sous VPC et de l'ID du sous-réseau sous Sous-réseaux (subnets).
  4. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
  5. Dans le panneau de navigation, choisissez Passerelles Internet. Vérifiez qu'il existe une passerelle Internet attachée à votre VPC. Sinon, choisissez Créer une passerelle Internet pour créer une passerelle Internet. Sélectionnez la passerelle Internet, puis choisissez Attacher au VPC et suivez les instructions pour l'attacher à votre VPC.
  6. Dans le panneau de navigation, sélectionnez Sous-réseaux, puis sélectionnez votre sous-réseau.
  7. Dans l'onglet Table de routage, vérifiez qu'il existe une route avec `0.0.0.0/0` comme destination et la passerelle Internet pour votre VPC comme cible. Si vous vous connectez à votre instance à l'aide de son adresse IPv6, vérifiez qu'il existe une route pour tout le trafic IPv6 (`::/0`) qui pointe vers la passerelle Internet. Sinon, procédez comme suit :

     a. Choisissez l'ID de la table de routage (rtb-xxxxxxxx) pour accéder à cette dernière.

     b. Dans l'onglet Routes, choisissez Edit routes (Modifier les routes). Choisissez Add route (Ajouter une route) et utilisez `0.0.0.0/0` comme destination et la passerelle Internet comme cible. Pour IPv6, choisissez Add route (Ajouter une route) et utilisez `::/0` comme destination et la passerelle Internet comme cible.

     c. Choisissez Save routes (Enregistrer les routes).

  Pour plus d'informations, consultez Utilisation d'une instance de base de données dans un VPC (p. 1620).

Pour les problèmes de connexion spécifiques au moteur, consultez les rubriques suivantes :

- Résolution des problèmes de connexion à votre instance de base de données SQL Server (p. 624)
- Résolution des problèmes de connexion à votre instance de base de données Oracle (p. 968)
- Résolution des problèmes de connexion à votre instance PostgreSQL (p. 1368)
- Maximum de connexions MySQL et MariaDB (p. 1646)

Test d'une connexion à une instance de base de données

Vous pouvez tester votre connexion à une instance de base de données à l'aide des outils courants Linux ou Microsoft Windows.

Depuis un terminal Linux ou Unix, vous pouvez tester la connexion en saisissant les informations suivantes (remplacez *DB-instance-endpoint* par le point de terminaison et *port* par le port de votre instance de base de données).

```
nc -zv DB-instance-endpoint port
```

Par exemple, le code suivant illustre un exemple de commande et la valeur renvoyée.

```
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!
```

Les utilisateurs Windows peuvent utiliser Telnet pour tester la connexion à une instance de base de données. Les actions Telnet ne sont prises en charge que pour le test de la connexion. Si l'opération aboutit, l'action ne retourne aucun message. Si une connexion n'aboutit pas, vous recevez un message d'erreur similaire au message suivant.

```
C:\>telnet sg-postgresql1.c6c8mntfake0.us-west-2.rds.amazonaws.com 819

  Connecting To sg-postgresql1.c6c8mntfake0.us-west-2.rds.amazonaws.com...Could not open
  connection to the host, on port 819: Connect failed
```

Si les actions Telnet aboutissent, votre groupe de sécurité est correctement configuré.

> **Note**
>
> Amazon RDS n'accepte pas le trafic ICMP (Internet Control Message Protocol), y compris ping.

Dépannage des problèmes d'authentification de connexion

Si vous pouvez vous connecter à votre instance de base de données, mais que vous obtenez des erreurs d'authentification, il se peut que vous vouliez réinitialiser le mot de passe utilisateur maître de l'instance de base de données. Vous pouvez modifier l'instance RDS pour ce faire.

Pour de plus amples informations sur la modification d'une instance de base de données, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).

Problèmes de sécurité Amazon RDS

Pour éviter les problèmes de sécurité, n'utilisez jamais votre nom d'utilisateur AWS et votre mot de passe pour un compte utilisateur. Une bonne pratique consiste à utiliser votre compte AWS principal pour créer des utilisateurs AWS Identity and Access Management (IAM) et les attribuer à des comptes utilisateur de base de données. Vous pouvez aussi utiliser votre compte maître pour créer d'autres comptes utilisateur si nécessaire.

Pour plus d'informations sur la création d'utilisateurs IAM, consultez Création d'un utilisateur IAM (p. 62).

Message d'erreur « Échec de l'extraction des attributs du compte. Certaines fonctions de la console sont peut être dégradées. »

Plusieurs raisons peuvent expliquer cette erreur. Cela peut être dû au fait que votre compte ne dispose pas de certaines autorisations ou que votre compte n'a pas été correctement configuré. Si votre compte est nouveau, vous n'avez peut-être pas attendu qu'il soit prêt. S'il s'agit d'un compte existant, il est possible que vos stratégies d'accès ne contiennent pas certaines autorisations permettant d'exécuter certaines actions, comme la création d'une instance de base de données. Pour résoudre le problème, votre administrateur IAM doit fournir les rôles nécessaires à votre compte. Pour de plus amples informations, veuillez consulter la documentation IAM.

Réinitialisation du mot de passe du propriétaire de l'instance de base de données

Si l'accès à votre instance de base de données est verrouillé, vous pouvez vous connecter en tant qu'utilisateur principal. Ensuite, vous pouvez réinitialiser les informations d'identification pour d'autres utilisateurs ou rôles administratifs. Si vous ne parvenez pas à vous connecter en tant qu'utilisateur principal, le propriétaire du compte AWS peut réinitialiser le mot de passe de l'utilisateur principal. Pour de plus amples informations sur les comptes ou rôles administratifs que vous devrez peut-être réinitialiser, veuillez consulter Privilèges du compte utilisateur principal (p. 1605).

Vous pouvez modifier le mot de passe d'une instance de base de données à l'aide de la console Amazon RDS, de la commande modify-db-instance de l'AWS CLI ou de l'opération d'API ModifyDBInstance. Pour plus d'informations sur la modification d'une instance de base de données , consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Panne ou redémarrage d'une instance de base de donnéesAmazon RDS

Une instance de base de données peut connaître une panne au redémarrage. Cela peut également se produire quand l'instance de base de données est placée dans un état qui empêche d'y accéder ou quand la base de données est redémarrée. Un redémarrage peut se produire quand vous redémarrez manuellement votre instance de base de données ou que vous modifiez un paramètre de l'instance de base de données qui nécessite un redémarrage avant que la modification ne puisse prendre effet.

Un redémarrage de l'instance de base de données se produit lorsque vous démarrez un paramètre qui nécessite un redémarrage ou quand vous provoquez manuellement un redémarrage. Un redémarrage peut se produire immédiatement si vous modifiez un paramètre et demandez que la modification prenne effet immédiatement, ou il peut intervenir pendant la fenêtre de maintenance de l'instance de base de données.

Un redémarrage d'instance de base de données se produit immédiatement quand l'une des conditions suivantes est vraie :

- Vous remplacez la période de rétention des sauvegardes pour une instance de base de données de 0 par une valeur différente de zéro, ou d'une valeur différente de zéro par zéro, et définissez Appliquer immédiatement sur la valeur `true` (vrai).

- Vous pouvez modifier la classe d'instance de base de données et Appliquer immédiatement est défini sur la valeur `true` (vrai).
- Vous remplacez le type de stockage Magnetic (Standard) [Magnétique (Standard)] par General Purpose (SSD) [Usage général (SSD)]) ou Provisioned IOPS (SSD) [IOPS dimensionné (SSD)], ou le type Provisioned IOPS (SSD) [IOPS dimensionné (SSD)] ou General Purpose (SSD) [Usage général (SSD)] par Magnetic (Standard) [Magnétique (Standard)].

Un redémarrage d'instance de base de données se produit pendant la fenêtre de maintenance quand l'une des conditions suivantes est vraie :

- Vous remplacez la période de rétention des sauvegardes pour une instance de base de données de 0 par une valeur différente de zéro, ou d'une valeur différente de zéro par zéro, et Appliquer immédiatement est défini sur la valeur `false` (faux).
- Vous pouvez modifier la classe d'instance de base de données et Appliquer immédiatement est défini sur la valeur `false` (vrai).

Lorsque vous modifiez un paramètre statique d'un groupe de paramètres de base de données, la modification prend effet seulement après le redémarrage de l'instance de base de données associée au groupe de paramètres. La modification nécessite un redémarrage manuel. L'instance de base de données n'est pas redémarrée automatiquement pendant la fenêtre de maintenance.

Pour afficher un tableau qui illustre les actions d'une instance de base de données et l'effet de l'application de la valeur Apply Immediately (Appliquer immédiatement), consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Modifications de paramètre de base de données Amazon RDS n'entrant pas en vigueur

Dans certains cas, vous pouvez modifier un paramètre dans un groupe de paramètres de base de données, mais vous ne voyez pas que les modifications prennent effet. Vous devrez alors probablement redémarrer l'instance de base de données associée au groupe de paramètres de base de données. Lorsque vous modifiez un paramètre dynamique, la modification prend effet immédiatement. Lorsque vous modifiez un paramètre statique, la modification ne prend effet que lorsque vous redémarrez l'instance de base de données associée au groupe de paramètres.

Vous pouvez redémarrer une instance de base de données à l'aide de la console RDS ou en appelant explicitement l'opération d'API `RebootDBInstance` (sans basculement, si l'instance de base de données est dans un Multi-AZ deployment). Les critères pour redémarrer l'instance de base de données associée après un changement de paramètre statique contribuent à atténuer le risque d'erreur de configuration d'un paramètre affectant un appel d'API. Par exemple, appeler `ModifyDBInstance` pour changer la classe de l'instance de base de données. Pour de plus amples informations, veuillez consulter Modification de paramètres dans un groupe de paramètres de bases de données (p. 229).

Manque d'espace de stockage de l'instance de base de données Amazon RDS

Si votre instance de base de données ne dispose plus d'un espace de stockage suffisant, il se peut qu'elle ne soit plus disponible. Nous vous recommandons vivement de surveiller en permanence la métrique

`FreeStorageSpace` publiée dans CloudWatch pour vous assurer que votre instance de base de données possède suffisamment d'espace de stockage disponible.

Si votre instance de base de données ne dispose plus d'un stockage suffisant, son état devient `storage-full`. Par exemple, l'appel de l'opération d'API `DescribeDBInstances` pour une instance de base de données qui a consommé la totalité de son stockage produit l'effet suivant.

```
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.clla4j4jgyph.us-east-1.rds.amazonaws.com  3306
us-east-1b  3
 SECGROUP  default  active
 PARAMGRP  default.mysql8.0  in-sync
```

Pour effectuer une récupération à partir de ce scénario, ajoutez plus d'espace de stockage à votre instance à l'aide de l'opération d'API `ModifyDBInstance` ou de la commande suivante de l'AWS CLI.

Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --allocated-storage 60 \
    --apply-immediately
```

Pour 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.clla4j4jgyph.us-east-1.rds.amazonaws.com  3306
us-east-1b  3  60
 SECGROUP  default  active
 PARAMGRP  default.mysql8.0  in-sync
```

Désormais, lorsque vous décrivez votre instance de base de données, vous constatez que son état est `modifying` (modification), ce qui signifie que le stockage est en cours de mise à l'échelle.

```
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.clla4j4jgyph.us-east-1.rds.amazonaws.com
3306  us-east-1b  3  60
 SECGROUP  default  active
 PARAMGRP  default.mysql8.0  in-sync
```

Une fois la mise à l'échelle du stockage terminée, l'état de votre instance de base de données devient `available` (disponible).

```
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.clla4j4jgyph.us-east-1.rds.amazonaws.com  3306
us-east-1b  3
 SECGROUP  default  active
 PARAMGRP  default.mysql8.0  in-sync
```

L'opération `DescribeEvents` vous permet de recevoir des notifications lorsque vous n'avez plus d'espace de stockage disponible. Par exemple, dans ce scénario, si vous appelez `DescribeEvents` après ces opérations, vous observez le résultat suivant.

```
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
```

Capacité d'instance de base de données insuffisante Amazon RDS

L'erreur `InsufficientDBInstanceCapacity` peut être renvoyée lorsque vous essayez de créer ou de modifier une instance de base de données, ou lorsque vous essayez de restaurer une instance de base de données à partir d'un instantané de bases de données. Lorsque cette erreur est renvoyée, les éléments suivants sont les raisons les plus courantes :

- La classe d'instance de base de données spécifique n'est pas disponible dans la zone de disponibilité demandée. Vous pouvez essayer une des actions suivantes pour résoudre le problème :
  - Renouveler la demande avec une classe d'instance de base de données différente.
  - Renouveler la demande avec une zone de disponibilité différente.
  - Renouveler la demande sans spécifier de zone de disponibilité explicite.

  Pour de plus amples informations sur le dépannage de problèmes de capacité d'instance pour Amazon EC2, veuillez consulter Capacité d'instance insuffisante dans le Guide de l'utilisateur Amazon Elastic Compute Cloud.
- L'instance de base de données se trouve sur la plateforme EC2-Classic. Par conséquent, elle n'est pas dans un VPC. Certaines classes d'instance de base de données nécessitent un VPC. Par exemple, vous obtenez cette erreur si vous êtes sur la plateforme EC2-Classic et que vous tentez d'augmenter la capacité en passant à une classe d'instance de base de données nécessitant un VPC. Pour de plus amples informations sur les types d'instance Amazon EC2 qui sont disponibles uniquement dans un VPC, consultez Types d'instance disponibles dans EC2-Classic dans le Guide de l'utilisateur Amazon Elastic Compute Cloud. Pour résoudre le problème, vous pouvez transférer l'instance de base de donnée vers un VPC. Pour plus d'informations, consultez Déplacement vers un VPC d'une instance de base de données n'appartenant pas à un VPC (p. 1627).

Pour plus d'informations sur la modification d'une instance de base de données , consultez Modification d'une instance de base de données Amazon RDS (p. 243).

Amazon RDS Problèmes MySQL et MariaDB

Vous pouvez diagnostiquer et corriger les problèmes des instances de base de données MySQL et MariaDB.

Rubriques

- Maximum de connexions MySQL et MariaDB (p. 1646)
- Diagnostic et résolution du retard entre réplicas en lecture (p. 1646)
- Diagnostic et résolution d'une défaillance de la réplication en lecture MySQL ou MariaDB (p. 1648)
- La création de déclencheurs avec la journalisation binaire activée requiert le privilège SUPER (p. 1649)
- Diagnostic et résolution des défaillances de restauration à un point donné dans le passé (p. 1650)
- Erreur d'arrêt de réplication (p. 1651)
- La création de réplica en lecture échoue ou la réplication s'arrête avec l'erreur irrécupérable 1236 (p. 1651)

Maximum de connexions MySQL et MariaDB

Le nombre maximum de connexions autorisées à une instance de base de données RDS MySQL ou MariaDB est basé sur la quantité de mémoire disponible pour la classe de l'instance de base de données. Une classe d'instance de base de données avec plus de mémoire disponible entraîne un plus grand nombre de connexions disponibles. Pour plus d'informations sur les classes d'instance de base de données, consultez Classes d'instances de base de données (p. 6).

La limite de connexions pour une instance de base de données est définie par défaut au nombre maximum pour la classe de l'instance de base de données. Vous pouvez limiter le nombre de connexions simultanées à toutes les valeurs jusqu'au nombre maximum de connexions autorisées. Utilisez le paramètre `max_connections` dans le groupe de paramètres pour l'instance de base de données. Pour plus d'informations, consultez Nombre maximal de connexions à une base de données (p. 1637) et Utilisation de groupes de paramètres de base de données (p. 225).

Vous pouvez récupérer le nombre maximum de connexions autorisées pour une instance de base de données MySQL ou MariaDB en exécutant la requête suivante.

```
SELECT @@max_connections;
```

Vous pouvez récupérer le nombre maximum de connexions actives pour une instance de base de données MySQL ou MariaDB en exécutant la requête suivante.

```
SHOW STATUS WHERE `variable_name` = 'Threads_connected';
```

Diagnostic et résolution du retard entre réplicas en lecture

Après que vous avez créé un réplica en lecture MySQL ou MariaDB et que le réplica en lecture est disponible, Amazon RDS réplique d'abord les modifications apportées à l'instance de base de données source à partir du moment où l'opération de création du réplica en lecture a été initiée. Durant cette phase, la durée du retard de réplication pour le réplica en lecture est supérieure à 0. Vous pouvez superviser ce retard dans Amazon CloudWatch en affichant la métrique Amazon RDS `ReplicaLag` .

La métrique `ReplicaLag` signale la valeur du champ `Seconds_Behind_Master` de la commande `SHOW SLAVE STATUS` MySQL ou MariaDB. Pour de plus amples informations, veuillez consulter SHOW SLAVE STATUS. Lorsque la métrique `ReplicaLag` atteint 0, le réplica a rattrapé l'instance de bases de données source. Si la métrique `ReplicaLag` retourne -1, la réplication n'est peut être pas active. Pour résoudre une erreur de réplication, consultez Diagnostic et résolution d'une défaillance de la réplication en lecture

MySQL ou MariaDB (p. 1648). Une valeur de -1 pour `ReplicaLag` peut également signifier que la valeur `Seconds_Behind_Master` ne peut pas être déterminée ou qu'elle est `NULL`.

La métrique `ReplicaLag` retourne -1 pendant une panne réseau ou lorsqu'un correctif est appliqué pendant la fenêtre de maintenance. Dans ce cas, attendez que la connexion réseau soit restaurée ou que la fenêtre de maintenance finisse avant de vérifier à nouveau la métrique `ReplicaLag` .

La technologie de réplication en lecture MySQL et MariaDB est asynchrone. Vous pouvez vous attendre à des augmentations occasionnelles de la métrique `BinLogDiskUsage` sur l'instance de base de données source et de la métrique `ReplicaLag` sur le réplica en lecture. Prenez l'exemple d'une situation dans laquelle un volume élevé d'opérations d'écriture sur l'instance de base de données source se produit en parallèle. Au même moment, les opérations d'écriture sur le réplica en lecture sont sérialisées à l'aide d'un seul thread d'E/S. Une telle situation peut entraîner un décalage entre l'instance source et le réplica en lecture.

Pour de plus amples informations sur les réplicas en lecture et MySQL, veuillez consulter Détails d'implémentation de réplication dans la documentation MySQL. Pour de plus amples informations sur les réplicas en lecture et MariaDB, veuillez consulter Présentation de la réplication dans la documentation MariaDB.

Vous pouvez réduire le retard entre les mises à jour d'une instance de base de données source et les mises à jour suivantes du réplica en lecture en procédant comme suit :

- Définissez la classe d'instance de base de données du réplica en lecture de telle sorte que sa taille de stockage soit comparable à celle de l'instance de base de données source.
- Veillez à ce que les paramètres des groupes de paramètres de base de données utilisés par l'instance de base de données source et le réplica en lecture soient compatibles. Pour obtenir plus d'informations et un exemple, reportez-vous à la présentation du paramètre `max_allowed_packet` dans la section suivante.
- Désactivez le cache de requête. Pour les tables modifiées fréquemment, l'utilisation du cache de requête peut augmenter le retard, parce que le cache est verrouillé et souvent actualisé. Si tel est le cas, il se peut que vous constatiez un retard de réplica inférieur si vous désactivez le cache de requête. Vous pouvez désactiver le cache de requête en définissant le paramètre `query_cache_type parameter` avec la valeur 0 dans le groupe de paramètres DB de l'instance de base de données. Pour de plus amples informations sur le cache de requête, veuillez consulter Configuration du pare-feu Windows.
- Préparez le groupe de tampons sur le réplica en lecture pour InnoDB pour MySQL, InnoDB pour MariaDB 10.2 ou version ultérieure, ou XtraDB pour MariaDB 10.1 ou version antérieure. Supposons par exemple que vous disposez d'un ensemble réduit de tables mises à jour fréquemment et que vous utilisez le schéma de table InnoDB ou XtraDB. Dans ce cas, videz ces tables sur le réplica en lecture. Le moteur de base de données analyse alors les lignes des tables du disque et les met en cache dans le groupe de tampons. Cette approche peut réduire le retard de réplica. Voici un exemple.

  Pour Linux, macOS ou Unix :

```
PROMPT> mysqldump \
    -h <endpoint> \
    --port=<port> \
    -u=<username> \
    -p <password> \
    database_name table1 table2 > /dev/null
```

  Pour Windows :

```
PROMPT> mysqldump ^
    -h <endpoint> ^
    --port=<port> ^
    -u=<username> ^
    -p <password> ^
```

```
database_name table1 table2 > /dev/null
```

Diagnostic et résolution d'une défaillance de la réplication en lecture MySQL ou MariaDB

Amazon RDS supervise l'état de réplication de vos réplicas en lecture et met à jour le champ État de la réplication de l'instance du réplica en lecture avec la valeur `Error` si la réplication s'arrête pour une raison quelconque. Vous pouvez passer en revue les détails de l'erreur associée et déclenchée par les moteurs MySQL ou MariaDB, en consultant le champ Erreur de réplication. Des événements indiquant l'état du réplica en lecture sont également générés, y compris RDS-EVENT-0045 (p. 474), RDS-EVENT-0046 (p. 474) et RDS-EVENT-0047 (p. 472). Pour plus d'informations sur les événements et l'abonnement aux événements, consultez Utilisation de la notification d'événement Amazon RDS (p. 467). Si un message d'erreur MySQL est renvoyé, veuillez consulter l'erreur dans la documentation sur les messages d'erreur MySQL. Si un message d'erreur MariaDB est renvoyé, consultez l'erreur dans la documentation sur les messages d'erreur MariaDB.

Voici d'autres situations courantes susceptibles d'entraîner des erreurs de réplication :

- La valeur du paramètre `max_allowed_packet` d'un réplica en lecture est inférieure au paramètre `max_allowed_packet` de l'instance de base de données source.

  Le paramètre `max_allowed_packet` est un paramètre personnalisé que vous pouvez définir dans un groupe de paramètres de base de données. Le paramètre `max_allowed_packet` est utilisé pour spécifier la taille maximale du langage de manipulation de données (DML) qui peut être exécuté sur la base de données. Si la valeur `max_allowed_packet` de l'instance de base de données source est inférieure à la valeur `max_allowed_packet` du réplica en lecture, le processus de réplication peut lever une erreur et arrêter la réplication. L'erreur la plus courante est `packet bigger than 'max_allowed_packet' bytes`. Vous pouvez corriger cette erreur en indiquant à la source et au réplica en lecture d'utiliser des groupes de paramètres de base de données avec les mêmes valeurs du paramètre `max_allowed_packet`.
- Écriture sur les tables d'un réplica en lecture. Si vous créez des index sur un réplica en lecture, le paramètre `read_only` doit être défini sur 0 pour créer les index. Si vous écrivez dans des tables sur le réplica en lecture, cela peut interrompre la réplication.
- Utilisation d'un moteur de stockage non transactionnel tel que MyISAM. Les réplicas en lecture nécessitent un moteur de stockage transactionnel. La réplication est uniquement prise en charge pour les moteurs de stockage suivants : InnoDB pour MySQL, InnoDB pour MariaDB 10.2 ou version ultérieure, ou XtraDB pour MariaDB 10.1 ou version antérieure.

  Pour convertir une table MyISAM en InnoDB, exécutez la commande suivante :

  ```
  alter table <schema>.<table_name> engine=innodb;
  ```
- Utilisation de requêtes non déterministes non sécurisées telles que `SYSDATE()`. Pour de plus amples informations, veuillez consulter Determination of Safe and Unsafe Statements in Binary Logging dans la documentation MySQL.

Les étapes suivantes peuvent vous aider à résoudre votre erreur de réplication :

- Si vous rencontrez une erreur logique et que vous pouvez l'ignorer en toute sécurité, suivez la procédure décrite dans Ignorer une erreur de réplication (p. 881). Votre instance de base de données MySQL ou MariaDB doit exécuter une version incluant la procédure `mysql_rds_skip_repl_error`. Pour plus d'informations, consultez mysql.rds_skip_repl_error (p. 917).
- Si vous rencontrez un problème de position de journal binaire, vous pouvez modifier la position de relecture du réplica avec la commande `mysql_rds_next_master_log`. Votre instance de base de données MySQL ou MariaDB doit exécuter une version prenant en charge la commande

`mysql_rds_next_master_log` afin de pouvoir modifier la position de relecture du réplica. Pour plus d'informations sur la version, consultez mysql.rds_next_master_log (p. 918).

- Si vous rencontrez temporairement un problème de performance en raison d'une charge DML élevée, vous pouvez définir le paramètre `innodb_flush_log_at_trx_commit` avec la valeur 2 dans le groupe de paramètres de base de données du réplica en lecture. Cette action peut aider le réplica en lecture à se rattraper, même si l'atomicité, la cohérence, l'isolation et la durabilité s'en trouvent temporairement réduites.
- Vous pouvez supprimer le réplica en lecture et créer une instance à l'aide du même identifiant d'instance de base de données. Dans ce cas, le point de terminaison reste le même que celui de votre ancien réplica en lecture.

Si une erreur de réplication est corrigée, le champ Replication State (Statut de réplication) prend la valeur replicating (réplication en cours). Pour plus d'informations, consultez Résolution d'un problème de réplica en lecture MySQL (p. 856).

La création de déclencheurs avec la journalisation binaire activée requiert le privilège SUPER

Lors de la création de déclencheurs dans une instance de base de données MySQL ou MariaDB RDS, vous pouvez recevoir l'erreur suivante.

```
"You do not have the SUPER privilege and binary logging is enabled"
```

L'utilisation des déclencheurs lorsque la journalisation binaire est activée nécessite le privilège SUPER, qui est limité pour les instances de base de données MySQL et MariaDB RDS. Vous pouvez créer des déclencheurs lorsque la journalisation binaire est activée sans le privilège SUPER en définissant le paramètre `log_bin_trust_function_creators` avec la valeur true. Pour définir le paramètre `log_bin_trust_function_creators` sur true, créez un groupe de paramètres DB ou modifiez un groupe de paramètres DB existant.

Pour créer un groupe de paramètres DB qui permet de créer des déclencheurs dans votre instance de base de données MySQL ou MariaDB RDS avec la journalisation binaire activée, utilisez les commandes de l'interface de ligne de commande suivantes. Pour modifier un groupe de paramètres existant, commencez par l'étape 2.

Pour créer un groupe de paramètres et autoriser les déclencheurs avec la journalisation binaire activée à l'aide de l'interface de ligne de commande

1. Créez un groupe de paramètres.

   Pour Linux, macOS ou Unix :

   ```
   aws rds create-db-parameter-group \
       --db-parameter-group-name allow-triggers \
       --db-parameter-group-family mysql8.0 \
       --description "parameter group allowing triggers"
   ```

   Pour 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. Modifiez le groupe de paramètres DB pour autoriser les déclencheurs.

Pour Linux, macOS ou 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"
```

Pour 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. Modifiez votre instance de base de données pour utiliser le nouveau groupe de paramètres DB.

   Pour Linux, macOS ou Unix :

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --db-parameter-group-name allow-triggers \
    --apply-immediately
```

   Pour Windows :

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --db-parameter-group-name allow-triggers ^
    --apply-immediately
```

4. Pour que les modifications deviennent effectives, redémarrez manuellement l'instance de base de données.

```
aws rds reboot-db-instance --db-instance-identifier mydbinstance
```

Diagnostic et résolution des défaillances de restauration à un point donné dans le passé

Restauration d'une instance de base de données incluant des tableaux temporaires

Lors d'une tentative de restauration à un instant dans le passé de votre instance de base de données MySQL ou MariaDB, vous pouvez recevoir l'erreur suivante.

```
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.
```

Cette restauration s'appuie à la fois sur les instantanés de sauvegarde et les journaux binaires de MySQL ou MariaDB pour restaurer votre instance de base de données à une date spécifique. Les informations des tables temporaires peuvent ne pas être fiables dans les journaux binaires et provoquer une erreur de restauration à un instant dans le passé. Si vous utilisez des tables temporaires dans votre instance de base de données MySQL ou MariaDB, vous pouvez réduire le risque d'une défaillance d'un instant dans le passé

en effectuant des sauvegardes plus fréquentes. Une telle défaillance est plus à même de se produire entre la création d'une table temporaire et l'instantané de sauvegarde suivant.

Restauration d'une instance de base de données incluant des tableaux en mémoire

Il se peut que vous rencontriez un problème lors de la restauration d'une base de données qui comporte des tables en mémoire. Les tables en mémoire sont vidées lors d'un redémarrage. En conséquence, vos tables en mémoire peuvent être vides après un redémarrage. Lorsque vous utilisez les tables en mémoire, nous vous recommandons de concevoir l'architecture de votre solution de façon à gérer les tables vides en cas de redémarrage. Si vous utilisez des tables en mémoire avec des instances de base de données répliquées, vous devrez peut-être recréer les réplicas en lecture après un redémarrage. Cela peut s'avérer nécessaire si un réplica en lecture redémarre et ne peut pas restaurer les données à partir d'une table en mémoire vide.

Pour plus d'informations sur les sauvegardes et les restaurations à un instant dans le passé, consultez Utilisation des sauvegardes (p. 317) et Restauration d'une instance de base de données à une date spécifiée (p. 365).

Erreur d'arrêt de réplication

Lorsque vous appelez la commande `mysql.rds_skip_repl_error`, vous pouvez recevoir le message d'erreur suivant : `Slave is down or disabled.`

Ce message d'erreur s'affiche car la réplication a été arrêtée et ne peut pas être redémarrée.

Si vous avez besoin d'ignorer un grand nombre d'erreurs, le retard de réplication peut augmenter et dépasser la période de rétention par défaut pour les fichiers journaux binaires. Dans ce cas, vous pouvez rencontrer une erreur irrécupérable due à des fichiers-journaux binaires purgés avant d'avoir été réutilisés sur le réplica. Cette purge entraîne l'arrêt de la réplication et vous ne pouvez plus appeler la commande `mysql.rds_skip_repl_error` pour ignorer les erreurs de réplication.

Vous pouvez atténuer ce problème en augmentant le nombre d'heures pendant lequel les fichiers journaux binaires sont conservés sur votre source de réplication. Une fois que vous avez augmenté le temps de rétention de journaux binaires, vous pouvez redémarrer la réplication et appeler la commande `mysql.rds_skip_repl_error` en fonction des besoins.

Pour définir le temps de rétention du journal binaire, utilisez la procédure mysql.rds_set_configuration (p. 921). Spécifiez un paramètre de configuration des heures de rétention des journaux binaires, ainsi que le nombre d'heures pendant lequel conserver les fichiers journaux binaires sur le cluster DB, 720 heures au plus (30 jours). L'exemple suivant définit la période de rétention des fichiers journaux binaires à 48 heures.

```
CALL mysql.rds_set_configuration('binlog retention hours', 48);
```

La création de réplica en lecture échoue ou la réplication s'arrête avec l'erreur irrécupérable 1236

Après avoir modifié les valeurs de paramètre par défaut pour une instance de base de données MySQL ou MariaDB, vous pouvez rencontrer un des problèmes suivants :

- Vous ne pouvez pas créer un réplica en lecture pour l'instance de base de données.
- La réplication échoue avec `fatal error 1236`.

Certaines valeurs de paramètres par défaut pour les instances de base de données MySQL et MariaDB aident à s'assurer que la base de données est conforme à ACID et que les réplicas en lecture sont sûrs en

cas d'incident. Pour cela, les paramètres s'assurent que chaque validation est entièrement synchronisée en écrivant la transaction dans le journal binaire avant qu'elle ne soit validée. La modification de ces paramètres à partir de leurs valeurs par défaut pour améliorer les performances peut entraîner l'échec de la réplication quand une transaction n'a pas été écrite dans le journal binaire.

Pour résoudre ce problème, définissez les valeurs de paramètres suivantes :

- `sync-binlog = 1`
- `innodb_support_xa = 1`
- `innodb_flush_log_at_trx_commit = 1`

Impossible de définir la période de rétention des sauvegardes sur 0

Plusieurs raisons peuvent vous obliger à définir la période de rétention des sauvegardes sur 0. Par exemple, vous pouvez immédiatement désactiver les sauvegardes automatiques en définissant la période de rétention sur 0.

Dans certains cas, vous pouvez définir la valeur sur 0 et recevoir un message indiquant que la période de rétention doit être comprise entre 1 et 35. Vérifiez alors que vous n'avez pas configuré un réplica en lecture pour l'instance. En effet, les réplicas en lecture requièrent des sauvegardes pour la gestion des journaux des réplicas en lecture, ce qui ne vous permet pas de définir la période de rétention sur 0.

Référence d'Interface de programmation d'application (API) Amazon RDS

En plus de la AWS Management Console et de l'AWS Command Line Interface (AWS CLI), Amazon Relational Database Service (Amazon RDS) fournit également une API. Vous pouvez utiliser l'API pour automatiser les tâches de gestion de vos instances de base de données et d'autres objets dans Amazon RDS.

- Pour obtenir la liste alphabétique des opérations d'API, consultez Actions.
- Pour obtenir la liste alphabétique des types de données, consultez Types de données.
- Pour consulter la liste des paramètres de requête courants, reportez-vous à la page Paramètres courants.
- Pour la description des codes d'erreur, veuillez consulter la page Erreurs courantes.

Pour de plus amples informations sur le AWS CLI, veuillez consulter la AWS Command Line Interface référence pour Amazon RDS.

Rubriques

- Utilisation de l'API Query (p. 1653)
- Applications de dépannage sur Amazon RDS (p. 1654)

Utilisation de l'API Query

Les sections suivantes abordent brièvement l'authentification de la demande et les paramètres utilisés avec l'API Query.

Pour obtenir des informations générales sur le fonctionnement de l'API Query, veuillez consulter Demandes de requête dans le Amazon EC2 API Reference.

Paramètres Query (Requête)

Ces demandes basées sur Query HTTP sont des demandes HTTP qui utilisent le verbe HTTP GET ou POST et un paramètre Query appelé `Action`.

Chaque demande Query doit inclure certains paramètres communs pour gérer l'authentification et la sélection d'une action.

Certaines actions demandent des listes de paramètres. Ces listes sont spécifiées en utilisant la notation `param.`*`n`*. Les valeurs de *`n`* sont des nombres entiers à partir de 1.

Pour de plus amples informations sur les régions et les points de terminaison Amazon RDS, accédez à Amazon Relational Database Service (RDS) dans la section Régions et points de terminaison du manuel Référence générale d'Amazon Web Services.

Authentification de demande Query

Vous pouvez uniquement envoyer des demandes Query via HTTPS, et vous devez inclure une signature dans chaque demande Query. Vous devez utiliser le processus Signature Version 4 ou 2. Pour de plus amples informations, veuillez consulter Processus de signature Signature Version 4 et Processus de signature Signature Version 2.

Applications de dépannage sur Amazon RDS

Amazon RDS fournit des erreurs spécifiques et descriptives pour vous aider à résoudre vos problèmes tout en interagissant avec l'API Amazon RDS.

Rubriques

- Récupération d'erreurs (p. 1654)
- Conseils pour le dépannage (p. 1654)

Pour de plus amples informations sur le dépannage des instances de base de données Amazon RDS, veuillez consulter Dépannage d'Amazon RDS (p. 1639).

Récupération d'erreurs

Généralement, vous souhaitez que votre application vérifie si une demande a généré une erreur avant de passer du temps à traiter les résultats. Le moyen le plus simple de déterminer si une erreur s'est produite est de rechercher un nœud `Error` dans la réponse de l'API Amazon RDS.

La syntaxe XPath fournit une méthode simple pour rechercher la présence d'un nœud `Error` et récupérer le code et le message d'erreur. L'extrait de code suivant utilise Perl et le module XML::XPath pour déterminer si une erreur s'est produite lors d'une demande. Si une erreur s'est produite, le code imprime le premier code et message d'erreur dans la réponse.

```
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"; }
```

Conseils pour le dépannage

Nous vous conseillons d'utiliser les processus suivants pour diagnostiquer et résoudre les problèmes avec l'API Amazon RDS.

- Vérifiez que Amazon RDS fonctionne normalement dans la région AWS que vous ciblez en consultant http://status.aws.amazon.com.
- Vérifiez la structure de votre demande

  Chaque opération Amazon RDS possède une page de référence dans la référence de l'API Amazon RDS. Revérifiez que vous utilisez les paramètres correctement. Afin de vous donner des idées sur les éventuels problèmes, observez les exemples de demandes ou de scénarios utilisateur pour voir s'ils effectuent des opérations similaires.
- Vérifiez le forum

Amazon RDS possède un forum communautaire de développement dans lequel vous pouvez chercher des solutions aux problèmes rencontrés par d'autres. Pour consulter le forum, consultez

https://forums.aws.amazon.com/

Historique du document

Version d'API actuelle : 2014-10-31

Le tableau ci-après décrit les modifications importantes dans chaque édition du Guide de l'utilisateur Amazon RDS après mai 2018. Pour recevoir les notifications des mises à jour de cette documentation, abonnez-vous à un flux RSS.

update-history-change	update-history-description	update-history-date
Prise en charge de MySQL 8.0.21 (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant MySQL version 8.0.21. Pour de plus amples informations, veuillez consulter MySQL sur les versions Amazon RDS.	October 22, 2020
Amazon RDS étend la prise en charge de l'exportation d'instantanés vers Amazon S3 (p. 1656)	Vous pouvez désormais exporter des données d'instantané de base de données vers Amazon S3 dans toutes les régions AWS commerciales. Pour de plus amples informations, veuillez consulter Exportation de données d'instantanés de bases de données vers Amazon S3.	October 22, 2020
Amazon RDS pour PostgreSQL prend en charge les mises à niveau de réplica en lecture (p. 1656)	Avec Amazon RDS pour PostgreSQL, lorsque vous effectuez une mise à niveau de version majeure de l'instance de base de données principale, les réplicas en lecture sont également automatiquement mis à niveau. Pour de plus amples informations, veuillez consulter Mise à niveau du moteur de base de données PostgreSQL.	October 15, 2020
Amazon RDS pour MariaDB, MySQL et PostgreSQL prennent en charge les classes d'instance de base de données Graviton2 (p. 1656)	Vous pouvez désormais utiliser les classes d'instance de base de données Graviton2 db.m6g.x et db.r6g.x pour créer des instances de base de données Amazon RDS exécutant MariaDB, MySQL ou PostgreSQL. Pour de plus amples informations, veuillez consulter Moteurs de base de données pris en charge pour toutes les classes d'instances de base de données disponibles.	October 15, 2020
Amazon RDS pour SQL Server prend en charge les mises	Vous pouvez mettre à niveau vos instances de base de données	October 6, 2020

à niveau vers SQL Server 2019 (p. 1656)	SQL Server vers SQL Server 2019. Pour de plus amples informations, veuillez consulter Mise à niveau du moteur de base de données Microsoft SQL Server.	
Amazon RDS pour Oracle prend en charge la spécification du jeu de caractères national (p. 1656)	Le jeu de caractères national, également appelé jeu de caractères NCHAR, est utilisé dans les types de données `NCHAR`, `NVARCHAR2` et `NCLOB`. Lorsque vous créez une base de données, vous pouvez spécifier AL16UTF16 (par défaut) ou UTF8 comme jeu de caractères NCHAR. Pour de plus amples informations, veuillez consulter Jeux de caractères Oracle pris en charge dans Amazon RDS.	October 2, 2020
Prise en charge de MySQL 5.7.31 (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant MySQL version 5.7.31. Pour de plus amples informations, veuillez consulter MySQL sur les versions Amazon RDS.	October 1, 2020
Amazon RDS for PostgreSQL prend en charge l'exportation de données vers Amazon S3 (p. 1656)	Vous pouvez interroger des données à partir d'une instance de base de données PostgreSQL et les exporter directement vers des fichiers stockés dans un compartiment Amazon S3. Pour de plus amples informations, veuillez consulter la documentation relative à l'exportation de données à partir d'une instance de base de données RDS for PostgreSQL vers Amazon S3.	September 24, 2020
Amazon RDS for PostgreSQL 12.4, 11.9, 10.14, 9.6.19 et 9.5.23 (p. 1656)	Amazon RDS for PostgreSQL prend en charge les versions 12.4, 11.9, 10.14, 9.6.19 et 9.5.23. Pour de plus amples informations, veuillez consulter Versions de bases de données PostgreSQL prises en charge.	September 24, 2020

Amazon RDS pour MySQL 8.0 prend en charge Percona XtraBackup (p. 1656)	Vous pouvez maintenant utiliser Percona XTraBackup pour restaurer une sauvegarde dans une instance de base de données Amazon RDS pour MySQL 8.0. Pour de plus amples informations, veuillez consulter Restauration d'une sauvegarde dans une instance de base de données Amazon RDS MySQL.	September 17, 2020
Amazon RDS for SQL Server prend en charge la sauvegarde et la restauration natives sur les instances de base de données avec les réplicas en lecture (p. 1656)	Vous pouvez restaurer une sauvegarde native SQL Server sur une instance de base de données avec réplicas en lecture configurés. Pour de plus amples informations, veuillez consulter Importation et exportation de bases de données SQL Server.	September 16, 2020
Amazon RDS pour SQL Server prend en charge des fuseaux horaires supplémentaires (p. 1656)	Vous pouvez faire correspondre votre fuseau horaire d'instance de base de données avec le fuseau horaire choisi. Pour de plus amples informations, veuillez consultez Fuseau horaire local pour les instances de bases de données Microsoft SQL Server.	September 11, 2020
Amazon RDS pour PostgreSQL version 13 bêta 3 dans l'environnement en préversion de base de données (p. 1656)	Amazon RDS pour PostgreSQL prend désormais en charge PostgreSQL version 13 bêta 3 dans l'environnement en préversion de base de données Pour de plus amples informations, veuillez consulter PostgreSQL version 13 bêta 3 dans l'environnement en préversion de base de données.	September 9, 2020
RDS for Oracle inclut les mises à jour de RU, RUR et PSU de juillet 2020 (p. 1656)	Des mises à jour du moteur de base de données ont été publiées en juillet 2020 pour Amazon RDS for Oracle. Pour de plus amples informations, veuillez consulter Oracle Database Engine Release Notes (Notes de mise à jour du moteur de base de données Oracle).	August 28, 2020

Amazon RDS pour SQL Server prend en charge l'indicateur de trace 692 (p. 1656)	Vous pouvez désormais utiliser l'indicateur de trace 692 comme paramètre de démarrage à l'aide de groupes de paramètres de base de données. L'activation de cet indicateur de trace désactive les insertions rapides lors du chargement en masse de données dans un segment de mémoire ou un index cluster. Pour de plus amples informations, veuillez consulter la section relative à la désactivation des insertions rapides pendant le chargement en masse.	August 27, 2020
Amazon RDS pour SQL Server prend en charge Microsoft SQL Server 2019 (p. 1656)	Vous pouvez désormais créer des instances de base de données RDS qui utilisent SQL Server 2019. Pour de plus amples informations, veuillez consulter Versions de Microsoft SQL Server sur Amazon RDS.	August 26, 2020
RDS pour Oracle prend en charge la base de données de réplica montée (p. 1656)	Lorsque vous créez ou modifiez un réplica Oracle, vous pouvez le placer en mode monté. Étant donné que la base de données de réplica n'accepte pas les connexions utilisateur, elle ne peut pas servir de charge de travail en lecture seule. Le réplica monté supprime les fichiers de journalisation archivés après leur application. L'utilisation principale des réplicas montés est la reprise après sinistre interrégion. Pour de plus amples informations, veuillez consulter Généralités sur les réplicas Oracle.	August 13, 2020
RDS pour Oracle planifie la mise à niveau des instances 1g SE1 LI (p. 1656)	Le 1er novembre 2020, nous prévoyons de commencer à mettre à niveau automatiquement les instances Oracle 11g SE1 License Included (LI) vers Oracle 19c pour Amazon RDS for Oracle. La dernière mise à jour (RU) Oracle sera installée sur toutes les instances 11g, y compris les instances réservées. Pour de plus amples informations, veuillez consulter Preparing for the Automatic Upgrade of Oracle 11g SE1.	July 31, 2020

Amazon RDS prend en charge les nouvelles classes d'instance de base de données Graviton2 dans la version préliminaire pour PostgreSQL et MySQL (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant PostgreSQL ou MySQL qui utilisent les classes d'instance de base de données db.m6g.x et db.r6g.x. Pour de plus amples informations, veuillez consulter Moteurs de base de données pris en charge pour toutes les classes d'instances de base de données disponibles.	July 30, 2020
RDS for Oracle prend en charge APEX 20.1v1 (p. 1656)	Vous pouvez utiliser APEX 20.1v1 avec toutes les versions prises en charge d'Oracle Database. Pour de plus amples informations, veuillez consulter Oracle Application Express.	July 28, 2020
Prise en charge de MySQL 8.0.20 (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant MySQL version 8.0.20. Pour de plus amples informations, veuillez consulter MySQL sur les versions Amazon RDS.	July 23, 2020
Amazon RDS pour MariaDB et MySQL prennent en charge les nouvelles classes d'instance de base de données (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant MariaDB et MySQL qui utilisent les classes d'instance de base de données db.m5.16xlarge, db.m5.8xlarge, db.r5.16xlarge et db.r5.8xlarge. Pour de plus amples informations, veuillez consulter Moteurs de base de données pris en charge pour toutes les classes d'instances de base de données disponibles.	July 23, 2020
RDS pour SQL Server prend en charge la désactivation des anciennes versions de TLS et les chiffrements (p. 1656)	Vous pouvez activer et désactiver certains protocoles de sécurité et chiffrements. Pour de plus amples informations, veuillez consulter Configuration des protocoles et des chiffrements de sécurité.	July 21, 2020
RDS prend en charge Oracle Spatial sur SE2 (p. 1656)	Vous pouvez utiliser Oracle Spatial dans Standard Edition 2 (SE2) pour toutes les versions de 12.2, 18c et 19c. Pour de plus amples informations, veuillez consulter Oracle Spatial.	July 9, 2020

Amazon RDS prend en charge AWS PrivateLink (p. 1656)	Amazon RDS prend désormais en charge la création de points de terminaison Amazon VPC pour les appels d'API Amazon RDS afin de conserver le trafic entre les applications et Amazon RDS dans le réseau AWS. Pour de plus amples informations, veuillez consulter la section relative à Amazon RDS et points de terminaison de VPC d'interface (AWS PrivateLink).	July 9, 2020
Amazon RDS for PostgreSQL versions 9.4.x sont obsolètes (p. 1656)	Amazon RDS for PostgreSQL ne prend plus en charge les versions 9.4.x. Pour connaître les versions prises en charge, veuillez consulter Versions de base de données PostgreSQL prises en charge.	July 8, 2020
Prise en charge de MariaDB 10.3.23 et 10.4.13 (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant MariaDB version 10.3.23 et 10.4.13. Pour de plus amples informations, veuillez consulter MariaDB sur les versions Amazon RDS.	July 6, 2020
Amazon RDS sur AWS Outposts (p. 1656)	Vous pouvez créer des instances de base de données Amazon RDS sur AWS Outposts. Pour de plus amples informations, veuillez consulter Utilisation d'Amazon RDS sur AWS Outposts.	July 6, 2020
Amazon RDS for Oracle crée automatiquement les fichiers d'inventaire (p. 1656)	Pour ouvrir des demandes de service pour les clients BYOL, le support Oracle demande les fichiers d'inventaire générés par Opatch. Amazon RDS for Oracle crée automatiquement des fichiers d'inventaire toutes les heures dans le répertoire BDUMP. Pour de plus amples informations, veuillez consulter Accès aux fichiers Opatch.	July 6, 2020
Prise en charge de MySQL 5.7.30 et 5.6.48 (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant MySQL versions 5.7.30 et 5.6.48. Pour de plus amples informations, veuillez consulter MySQL sur les versions Amazon RDS.	June 25, 2020

Amazon RDS pour Oracle prend en charge ADRCI (p. 1656)	L'utilitaire ADRCI (Automatic Diagnostic Repository Command Interpreter) est un outil de ligne de commande Oracle qui vous permet de gérer les données de diagnostic. En utilisant les fonctions du package Amazon RDS `rdsadmin_adrci_util`, vous pouvez répertorier et compiler les problèmes et les incidents, et afficher les fichiers de suivi. Pour de plus amples informations, veuillez consulter Tâches de diagnostic communes DBA pour les instances de bases de données Oracle.	June 17, 2020
Amazon RDS for PostgreSQL prend en charge PostgreSQL 12.3 (p. 1656)	Amazon RDS for PostgreSQL prend en charge la version 12.3 Pour de plus amples informations, veuillez consulter Versions de bases de données PostgreSQL prises en charge.	June 17, 2020
Prise en charge de MySQL 8.0.19 (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant MySQL version 8.0.19. Pour de plus amples informations, veuillez consulter MySQL sur les versions Amazon RDS.	June 2, 2020
MySQL 8.0 prend en charge les noms de table en minuscules (p. 1656)	Vous pouvez désormais définir le paramètre `lower_case_table_names` sur `1` pour les instances de base de données Amazon RDS exécutant MySQL version 8.0.19 et versions 8.0 supérieures. Pour de plus amples informations, veuillez consulter Exceptions des paramètres MySQL pour les instances de base de données Amazon RDS.	June 2, 2020

Amazon RDS pour Microsoft SQL Server prend en charge SQL Server Integration Services (SSIS) (p. 1656)	SSIS est une plateforme d'intégration de données et d'applications de flux de travail. Vous pouvez activer SSIS sur des instances de base de données existantes ou nouvelles. Il est installé sur la même instance de base de données que votre moteur de base de données. Pour de plus amples informations, veuillez consulter Prise en charge de SQL Server Integration Services dans SQL Server.	May 19, 2020
Amazon RDS for Microsoft SQL Server prend en charge l'intégration S3 sur les instances Multi-AZ (p. 1656)	Vous pouvez désormais utiliser Amazon S3 avec des fonctionnalités SQL Server telles que l'insertion en bloc sur des instances de base de données Multi-AZ. Pour de plus amples informations, veuillez consulter Intégration d'une instance de base de données Amazon RDS pour SQL Server avec Amazon S3.	May 15, 2020
Amazon RDS for Microsoft SQL Server prend en charge SQL Server Reporting Services (SSRS) (p. 1656)	SSRS est une application basée sur un serveur et utilisée pour la génération et la diffusion de rapports. Vous pouvez activer SSRS sur des instances de base de données existantes ou nouvelles. Il est installé sur la même instance de base de données que votre moteur de base de données. Pour de plus amples informations, veuillez consulter Support for SQL Server Reporting Services in SQL Server.	May 15, 2020
RU, RUR et PSU Amazon RDS for Oracle (avril 2020) (p. 1656)	Des mises à jour du moteur de base de données ont été publiées en avril 2020 pour Amazon RDS for Oracle. Pour de plus amples informations, veuillez consulter Oracle Database Engine Release Notes (Notes de mise à jour du moteur de base de données Oracle).	May 13, 2020

Amazon RDS for Oracle prend en charge la purge de la corbeille (p. 1656)	La procédure `rdsadmin.rdsadmin_util.purge_dba_recyclebin` purge la corbeille. Pour de plus amples informations, veuillez consulter Purging the Recycle Bin.	May 13, 2020
Amazon RDS for Oracle améliore la facilité de gestion d'Automatic Workload Repository (AWR) (p. 1656)	Les procédures `rdsadmin.rdsadmin_diagnostic_util` génèrent des rapports AWR et extraient des données AWR dans des fichiers de vidage. Pour de plus amples informations, veuillez consulter Generating Performance Reports with Automatic Workload Repository (AWR).	May 13, 2020
Amazon RDS for Microsoft SQL Server prend en charge Microsoft Distributed Transaction Coordinator (MSDTC) (p. 1656)	Amazon RDS for SQL Server prend en charge les transactions distribuées entre les hôtes. Pour de plus amples informations, veuillez consulter Support for Microsoft Distributed Transaction Coordinator in SQL Server.	May 4, 2020
Amazon RDS pour PostgreSQL versions 11.7, 10.12, 9.6.17 et 9.5.21 (p. 1656)	Amazon RDS pour PostgreSQL prend en charge les versions 11.7, 10.12, 9.6.17 et 9.5.21. Pour de plus amples informations, veuillez consulter Versions de bases de données PostgreSQL prises en charge.	April 28, 2020
Amazon RDS pour Microsoft SQL Server prend en charge les nouvelles versions (p. 1656)	Vous pouvez maintenant créer des instances de base de données Amazon RDS exécutant SQL Server versions 2017 CU19 14.00.3281.6, 2016 SP2 CU11 13.00.5598.27, 2014 SP3 CU4 12.00.6329.1 et 2012 SP4 GDR 11.0.7493.4 pour toutes les éditions. Pour de plus amples informations, veuillez consulter Versions de Microsoft SQL Server sur Amazon RDS.	April 28, 2020
Amazon RDS disponible dans la région Région Europe (Milan) (p. 1656)	Amazon RDS est désormais disponible dans la région Région Europe (Milan). Pour de plus amples informations, veuillez consulter Régions et zones de disponibilité.	April 28, 2020

Amazon RDS prend en charge les zones locales (p. 1656)	Vous pouvez désormais lancer des instances de base de données dans un sous-réseau de zone locale. Pour de plus amples informations, veuillez consulter Régions, zones de disponibilité et zones locales.	April 23, 2020
Amazon RDS disponible dans la région Région Afrique (Le Cap) (p. 1656)	Amazon RDS est désormais disponible dans la région Région Afrique (Le Cap). Pour de plus amples informations, veuillez consulter Régions et zones de disponibilité.	April 22, 2020
Amazon RDS pour Microsoft SQL Server prend en charge SQL Server Analysis Services (SSAS) (p. 1656)	SSAS est un outil de traitement analytique en ligne (OLAP) et d'exploration de données installé dans SQL Server. Vous pouvez activer SSAS sur des instances de base de données existantes ou nouvelles. Il est installé sur la même instance de base de données que votre moteur de base de données. Pour plus d'informations, consultez Prise en charge de SQL Server Analysis Services dans SQL Server.	April 17, 2020
Proxy Amazon RDS pour PostgreSQL (p. 1656)	Le proxy Amazon RDS est désormais disponible pour PostgreSQL. Vous pouvez utiliser le proxy RDS pour réduire la surcharge de connexions sur votre instance de base de données ainsi que le risque d'erreurs liées à un trop grand nombre de connexions. Le proxy RDS est actuellement disponible en version préliminaire pour PostgreSQL. Pour de plus amples informations, veuillez consulter Gestion des connexions avec le proxy Amazon RDS (version préliminaire).	April 8, 2020
Amazon RDS pour Oracle prend en charge Oracle APEX version 19.2.v1 (p. 1656)	Amazon RDS pour Oracle prend désormais en charge Oracle Application Express (APEX) version 19.2.v1. Pour de plus amples informations, veuillez consulter Oracle Application Express.	April 8, 2020

Amazon RDS pour MariaDB prend en charge une nouvelle version majeure (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS qui exécutent MariaDB version 10.4. Pour de plus amples informations, veuillez consulter MariaDB sur les versions Amazon RDS.	April 6, 2020
Amazon RDS Performance Insights est disponible pour Amazon RDS for MariaDB 10.4 (p. 1656)	Amazon RDS Performance Insights est désormais disponible pour Amazon RDS for MariaDB version 10.4.8 et versions 10.4 ultérieures. Pour de plus amples informations, veuillez consulter Utilisation d'Amazon RDS Performance Insights.	April 6, 2020
Amazon RDS for PostgreSQL versions 9.3.x sont obsolètes (p. 1656)	Amazon RDS pour PostgreSQL ne prend plus en charge les versions 9.3.x. Pour connaître les versions prises en charge, veuillez consulter Versions de base de données PostgreSQL prises en charge.	April 3, 2020
Amazon RDS for Microsoft SQL Server prend en charge les réplicas en lecture (p. 1656)	Vous pouvez désormais créer des réplicas en lecture pour les instances de base de données SQL Server. Pour de plus amples informations, veuillez consulter Utilisation des réplicas en lecture.	April 3, 2020
Amazon RDS for Microsoft SQL Server prend en charge les sauvegardes dans plusieurs fichiers (p. 1656)	Vous pouvez désormais sauvegarder des bases de données dans plusieurs fichiers à l'aide de la fonction de sauvegarde et de restauration natives de SQL Server. Pour de plus amples informations, veuillez consulter Sauvegarde d'une base de données.	April 2, 2020
Amazon RDS for PostgreSQL prend en charge PostgreSQL 12.2 (p. 1656)	Amazon RDS for PostgreSQL prend en charge la version 12.2 Pour de plus amples informations, veuillez consulter Versions de bases de données PostgreSQL prises en charge.	March 31, 2020

Intégration de Amazon RDS for Oracle à AWS License Manager (p. 1656)	Amazon RDS for Oracle est désormais intégré à AWS License Manager. Si vous utilisez le modèle Réutilisez vos licences, l'intégration à AWS License Manager facilite la surveillance de l'utilisation de votre licence Oracle au sein de votre organisation. Pour de plus amples informations, veuillez consulter Intégration à AWS License Manager.	March 23, 2020
Prise en charge de 64 Tio sur les instances db.r5 dans Amazon RDS pour MariaDB et MySQL (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS pour MariaDB et MySQL qui utilisent la classe d'instance de base de données db.r5 avec une capacité maximale de stockage de 64 Tio. Pour de plus amples informations, veuillez consulter Autres facteurs ayant un impact sur les performances de stockage.	March 18, 2020
Prise en charge de MySQL 8.0.17 (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant MySQL version 8.0.17. Pour de plus amples informations, veuillez consulter MySQL sur les versions Amazon RDS.	March 10, 2020
Amazon RDS Performance Insights est disponible pour Amazon RDS for MySQL 8.0 (p. 1656)	Amazon RDS Performance Insights est désormais disponible pour Amazon RDS for MySQL version 8.0.17 et versions 8.0 ultérieures. Pour de plus amples informations, veuillez consulter Utilisation d'Amazon RDS Performance Insights.	March 10, 2020
Prise en charge de MySQL 5.6.46 (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant MySQL version 5.6.46. Pour de plus amples informations, veuillez consulter MySQL sur les versions Amazon RDS.	February 28, 2020

Amazon RDS Performance Insights est disponible pour Amazon RDS for MariaDB 10.3 (p. 1656)	Amazon RDS Performance Insights est désormais disponible pour Amazon RDS for MariaDB version 10.3.13 et versions 10.3 ultérieures. Pour de plus amples informations, veuillez consulter Utilisation d'Amazon RDS Performance Insights.	February 26, 2020
Prise en charge de MySQL 5.7.28 (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant MySQL version 5.7.28. Pour de plus amples informations, veuillez consulter MySQL sur les versions Amazon RDS.	February 20, 2020
Prise en charge de MariaDB 10.3.20 (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant MariaDB version 10.3.20. Pour de plus amples informations, veuillez consulter MariaDB sur les versions Amazon RDS.	February 20, 2020
Mises à jour RU, RUR et PSU pour Amazon RDS for Oracle en janvier 2020 (p. 1656)	Des mises à jour du moteur de base de données ont été publiées en janvier 2020 pour Amazon RDS for Oracle. Pour de plus amples informations, veuillez consulter Oracle Database Engine Release Notes (Notes de mise à jour du moteur de base de données Oracle).	February 20, 2020
Amazon RDS for Microsoft SQL Server prend en charge une nouvelle classe d'instance de base de données (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant SQL Server qui utilisent la classe d'instance de base de données db.z1d. Pour de plus amples informations, veuillez consulter Prise en charge des classes d'instances de bases de données pour Microsoft SQL Server.	February 19, 2020
Prise en charge des domaines Active Directory entre comptes et VPC dans Amazon RDS SQL Server (p. 1656)	Amazon RDS for Microsoft SQL Server prend désormais en charge l'association d'instances de base de données avec des domaines Active Directory appartenant à différents comptes et VPC. Pour de plus amples informations, veuillez consulter Utilisation de l'authentification Windows avec une instance de base de données Microsoft SQL Server.	February 13, 2020

Option OLAP d'Oracle (p. 1656)	Amazon RDS for Oracle prend désormais en charge l'option OLAP (Online Analytical Processing) pour les instances de base de données Oracle. Vous pouvez utiliser Oracle OLAP pour analyser de grandes quantités de données en créant des objets et des cubes dimensionnels conformément à la norme OLAP. Pour de plus amples informations, veuillez consulter Option OLAP d'Oracle.	February 13, 2020
Prise en charge de FIPS 140-2 pour Oracle (p. 1656)	Amazon RDS for Oracle prend en charge la publication Federal Information Processing Standard 140-2 (FIPS 140-2) pour les connexions SSL/TLS. Pour de plus amples informations, veuillez consulter Prise en charge de FIPS.	February 11, 2020
Amazon RDS for PostgreSQL prend en charge de nouvelles versions (p. 1656)	Amazon RDS for PostgreSQL prend en charge les versions 11.6, 10.11, 9.6.16, 9.5.20 et 9.4.25. Pour de plus amples informations, veuillez consulter Versions de bases de données PostgreSQL prises en charge.	February 11, 2020
Amazon RDS for PostgreSQL prend en charge de nouvelles classes d'instance de base de données (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant PostgreSQL qui utilisent les classes d'instance de base de données db.m5.16xlarge, db.m5.8xlarge, db.r5.16xlarge et db.r5.8xlarge. Pour de plus amples informations, veuillez consulter Moteurs de base de données pris en charge pour toutes les classes d'instances de base de données disponibles.	February 11, 2020
L'analyse des performances prend en charge l'analyse statistique de l'exécution des requêtes MariaDB et MySQL. (p. 1656)	Il est désormais possible d'analyser les statistiques des requêtes en cours d'exécution à l'aide de l'analyse des performances pour les instances de base de données MariaDB et MySQL. Pour de plus amples informations, veuillez consulter Analyse des statistiques pour les requêtes en cours d'exécution.	February 4, 2020

Prise en charge de l'exportation des données d'instantanés de bases de données vers Amazon S3 pour MariaDB, MySQL et PostgreSQL (p. 1656)	Amazon RDS prend en charge l'exportation des données d'instantanés de bases de données vers Amazon S3 pour MariaDB, MySQL et PostgreSQL. Pour de plus amples informations, veuillez consulter Exportation de données d'instantanés de bases de données vers Amazon S3.	January 23, 2020
Amazon RDS for MySQL prend en charge l'authentification Kerberos (p. 1656)	Vous pouvez désormais utiliser l'authentification Kerberos pour authentifier les utilisateurs lorsqu'ils se connectent à vos instances de base de données Amazon RDS for MySQL. Pour de plus amples informations, veuillez consulter Utilisation de l'authentification Kerberos pour MySQL.	January 21, 2020
Mise à jour (RU) d'octobre 2019 Amazon RDS for Oracle et révision de mise à jour (RUR) pour Oracle 19c (p. 1656)	Amazon RDS for Oracle a publié des mises à jour du moteur de base de données en octobre 2019 pour Oracle 19c. Pour de plus amples informations, veuillez consulter Oracle Database Engine Release Notes (Notes de mise à jour du moteur de base de données Oracle).	January 9, 2020
L'Analyse des performances Amazon RDS prend en charge l'affichage de texte SQL supplémentaire pour Amazon RDS for Microsoft SQL Server (p. 1656)	L'Analyse des performances Amazon RDS prend désormais en charge l'affichage de texte SQL supplémentaire dans le tableau de bord Analyse des performances pour les instances de base de données Amazon RDS for Microsoft SQL Server. Pour de plus amples informations, veuillez consulter Affichage de texte SQL supplémentaire sur le tableau de bord de Performance Insights.	December 17, 2019

Proxy Amazon RDS (p. 1656)	Vous pouvez réduire la surcharge de gestion des connexions sur votre cluster et réduire le risque d'erreurs liées au « nombre de connexions trop élevé » à l'aide du proxy Amazon RDS. Vous associez chaque proxy à une instance de base de données RDS ou un cluster de base de données Aurora. Ensuite, vous utilisez le point de terminaison du proxy dans la chaîne de connexion de votre application. Le proxy Amazon RDS est actuellement en version préliminaire publique. Il prend en charge le moteur de base de données RDS MySQL. Pour de plus amples informations, veuillez consulter Gestion des connexions avec le proxy Amazon RDS (version préliminaire).	December 3, 2019
Amazon RDS sur AWS Outposts (version préliminaire) (p. 1656)	Avec Amazon RDS sur AWS Outposts, vous pouvez créer des bases de données relationnelles gérées par AWS dans vos centres de données sur site. RDS sur outposts vous permet d'exécuter des bases de données RDS sur AWS Outposts. Pour de plus amples informations, veuillez consulter Amazon RDS sur AWS Outposts (version préliminaire).	December 3, 2019
Amazon RDS for Oracle prend en charge les réplicas en lecture entre régions (p. 1656)	Amazon RDS for Oracle prend désormais en charge les réplicas en lecture entre régions avec Active Data Guard. Pour de plus amples informations, veuillez consulter Utilisation des réplicas en lecture et Utilisation des réplicas en lecture Oracle.	November 26, 2019
L'analyse des performances prend en charge l'analyse statistique de l'exécution de requêtes Oracle. (p. 1656)	Il est désormais possible d'analyser les statistiques des requêtes en cours d'exécution à l'aide de l'analyse des performances pour les instances de bases de données Oracle. Pour de plus amples informations, veuillez consulter Analyse des statistiques pour les requêtes en cours d'exécution.	November 25, 2019

Amazon RDS pour Microsoft SQL Server prend en charge de nouvelles classes d'instances de bases de données (p. 1656)	Vous pouvez désormais créer des instances de bases de données Amazon RDS exécutant SQL Server qui utilisent les classes d'instances de bases de données db.x1e et db.x1. Pour de plus amples informations, veuillez consulter Prise en charge des classes d'instances de bases de données pour Microsoft SQL Server.	November 25, 2019
Amazon RDS pour Microsoft SQL Server prend en charge les restaurations différentielles et de journaux (p. 1656)	Vous pouvez restaurer des sauvegardes différentielles et des journaux à l'aide de la sauvegarde et de la restauration natives SQL Server. Pour de plus amples informations, veuillez consulter Utilisation de la sauvegarde et de la restauration natives.	November 25, 2019
Amazon RDS pour Microsoft SQL Server prend en charge la publication des journaux dans CloudWatch Logs (p. 1656)	Vous pouvez configurer votre instance de base de données Amazon RDS SQL Server pour qu'elle publie les événements de journaux directement dans Amazon CloudWatch Logs. Pour de plus amples informations, veuillez consulter Publication de journaux SQL Server dans Amazon CloudWatch Logs.	November 25, 2019
Fonction multi-AZ prise en charge sur Amazon RDS pour Microsoft SQL Server dans les nouvelles régions (p. 1656)	La fonction multi-AZ sur SQL Server est désormais disponible dans les régions : Chine, Moyen-Orient (Bahreïn) et Europe (Stockholm). Pour de plus amples informations, veuillez consulter Déploiements multi-AZ pour Microsoft SQL Server.	November 22, 2019
Amazon RDS pour Microsoft SQL Server prend désormais en charge l'insertion en bloc et l'intégration S3 (p. 1656)	Vous pouvez transférer des fichiers entre une instance de base de données SQL Server et un compartiment Amazon S3. Ensuite, vous pouvez utiliser Amazon S3 avec des fonctionnalités SQL Server, telles que l'insertion en bloc. Pour de plus amples informations, veuillez consulter Intégration d'une instance de base de données Amazon RDS pour SQL Server avec Amazon S3.	November 21, 2019

Versions RU, RUR et PSU d'octobre 2019 pour Amazon RDS pour Oracle (p. 1656)	Des mises à jour du moteur de base de données ont été publiées en octobre 2019 pour Amazon RDS pour Oracle. Pour de plus amples informations, veuillez consulter Oracle Database Engine Release Notes (Notes de mise à jour du moteur de base de données Oracle).	November 19, 2019
Compteurs d'analyse des performances pour Amazon RDS pour Microsoft SQL Server (p. 1656)	Vous pouvez désormais ajouter des compteurs de performances à vos graphiques d'analyse des performances pour les instances de bases de données Microsoft SQL Server. Pour de plus amples informations, veuillez consulter Compteurs d'analyse des performances pour Amazon RDS for Microsoft SQL Server.	November 12, 2019
Amazon RDS pour Microsoft SQL Server prend en charge de nouvelles tailles de classes d'instances de bases de données (p. 1656)	Vous pouvez désormais créer des instances de bases de données Amazon RDS exécutant SQL Server qui utilisent les tailles d'instances 8xlarge et 16xlarge pour les classes d'instances de bases de données db.m5 et db.r5. Les tailles d'instance « small » à 2xlarge sont désormais disponibles pour la classe d'instance db.t3. Pour de plus amples informations, veuillez consulter Prise en charge des classes d'instances de bases de données pour Microsoft SQL Server.	November 11, 2019
Prise en charge pour les mises à niveau d'instantanés PostgreSQL (p. 1656)	Si vous avez des instantanés de bases de données manuels existants de vos instances de bases de données Amazon RDS PostgreSQL, vous pouvez désormais les mettre à niveau vers une version ultérieure du moteur de base de données PostgreSQL. Pour de plus amples informations, veuillez consulter Mise à niveau d'un instantané de base de données PostgreSQL.	November 7, 2019

Amazon RDS pour Oracle prend en charge une nouvelle version majeure (p. 1656)	Vous pouvez désormais créer des instances de bases de données Amazon RDS exécutant Oracle version 19.0. Pour de plus amples informations, veuillez consulter Oracle 19c avec Amazon RDS.	November 7, 2019
Amazon RDS pour PostgreSQL version 12.0 dans l'environnement en préversion de base de données (p. 1656)	Amazon RDS pour PostgreSQL prend désormais en charge PostgreSQL version 12.0 dans l'environnement en préversion de base de données. Pour de plus amples informations, veuillez consulter PostgreSQL version 12.0 dans l'environnement en préversion de base de données.	November 1, 2019
Amazon RDS for PostgreSQL prend en charge l'authentification Kerberos (p. 1656)	Vous pouvez désormais utiliser l'authentification Kerberos pour authentifier les utilisateurs lorsqu'ils se connectent à votre instance de base de données Amazon RDS exécutant PostgreSQL. Pour de plus amples informations, veuillez consulter Utilisation de l'authentification Kerberos avec Amazon RDS pour PostgreSQL.	October 28, 2019
Tâches de base de données OEM Management Agent pour les instances de base de données Oracle (p. 1656)	Les instances de base de données Amazon RDS pour Oracle prennent désormais en charge les procédures d'appel de certaines commandes EMCTL sur Management Agent. Pour de plus amples informations, veuillez consulter Tâches de base de données de l'agent OEM.	October 24, 2019
Amazon RDS pour PostgreSQL versions 11.5, 10.10, 9.6.15, 9.5.19 et 9.4.24. (p. 1656)	Amazon RDS pour PostgreSQL prend en charge les versions 11.5, 10.10, 9.6.15, 9.5.19 et 9.4.24. Pour de plus amples informations, veuillez consulter Versions de bases de données PostgreSQL prises en charge.	October 8, 2019

Amazon RDS pour PostgreSQL prend en charge les bases de données transportables PostgreSQL (p. 1656)	Les bases de données transportables PostgreSQL offrent une méthode extrêmement rapide de migration d'une base de données RDS PostgreSQL entre deux instances de base de données. Pour de plus amples informations, veuillez consulter Transport de bases de données PostgreSQL entre des instances de base de données.	October 8, 2019
Amazon RDS for Oracle prend en charge l'authentification Kerberos (p. 1656)	Vous pouvez désormais utiliser l'authentification Kerberos pour authentifier les utilisateurs lorsqu'ils se connectent à votre instance de base de données Amazon RDS qui exécute Oracle. Pour de plus amples informations, veuillez consulter Utilisation de l'authentification Kerberos avec Amazon RDS for Oracle.	September 30, 2019
Amazon RDS pour PostgreSQL version 12 bêta 3 dans l'environnement en préversion de base de données (p. 1656)	Amazon RDS pour PostgreSQL prend désormais en charge PostgreSQL version 12 bêta 3 dans l'environnement en préversion de base de données. Pour plus d'informations, consultez PostgreSQL version 12 bêta 3 sur Amazon RDS dans l'environnement en préversion de base de données.	August 28, 2019
Prise en charge de MySQL 8.0.16 (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant MySQL version 8.0.16. Pour de plus amples informations, veuillez consulter MySQL sur les versions Amazon RDS.	August 19, 2019
Amazon RDS pour Oracle prend en charge une nouvelle version majeure (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant Oracle version 18.0. Pour plus d'informations, consultez Oracle 18c avec Amazon RDS.	August 15, 2019

Amazon RDS pour Oracle Juillet 2019 RU, RUR et PSU (p. 1656)	Amazon RDS pour Oracle a lancé une version de moteur de base de données 12.2.0.1.ru-2019-07.rur-2019-07.r1 pour prendre en charge les versions Release Update (RU) et Release Update Revision (RUR) de juillet 2019. Amazon RDS pour Oracle a également lancé les versions de moteur de base de données 12.1.0.2.v17 et 11.2.0.4.v21 pour prendre en charge la mise à jour Oracle Database Patch Set Update (PSU) de juillet 2019. Pour de plus amples informations, veuillez consulter Oracle Database Engine Release Notes (Notes de mise à jour du moteur de base de données Oracle).	August 8, 2019
Management Agent pour OEM 13c Version 3 (p. 1656)	Amazon RDS pour les instances de base de données Oracle prend désormais en charge Management Agent pour le contrôle de cloud Oracle Enterprise Manager (OEM) 13c Version 3. Pour de plus amples informations, veuillez consulter Oracle Management Agent pour Enterprise Manager Cloud Control.	August 7, 2019
Amazon RDS pour PostgreSQL version 12 bêta 2 dans l'environnement en préversion de base de données (p. 1656)	Amazon RDS pour PostgreSQL prend désormais en charge PostgreSQL version 12 bêta 2 dans l'environnement en préversion de base de données Pour plus d'informations, consultez PostgreSQL version 12 bêta 2 sur Amazon RDS dans l'environnement en préversion de base de données.	August 6, 2019
Amazon RDS prend en charge les classements de serveur pour SQL Server (p. 1656)	Amazon RDS pour SQL Server prend en charge une sélection de classements pour les nouvelles instances de base de données. Pour plus d'informations, consultez Classements et jeux de caractères pour Microsoft SQL Server.	July 29, 2019

Amazon RDS pour PostgreSQL versions 11.4, 10.9, 9.6.14, 9.5.18 et 9.4.23 (p. 1656)	Amazon RDS pour PostgreSQL prend en charge les versions mineures 11.4, 10.9, 9.6.14, 9.5.18 et 9.4.23. Pour de plus amples informations, veuillez consulter Versions de bases de données PostgreSQL prises en charge.	July 3, 2019
Amazon RDS pour Oracle prend en charge Oracle APEX version 19.1.v1 (p. 1656)	Amazon RDS pour Oracle prend désormais en charge Oracle Application Express (APEX) version 19.1.v1. Pour de plus amples informations, veuillez consulter Oracle Application Express.	June 28, 2019
Amazon RDS pour PostgreSQL version 13 bêta 1 dans l'environnement en préversion de base de données (p. 1656)	Amazon RDS pour PostgreSQL prend désormais en charge PostgreSQL version 13 bêta 1 dans l'environnement en préversion de base de données Pour de plus amples informations, veuillez consulter PostgreSQL version 13 bêta 1 dans l'environnement en préversion de base de données.	June 22, 2019
Dimensionnement automatique du stockage Amazon RDS (p. 1656)	Le dimensionnement du stockage pour les instances de base de données Amazon RDS permettent à Amazon RDS d'augmenter automatiquement le stockage associé à une instance de base de données pour réduire les risques de conditions liées à un manque d'espace. Pour plus d'informations sur le dimensionnement automatique du stockage, consultez Utilisation du stockage pour les instances de base de données Amazon RDS.	June 20, 2019
Amazon RDS pour Oracle prend en charge les classes d'instance de base de données db.z1d (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant Oracle qui utilisent les classes d'instances de base de données db.z1d. Pour plus d'informations, veuillez consulter Classe d'instance de base de données.	June 13, 2019

Amazon RDS Performance Insights prend en charge l'affichage de texte SQL supplémentaire pour Amazon RDS pour Oracle (p. 1656)	Amazon RDS Performance Insights prend désormais en charge l'affichage de texte SQL supplémentaire dans le tableau de bord Performance Insights pour les instances de base de données Amazon RDS pour Oracle. Pour de plus amples informations, veuillez consulter Affichage de texte SQL supplémentaire sur le tableau de bord de Performance Insights.	June 10, 2019
Amazon RDS ajoute la prise en charge de restaurations natives des bases de données allant jusqu'à 16 To. (p. 1656)	Vous pouvez dorénavant effectuer la restauration native des bases allant jusqu'à 16 To depuis SQL Server vers Amazon RDS. Pour plus d'informations, consultez Amazon RDS pour SQL Server : limitations et recommandations.	June 4, 2019
Amazon RDS ajoute la prise en charge de Microsoft SQL Server Audit (p. 1656)	Amazon RDS pour Microsoft SQL Server vous permet d'auditer des événements au niveau du serveur et de la base de données à l'aide de SQL Server Audit et de consulter les résultats sur votre instance de base de données ou d'envoyer les fichiers journaux d'audit directement à Amazon S3. Pour de plus amples informations, veuillez consulter SQL Server Audit.	May 23, 2019
Améliorations des recommandations Amazon RDS (p. 1656)	Amazon RDS fournit maintenant des recommandations automatisées pour les ressources de base de données. Par exemple, Amazon RDS fournit maintenant des recommandations pour les paramètres de base de données. Pour de plus amples informations, veuillez consulter Utilisations des recommandations Amazon RDS.	May 22, 2019
Prise en charge de plus de bases de données par instance de base de données pour Amazon RDS SQL Server (p. 1656)	Vous pouvez créer jusqu'à 30 bases de données sur chacune de vos instances de base de données exécutant Microsoft SQL Server. Pour de plus amples informations, veuillez consultez Limites pour les instances de bases de données for Microsoft SQL Server.	May 21, 2019

Prise en charge de 64 Tio et de 80k d'E/S par seconde de stockage pour Amazon RDS pour MariaDB, MySQL et PostgreSQL (p. 1656)	Vous pouvez désormais créer des instances de bases de données Amazon RDS pour MySQL, MariaDB et PostgreSQL avec jusqu'à 64 Tio de stockage et 80 000 E/S par seconde provisionnées. Pour plus d'informations, consultez Stockage d'instance de base de données.	May 20, 2019
Amazon RDS pour MySQL prend en charge les vérifications préalables aux mises à niveau (p. 1656)	Lorsque vous mettez à niveau une instance de base de données de MySQL 5.7 vers MySQL 8.0, Amazon RDS recherche les incompatibilités en premier lieu. Pour de plus amples informations, veuillez consulter Vérifications préalables aux mises à niveau de MySQL 5.7 vers 8.0.	May 17, 2019
Prise en charge du plug-in de validation de mot de passe MySQL (p. 1656)	Vous pouvez désormais utiliser le plug-in MySQL `validate_password` pour une sécurité améliorée de Amazon RDS pour les instances de base de données MySQL. Pour de plus amples informations, veuillez consulter Utilisation du plug-in de validation de mot de passe.	May 16, 2019
Amazon RDS pour Oracle Avril 2019 RU, RUR et PSU (p. 1656)	Amazon RDS pour Oracle a lancé une version de moteur de base de données 12.2.0.1.ru-2019-04.rur-2019-04.r1 pour prendre en charge les versions Release Update (RU) et Release Update Revision (RUR) d'avril 2019. Amazon RDS pour Oracle a également lancé les versions de moteur de base de données 12.1.0.2.v16 et 11.2.0.4.v20 pour prendre en charge la mise à jour Oracle Database Patch Set Update (PSU) d'avril 2019. Pour de plus amples informations, veuillez consulter Oracle Database Engine Release Notes (Notes de mise à jour du moteur de base de données Oracle).	May 16, 2019

Compteurs Performance Insights pour Amazon RDS pour Oracle (p. 1656)	Vous pouvez désormais ajouter des compteurs de performances à vos graphiques Performance Insights pour les instances de base de données Oracle. Pour de plus amples informations, veuillez consulter Compteurs Performance Insights Counters pour Amazon RDS pour Oracle.	May 8, 2019
Amazon RDS pour PostgreSQL versions 11.2, 10.7, 9.6.12, 9.5.16 et 9.4.21 (p. 1656)	Amazon RDS pour PostgreSQL prend en charge les versions mineures 11.2, 10.7, 9.6.12, 9.5.16 et 9.4.21. Pour de plus amples informations, veuillez consulter Versions de bases de données PostgreSQL prises en charge.	May 1, 2019
Prise en charge de la facturation par seconde (p. 1656)	Amazon RDS est désormais facturé par incréments d'une seconde dans toutes les régions AWS, à l'exception de la régions AWS GovCloud (US) pour les instances à la demande. Pour de plus amples informations, veuillez consulter Facturation des instances de base de données pour Amazon RDS.	April 25, 2019
Prise en charge de l'importation de données de Amazon S3 pour Amazon RDS pour PostgreSQL (p. 1656)	Vous pouvez désormais importer les données des fichiers Amazon S3 dans une table d'une instance de base de données RDS PostgreSQL. Pour de plus amples informations, veuillez consulter Importation de données Amazon S3 dans une instance de base de données RDS PostgreSQL.	April 24, 2019
Prise en charge de la restauration des sauvegardes 5.7 depuis Amazon S3 (p. 1656)	Vous pouvez désormais créer une sauvegarde de votre base de données sur site, la stocker sur Amazon S3, puis restaurer le fichier de sauvegarde sur une nouvelle instance de base de données Amazon RDS qui exécute MySQL. Pour de plus amples informations, veuillez consulter Restauration d'une sauvegarde dans une instance de base de données Amazon RDS MySQL.	April 17, 2019

Prise en charge de plusieurs mises à niveau de version majeures pour Amazon RDS pour PostgreSQL (p. 1656)	Avec Amazon RDS pour PostgreSQL, vous pouvez désormais choisir parmi plusieurs versions majeures lorsque vous mettez à niveau le moteur de base de données. Cette fonctionnalité vous permet de passer à une nouvelle version majeure lorsque vous mettez à niveau certaines versions de moteur PostgreSQL. Pour de plus amples informations, veuillez consulter Mise à niveau du moteur de base de données PostgreSQL.	April 16, 2019
Prise en charge de 64 Tio de stockage pour Amazon RDS pour Oracle (p. 1656)	Vous pouvez désormais créer des instances de bases de données Amazon RDS pour Oracle avec jusqu'à 64 Tio de stockage et 80 000 E/S par seconde provisionnées. Pour plus d'informations, consultez Stockage d'instance de base de données.	April 4, 2019
Prise en charge de MySQL 8.0.15. (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant MySQL version 8.0. Pour de plus amples informations, veuillez consulter MySQL sur les versions Amazon RDS.	April 3, 2019
Prise en charge de MariaDB 10.3.13 (p. 1656)	Vous pouvez désormais créer des instances de bases de données Amazon RDS qui exécutent la version 10.3.13 de MariaDB. Pour de plus amples informations, veuillez consulter MariaDB sur les versions Amazon RDS.	April 3, 2019

Microsoft SQL Server 2008 R2 obsolète sur Amazon RDS (p. 1656)	La prise en charge de Microsoft SQL Server 2008 R2 est obsolète et coïncide avec le plan de Microsoft d'éliminer la prise en charge étendue pour cette version le 09 juillet 2019. Tout instantané de Microsoft SQL Server 2008 R2 existant doit être mis à niveau automatiquement vers la dernière version mineure de Microsoft SQL Server 2012 à compter du 1er juin 2019. Pour de plus amples informations, veuillez consulter Prise en charge de Microsoft SQL Server 2008 R2 sur Amazon RDS.	April 2, 2019
Groupes de disponibilité Always On pris en charge dans Microsoft SQL Server 2017 (p. 1656)	Vous pouvez désormais utiliser les groupes de disponibilité Always On dans SQL Server 2017 Enterprise Edition 14.00.3049.1 ou une version ultérieure. Pour de plus amples informations, veuillez consulter Déploiements multi-AZ pour Microsoft SQL Server.	March 29, 2019
Afficher les métriques de volume (p. 1656)	Vous pouvez désormais afficher les métriques pour les volumes Amazon Elastic Block Store (Amazon EBS), qui sont les appareils physiques utilisés pour le stockage dans les bases de données et les journaux. Pour de plus amples informations, veuillez consulter Affichage de la surveillance améliorée.	March 20, 2019
Prise en charge de MySQL 5.7.25 (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant MySQL version 5.7.25. Pour de plus amples informations, veuillez consulter MySQL sur les versions Amazon RDS.	March 19, 2019
Amazon RDS pour Oracle prend en charge les tâches RMAN DBA (p. 1656)	Amazon RDS pour Oracle prend maintenant en charge les tâches Oracle Recovery Manager (RMAN) DBA, dont les sauvegardes RMAN. Pour de plus amples informations, veuillez consulter Tâches courantes DBA Recovery Manager (RMAN) pour les instances de base de données Oracle.	March 14, 2019

Amazon RDS pour PostgreSQL prend en charge la version 11.1 (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant PostgreSQL version 11.1. Pour de plus amples informations, veuillez consulter PostgreSQL Version 11.1 sur Amazon RDS.	March 12, 2019
MariaDB 10.2.21 (p. 1656)	Vous pouvez désormais créer des instances de bases de données Amazon RDS qui exécutent la version 10.2 de MariaDB. Pour de plus amples informations, veuillez consulter MariaDB sur les versions Amazon RDS.	March 11, 2019
La restauration de plusieurs fichiers est disponible dans Amazon RDS pour SQL Server (p. 1656)	Vous pouvez désormais restaurer à partir de plusieurs fichiers avec Amazon RDS pour SQL Server. Pour de plus amples informations, veuillez consulter Restauration d'une base de données.	March 11, 2019
Amazon RDS for Oracle prend en charge les réplicas en lecture (p. 1656)	Amazon RDS for Oracle prend désormais en charge les réplicas en lecture avec Active Data Guard. Pour de plus amples informations, veuillez consulter Utilisation des réplicas en lecture et Utilisation des réplicas en lecture Oracle.	March 11, 2019
Amazon RDS Performance Insights est disponible pour Amazon RDS pour MariaDB (p. 1656)	Amazon RDS Performance Insights est désormais disponible pour Amazon RDS pour MariaDB. Pour de plus amples informations, veuillez consulter Utilisation d'Amazon RDS Performance Insights.	March 11, 2019
MySQL 8.0.13 et 5.7.24 (p. 1656)	Vous pouvez désormais créer des instances de bases de données Amazon RDS qui exécutent les versions 8.0.13 et 5.7.24 de MySQL. Pour plus d'informations, consultez MySQL sur les versions Amazon RDS.	March 8, 2019
Amazon RDS Performance Insights est disponible pour Amazon RDS pour SQL Server (p. 1656)	Amazon RDS Performance Insights est désormais disponible pour Amazon RDS pour SQL Server. Pour de plus amples informations, veuillez consulter Utilisation d'Amazon RDS Performance Insights.	March 4, 2019

Amazon RDS pour Oracle prend en charge l'intégration Amazon S3 (p. 1656)	Vous pouvez désormais transférer des fichiers entre un Amazon RDS pour une instance de base de données Oracle et un compartiment Amazon S3. Pour de plus amples informations, veuillez consulter Intégration de Amazon RDS pour Oracle et Amazon S3.	February 26, 2019
Amazon RDS pour MySQL et Amazon RDS pour MariaDB prennent n charge les classes d'instances de bases de données db.t3 (p. 1656)	Vous pouvez désormais créer des instances de bases de données Amazon RDS exécutant MySQL ou MariaDB qui utilisent les classes d'instances de bases de données db.t3. Pour plus d'informations, veuillez consulter Classe d'instance de base de données.	February 20, 2019
Amazon RDS pour MySQL et Amazon RDS pour MariaDB prennent en charge les classes d'instances de bases de données db.r5 (p. 1656)	Vous pouvez désormais créer des instances de bases de données Amazon RDS exécutant MySQL ou MariaDB qui utilisent les classes d'instances de bases de données db.r5. Pour plus d'informations, veuillez consulter Classe d'instance de base de données.	February 20, 2019
Compteurs Performance Insights pour Amazon RDS MySQL et PostgreSQL (p. 1656)	Vous pouvez désormais ajouter des compteurs de performances à vos graphiques Performance Insights pour les instances de base de données Amazon RDS MySQL et PostgreSQL. Pour de plus amples informations, veuillez consulter Composants du tableau de bord de Performance Insights.	February 19, 2019
Amazon RDS pour PostgreSQL prend désormais en charge l'ajustement du paramètre d'autovacuum adaptatif (p. 1656)	L'ajustement du paramètre d'autovacuum adaptatif avec Amazon RDS pour PostgreSQL permet d'éviter le renvoi à la ligne de l'ID de transaction en ajustant les valeurs du paramètre d'autovacuum automatiquement. Pour de plus amples informations, veuillez consulter Réduction de la probabilité de renvoi à la ligne de l'ID de transaction.	February 12, 2019

Amazon RDS pour Oracle prend en charge Oracle APEX versions 18.1.v1 et 18.2.v1 (p. 1656)	Amazon RDS pour Oracle prend désormais en charge Oracle Application Express (APEX) versions 18.1.v1. et 18.2.v1. Pour de plus amples informations, veuillez consulter Oracle Application Express.	February 11, 2019
Amazon RDS pour Oracle RU, RUR et PSU en janvier 2019 (p. 1656)	Amazon RDS pour Oracle a lancé une version de moteur de base de données 12.2.0.1.ru-2019-01.rur-2019-01.r1 pour prendre en charge les versions Release Update (RU) et Release Update Revision (RUR) d'avril 2019. Amazon RDS pour Oracle a également lancé les versions de moteur de base de données 12.1.0.2.v15 et 11.2.0.4.v19 pour prendre en charge la mise à jour Oracle Database Patch Set Update (PSU) de janvier 2019. Pour de plus amples informations, veuillez consulter Oracle Database Engine Release Notes (Notes de mise à jour du moteur de base de données Oracle).	February 8, 2019
Amazon RDS Performance Insights prend en charge l'affichage de texte SQL supplémentaire pour Amazon RDS MySQL (p. 1656)	Amazon RDS Performance Insights prend désormais en charge l'affichage de texte SQL supplémentaire dans le tableau de bord Performance Insights pour les instances de base de données Amazon RDS MySQL. Pour de plus amples informations, veuillez consulter Affichage de texte SQL supplémentaire sur le tableau de bord de Performance Insights.	February 6, 2019
Amazon RDS pour PostgreSQL prend en charge les classes d'instance de base de données db.t3 (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant PostgreSQL qui utilisent les classes d'instances de base de données db.t3. Pour plus d'informations, veuillez consulter Classe d'instance de base de données.	January 25, 2019

Amazon RDS pour Oracle prend en charge les classes d'instance de base de données db.t3 (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant Oracle qui utilisent les classes d'instances de base de données db.t3. Pour plus d'informations, veuillez consulter Classe d'instance de base de données.	January 25, 2019
Amazon RDS Performance Insights prend en charge l'affichage de texte SQL supplémentaire pour Amazon RDS PostgreSQL (p. 1656)	Amazon RDS Performance Insights prend désormais en charge l'affichage de texte SQL supplémentaire dans le tableau de bord Performance Insights pour les instances de base de données Amazon RDS PostgreSQL. Pour de plus amples informations, veuillez consulter Affichage de texte SQL supplémentaire sur le tableau de bord de Performance Insights.	January 24, 2019
Amazon RDS pour Oracle prend en charge une nouvelle version de SQLT (p. 1656)	Amazon RDS pour Oracle prend désormais en charge SQLT version 12.2.180725. Pour de plus amples informations, veuillez consulter Oracle SQLT.	January 22, 2019
Amazon RDS pour PostgreSQL prend en charge les nouvelles versions mineures (p. 1656)	Amazon RDS pour PostgreSQL prend désormais en charge les nouvelles versions mineures : 10.6, 9.6.11, 9.5.15, 9.4.20 et 9.3.25. Pour plus d'informations, consultez Amazon RDS for PostgreSQL Versions and Extensions (Amazon RDS pour les versions et extensions PostgreSQL).	December 19, 2018
Amazon RDS pour PostgreSQL prend en charge les classes d'instance de base de données db.r5 (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant PostgreSQL qui utilisent les classes d'instances de base de données db.r5. Pour plus d'informations, veuillez consulter Classe d'instance de base de données.	December 19, 2018

Amazon RDS pour PostgreSQL prend désormais en charge la gestion restreinte des mots de passe (p. 1656)	Amazon RDS pour PostgreSQL permet de limiter les utilisateurs autorisés à gérer les mots de passe et les modifications de leur date d'expiration via le paramètre `rds.restrict_password_commands` et le rôle `rds_password`. Pour plus d'informations, consultez Restriction de la gestion des mots de passe.	December 19, 2018
Amazon RDS pour PostgreSQL prend en charge l'importation des journaux de base de données dans Amazon CloudWatch Logs (p. 1656)	Amazon RDS pour PostgreSQL prend en charge l'importation des journaux de base de données dans CloudWatch Logs. Pour plus d'informations, consultez Publication des journaux PostgreSQL vers CloudWatch Logs.	December 10, 2018
Amazon RDS pour Oracle prend en charge les classes d'instance de base de données db.r5 (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant Oracle qui utilisent les classes d'instances de base de données db.r5. Pour plus d'informations, veuillez consulter Classe d'instance de base de données.	November 20, 2018
Rétention des sauvegardes lors de la suppression d'une instance de base de données (p. 1656)	Amazon RDS conserve des sauvegardes automatiques lorsque vous supprimez une instance de base de données. Pour plus d'informations, consultez la page Utilisation des sauvegardes.	November 15, 2018
Amazon RDS pour PostgreSQL prend en charge les classes d'instance de base de données db.m5 (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant PostgreSQL qui utilisent les classes d'instances de base de données db.m5. Pour plus d'informations, veuillez consulter Classe d'instance de base de données.	November 15, 2018

PSu Amazon RDS pour Oracle d'octobre 2018 (p. 1656)	Amazon RDS pour Oracle a publié les versions 12.1.0.2.v14 et 11.2.0.4.v18 du moteur de base de données pour prendre en charge la mise à jour d'ensemble de correctifs (PSU) Oracle Database d'octobre 2018. Pour de plus amples informations, veuillez consulter Oracle Database Engine Release Notes (Notes de mise à jour du moteur de base de données Oracle).	November 13, 2018
Amazon RDS pour Oracle prend en charge une nouvelle version majeure (p. 1656)	Vous pouvez désormais créer des instances de bases de données Amazon RDS qui exécutent la version 12.2 d'Oracle. Pour plus d'informations, consultez Oracle 12c version 12.2.0.1 avec Amazon RDS.	November 13, 2018
Amazon RDS pour SQL Server prend en charge la fonction AlwaysOn (p. 1656)	Amazon RDS pour SQL Server prend en charge les groupes de disponibilité Always On. Pour de plus amples informations, veuillez consulter Déploiements multi-AZ pour Microsoft SQL Server.	November 8, 2018
Amazon RDS pour PostgreSQL prend en charge l'accès au réseau sortant avec des serveurs DNS personnalisés (p. 1656)	Amazon RDS pour PostgreSQL prend en charge l'accès au réseau sortant avec des serveurs DNS personnalisés. Pour plus d'informations, consultez Utilisation d'un serveur DNS personnalisé pour l'accès au réseau sortant.	November 8, 2018
Amazon RDS pour MariaDB, MySQL et PostgreSQL prend en charge 32 Tio de stockage (p. 1656)	Vous pouvez désormais créer des instances de bases de données Amazon RDS pour MySQL, MariaDB et PostgreSQL avec jusqu'à 32 Tio de stockage. Pour plus d'informations, consultez Stockage d'instance de base de données.	November 7, 2018

Amazon RDS pour Oracle prend en charge les types de données étendus (p. 1656)	Vous pouvez désormais activer les types de données étendus sur les instances de base de données Amazon RDS exécutant Oracle. Avec les types de données étendus, la taille maximum est de 32 767 octets pour les types de données VARCHAR2, NVARCHAR2 et RAW. Pour plus d'informations, consultez Utilisation des types de données étendus.	November 6, 2018
Amazon RDS pour Oracle prend en charge les classes d'instance de base de données db.m5 (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant Oracle qui utilisent les classes d'instances de base de données db.m5. Pour plus d'informations, veuillez consulter Classe d'instance de base de données.	November 2, 2018
Migration de Amazon RDS pour Oracle de SE, SE1 ou SE2 vers EE (p. 1656)	Vous pouvez désormais migrer depuis n'importe quelle édition Oracle Database Standard Edition (SE, SE1 ou SE2) vers Oracle Database Enterprise Edition (EE). Pour plus d'informations, consultez Migration d'une édition Oracle à une autre.	October 31, 2018
Amazon RDS peut désormais arrêter les instances multi-AZ (p. 1656)	Amazon RDS peut désormais arrêter une instance de base de données faisant partie d'un déploiement multi-AZ. Auparavant, la fonction arrêter une instance était limitée pour les instances multi-AZ. Pour plus d'informations, consultez Arrêt temporaire d'une instance de base de données Amazon RDS.	October 29, 2018
Amazon RDS Performance Insights est disponible pour Amazon RDS Oracle (p. 1656)	Amazon RDS Performance Insights est désormais disponible pour Amazon RDS Oracle. Pour de plus amples informations, veuillez consulter Utilisation d'Amazon RDS Performance Insights.	October 29, 2018

Amazon RDS pour PostgreSQL prend en charge PostgreSQL version 11 dans l'environnement en préversion de base de données (p. 1656)	Amazon RDS pour PostgreSQL prend désormais en charge PostgreSQL version 11 dans l'environnement en préversion de base de données. Pour plus d'informations, consultez PostgreSQL version 11 sur Amazon RDS dans l'environnement en préversion de base de données.	October 25, 2018
MySQL prend en charge une nouvelle version majeure (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS exécutant MySQL version 8.0. Pour plus d'informations, consultez MySQL sur les versions Amazon RDS.	October 23, 2018
MariaDB prend en charge une nouvelle version majeure (p. 1656)	Vous pouvez désormais créer des instances de bases de données Amazon RDS qui exécutent la version 10.3 de MariaDB. Pour plus d'informations, consultez MariaDB sur les versions Amazon RDS.	October 23, 2018
Amazon RDS pour Oracle prend en charge Oracle JVM (p. 1656)	Amazon RDS pour Oracle prend désormais en charge l'option Oracle Java Virtual Machine (JVM). Pour plus d'informations, consultez Oracle Java Virtual Machine.	October 16, 2018
Groupe de paramètres personnalisés pour la restauration et la restauration à un instant dans le passé (p. 1656)	Vous pouvez désormais spécifier un groupe de paramètres personnalisés lorsque vous restaurez un instantané ou procédez à une opération de restauration à un instant dans le passé. Pour plus d'informations, consultez Restauration à partir d'un instantané de base de données et Restauration d'une instance de base de données à une date spécifiée.	October 15, 2018
Amazon RDS pour Oracle prend en charge 512 Tio de stockage (p. 1656)	Vous pouvez désormais créer des instances de base de données Oracle RDS avec un maximum de 32 Tio de stockage. Pour plus d'informations, consultez Stockage d'instance de base de données.	October 15, 2018

Amazon RDS pour MySQL prend en charge les GTID (p. 1656)	Amazon RDS pour MySQL prend désormais en charge les identifiants de transaction globaux (GTID), qui sont uniques parmi toutes les instances de base de données et dans une configuration de réplication. Pour plus d'informations, consultez Utilisation de la réplication basée sur des identifiants de transaction globaux (GTID) pour Amazon RDS MySQL.	October 10, 2018
MySQL 5.7.23, 5.6.41 et 5.5.61 (p. 1656)	Vous pouvez désormais créer des instances de base de données Amazon RDS qui exécutent les versions MySQL 5.7.23, 5.6.41 et 5.5.61. Pour plus d'informations, consultez MySQL sur les versions Amazon RDS.	October 8, 2018
Amazon RDS pour PostgreSQL prend en charge les nouvelles versions mineures (p. 1656)	Amazon RDS pour PostgreSQL prend désormais en charge les nouvelles versions mineures : 10.5, 9.6.10, 9.5.14, 9.4.19 et 9.3.24. Pour plus d'informations, consultez Amazon RDS for PostgreSQL Versions and Extensions (Amazon RDS pour les versions et extensions PostgreSQL).	October 4, 2018
Amazon RDS pour Oracle prend en charge une nouvelle version de SQLT (p. 1656)	Amazon RDS pour Oracle prend désormais en charge SQLT version 12.2.180331. Pour de plus amples informations, veuillez consulter Oracle SQLT.	October 4, 2018
Correctif PSU Amazon RDS pour Oracle de juillet 2018 (p. 1656)	Amazon RDS pour Oracle a publié les versions 12.1.0.2.v13 et 11.2.0.4.v17 du moteur de base de données pour prendre en charge la mise à jour d'ensemble de correctifs (PSU) Oracle Database de juillet 2018. Pour de plus amples informations, veuillez consulter Oracle Database Engine Release Notes (Notes de mise à jour du moteur de base de données Oracle).	October 3, 2018

Amazon RDS pour PostgreSQL prend désormais en charge l'authentification IAM (p. 1656)	Amazon RDS pour PostgreSQL prend désormais en charge l'authentification IAM. Pour plus d'informations, consultez Authentification de base de données IAM pour MySQL et PostgreSQL.	September 27, 2018
Vous pouvez activer la protection contre la suppression pour vos instances de base de données Amazon RDS (p. 1656)	Lorsque vous activez la protection contre la suppression pour une instance de base de données, la base de données ne peut être supprimée par aucun utilisateur. Pour plus d'informations, consultez Suppression d'une instance de base de données.	September 26, 2018
Amazon RDS pour MySQL et Amazon RDS pour MariaDB prennent désormais en charge les classes d'instances de bases de données db.m5 (p. 1656)	Vous pouvez désormais créer des instances de bases de données Amazon RDS exécutant MySQL ou MariaDB qui utilisent les classes d'instances de bases de données db.m5. Pour plus d'informations, veuillez consulter Classe d'instance de base de données.	September 18, 2018
Amazon RDS prend désormais en charge les mises à niveau à SQL Server 2017 (p. 1656)	Vous pouvez mettre à jour une instance de base de données existante vers SQL Server 2017 depuis n'importe quelle version, sauf SQL Server 2008. Pour mettre à niveau SQL Server 2008, mettez-vous d'abord à niveau avec une autre version. Pour plus d'informations, consultez Mise à niveau du moteur de base de données Microsoft SQL Server.	September 11, 2018
Amazon RDS pour PostgreSQL prend désormais en charge PostgreSQL version 11 bêta 3 dans l'environnement en préversion de base de données (p. 1656)	Dans cette édition, la taille de segment Write-Ahead Log (WAL) (wal_segment_size) est désormais définie à 64Mo. Pour plus d'informations sur la version PostgreSQL 11 Beta 3, consultez PostgreSQL 11 Beta 3 Released (Publication de PostgreSQL 11 Beta 3). Pour plus d'informations sur l'environnement en préversion de base de données, consultez Working with the Database Preview Environment (Travailler avec l'environnement en préversion de base de données).	September 7, 2018

Guide de l'utilisateur Amazon Aurora (p. 1656)	Le Amazon Aurora Guide de l'utilisateur présente tous les concepts Amazon Aurora et fournit des instructions sur l'utilisation des différentes fonctions, à la fois avec la console et via l'interface de ligne de commande. Le Amazon RDS Guide de l'utilisateur prend désormais en charge les moteurs de base de données non-Aurora.	August 31, 2018
Amazon RDS Performance Insights est disponible pour MySQL Amazon RDS (p. 1656)	Amazon RDS Performance Insights est désormais disponible pour MySQL Amazon RDS. Pour de plus amples informations, veuillez consulter Utilisation d'Amazon RDS Performance Insights.	August 28, 2018
Aurora avec compatibilité PostgreSQL prend désormais en charge Aurora Auto Scaling (p. 1656)	L'Auto Scaling des réplicas Aurora est désormais disponible pour Aurora avec compatibilité PostgreSQL. Pour plus d'informations, consultez Utilisation d'Auto Scaling Amazon Aurora avec des réplicas Aurora.	August 16, 2018
Aurora Serverless pour Aurora MySQL (p. 1656)	Aurora Serverless est une configuration à scalabilité automatique et à la demande pour Amazon Aurora. Pour de plus amples informations, veuillez consulter Utilisation de Amazon Aurora Serverless.	August 9, 2018
MySQL 5.7.22 et 5.6.40 (p. 1656)	Vous pouvez désormais créer des instances de bases de données Amazon RDS en exécutant les versions 5.7.22 et 5.6.40 de MySQL. Pour plus d'informations, consultez MySQL sur les versions Amazon RDS.	August 6, 2018
Aurora est désormais disponible dans la région Chine (Ningxia) (p. 1656)	Aurora MySQL et Aurora PostgreSQL sont désormais disponibles dans la région Chine (Ningxia). Pour plus d'informations, consultez Disponibilité de Amazon Aurora MySQL et Disponibilité de Amazon Aurora PostgreSQL.	August 6, 2018

Amazon RDS pour MySQL prend en charge la réplication retardée (p. 1656)	Amazon RDS pour MySQL prend désormais en charge la réplication retardée comme stratégie pour la reprise après sinistre. Pour plus d'informations, consultez Configuration de la réplication retardée avec MySQL.	August 6, 2018
Amazon RDS Performance Insights est disponible pour Aurora MySQL (p. 1656)	Amazon RDS Performance Insights est désormais disponible pour Aurora MySQL. Pour plus d'informations, consultez Utilisation d'Amazon RDS Performance Insights.	August 6, 2018
Amazon RDS Intégration de Performance Insights avec Amazon CloudWatch (p. 1656)	Amazon RDS Performance Insights publie automatiquement les métriques dans Amazon CloudWatch. Pour plus d'informations, consultez Métriques Performance Insights publiées dans CloudWatch.	August 6, 2018
Recommandations concernant Amazon RDS (p. 1656)	Amazon RDS fournit maintenant des recommandations automatisées pour les ressources de base de données. Pour de plus amples informations, veuillez consulter Utilisations des recommandations Amazon RDS.	July 25, 2018
Amazon RDS pour PostgreSQL prend en charge les nouvelles versions mineures (p. 1656)	Amazon RDS pour PostgreSQL prend désormais en charge les nouvelles versions mineures : 10.4, 9.6.9, 9.5.13, 9.4.18 et 9.3.23. Pour plus d'informations, consultez Amazon RDS for PostgreSQL Versions and Extensions (Amazon RDS pour les versions et extensions PostgreSQL).	July 25, 2018
Copies d'instantanés incrémentielles entre régions AWS (p. 1656)	Amazon RDS prend en charge les copies d'instantanés incrémentiels d'une région AWS à l'autre pour les instances chiffrées et non chiffrées. Pour plus d'information, consultez Copie d'instantanés dans des régions AWS.	July 24, 2018
Amazon RDS Performance Insights est disponible pour Amazon RDS pour PostgreSQL (p. 1656)	Amazon RDS Performance Insights est désormais disponible pour Amazon RDS pour PostgreSQL. Pour de plus amples informations, veuillez consulter Utilisation d'Amazon RDS Performance Insights.	July 18, 2018

Amazon RDS pour Oracle prend en charge Oracle APEX version 5.1.4.v1 (p. 1656)	Amazon RDS pour Oracle prend désormais en charge Oracle Application Express (APEX) version 5.1.4.v1. Pour de plus amples informations, veuillez consulter Oracle Application Express.	July 10, 2018
Amazon RDS pour Oracle prend en charge la publication des journaux dans Amazon CloudWatch Logs (p. 1656)	Amazon RDS pour Oracle prend désormais en charge la publication des données de journaux d'alerte, d'audit, de trace et d'écouteur dans un groupe de journaux dans CloudWatch Logs. Pour plus d'informations, consultez Publication des journaux Oracle dans Amazon CloudWatch Logs.	July 9, 2018
MariaDB 10.2.15, 10.1.34 et 10.0.35 (p. 1656)	Vous pouvez désormais créer des instances de bases de données Amazon RDS en exécutant les versions 10.2.15, 10.1.34 et 10.0.35 de MySQL. Pour de plus amples informations, veuillez consulter MariaDB sur les versions Amazon RDS.	July 5, 2018
Aurora PostgreSQL 1.2 est disponible et compatible avec PostgreSQL 9.6.8 (p. 1656)	Aurora PostgreSQL 1.2 est désormais disponible et compatible avec PostgreSQL 9.6.8. Pour plus d'informations, consultez la Version 1.2.	June 27, 2018
Les réplicas en lecture pour Amazon RDS PostgreSQL prennent en charge les déploiements multi-AZ (p. 1656)	Les réplicas en lecture RDS dans Amazon RDS PostgreSQL prennent désormais en charge plusieurs zones de disponibilité. Pour plus d'informations, consultez Utilisation des réplicas en lecture PostgreSQL.	June 25, 2018
Performance Insights est disponible pour Aurora PostgreSQL (p. 1656)	Performance Insights est généralement disponible pour Aurora PostgreSQL, avec la prise en charge de la conservation étendue des données de performance. Pour plus d'informations, consultez Utilisation d'Amazon RDS Performance Insights.	June 21, 2018

Aurora PostgreSQL est disponible dans la région USA Ouest (Californie du Nord) (p. 1656)	Aurora PostgreSQL est désormais disponible dans la région USA Ouest (Californie du Nord). Pour plus d'informations, consultez Disponibilité pour Amazon Aurora PostgreSQL.	June 11, 2018
Amazon RDS pour Oracle prend désormais en charge la configuration de l'UC (p. 1656)	Amazon RDS pour Oracle prend en charge la configuration du nombre de cœurs d'UC et du nombre de threads pour chaque cœur du processus d'une classe d'instance de base de données. Pour plus d'informations, consultez Configuration du processeur de la classe d'instance de base de données.	June 5, 2018
Amazon RDS pour Oracle PSU avril 2018 (p. 1656)	Amazon RDS pour Oracle a publié les versions 12.1.0.2.v12 et 11.2.0.4.v16 du moteur de base de données pour prendre en charge la mise à jour d'ensemble de correctifs (PSU) Oracle Database d'avril 2018. Pour de plus amples informations, veuillez consulter Oracle Database Engine Release Notes (Notes de mise à jour du moteur de base de données Oracle).	June 1, 2018

Mises à jour antérieures

Le tableau ci-après décrit les modifications importantes apportées dans chaque version du Guide de l'utilisateur Amazon RDS avant juin 2018.

Modifier	Description	Date de modification
Amazon RDS pour PostgreSQL prend désormais en charge PostgreSQL version 11 bêta 1 dans l'environnement en préversion de base de données	PostgreSQL version 11 Bêta 1 contient plusieurs améliorations qui sont décrites dans PostgreSQL 11 Bêta 1 Released. Pour plus d'informations sur l'environnement en préversion de base de données, consultez Utilisation de l'environnement en préversion de base de données (p. 1465).	31 mai 2018
Amazon RDS pour Oracle prend désormais en charge TLS versions 1.0 et 1.2	Amazon RDS pour Oracle prend en charge le protocole TLS (Transport Layer Security) version 1.0 et 1.2. Pour plus d'informations, consultez Versions TLS pour l'option Oracle SSL (p. 1069).	30 mai 2018

Modifier	Description	Date de modification
Aurora MySQL prend en charge la publication des journaux dans Amazon CloudWatch Logs	Aurora MySQL prend désormais en charge la publication des journaux généraux, des journaux de requêtes lentes, des journaux d'audit et des journaux d'erreurs dans un groupe de journaux dans CloudWatch Logs. Pour plus d'informations, consultez Publication de Aurora MySQL dans CloudWatch Logs.	23 mai 2018
Environnement en préversion de base de données pour Amazon RDS PostgreSQL	Vous pouvez désormais lancer une nouvelle instance de Amazon RDS PostgreSQL en mode préversion. Pour plus d'informations sur l'environnement en préversion de base de données, consultez Utilisation de l'environnement en préversion de base de données (p. 1465).	22 mai 2018
Amazon RDS pour les instances de bases de données Oracle prend en charge les nouvelles classes d'instance de base de données	Les instances de base de données Oracle prennent désormais en charge les classes d'instances de base de données db.x1e et db.x1. Pour plus d'informations, consultez Classes d'instances de base de données (p. 6) et Prise en charge des classes d'instance de base de données pour Oracle (p. 933).	22 mai 2018
Amazon RDS PostgreSQL prend désormais en charge postgres_fdw sur un réplica en lecture.	Vous pouvez désormais utiliser postgres_fdw pour vous connecter à un serveur distant à partir d'un réplica en lecture. Pour plus d'informations, consultez Accès aux données externes à l'aide de l'extension postgres_fdw (p. 1447).	17 mai 2018
Amazon RDS pour Oracle prend désormais en charge la définition des paramètres sqlnet.ora	Vous pouvez désormais définir les paramètres sqlnet.ora avec Amazon RDS pour Oracle. Pour plus d'informations, consultez Modification des paramètres Oracle sqlnet.ora (p. 972).	10 mai 2018
Aurora PostgreSQL est disponible dans la région Asie-Pacifique (Séoul).	Aurora PostgreSQL est désormais disponible dans la région Asie-Pacifique (Séoul). Pour plus d'informations, consultez Disponibilité pour Amazon Aurora PostgreSQL.	9 mai 2018
Aurora MySQL prend en charge le retour sur trace	Aurora MySQL permet désormais d'effectuer un retour sur trace d'un cluster de base de données à une heure spécifique, sans restaurer les données à partir d'une sauvegarde. Pour plus d'informations, consultez Retour en arrière d'un cluster de base de données Amazon Aurora.	9 mai 2018
Aurora MySQL prend en charge la migration et la réplication chiffrées depuis une base de données MySQL externe	Aurora MySQL prend désormais en charge la migration et la réplication chiffrées depuis une base de données MySQL externe. Pour plus d'informations, consultez Migrer des données depuis une base de données MySQL externe vers un cluster de base de données Amazon Aurora MySQL et la Réplication entre Aurora et MySQL ou entre Aurora et un autre cluster de base de données Aurora.	25 avril 2018

Modifier	Description	Date de modification
Aurora avec compatibilité PostgreSQL prend en charge le protocole de copie sur écriture.	Vous pouvez désormais cloner des bases de données dans un cluster de bases de données Aurora PostgreSQL. Pour plus d'informations, consultez Clonage de base de données dans un cluster de base de données Aurora.	10 avril 2018
MariaDB 10.2.12, 10.1.31 et 10.0.34	Vous pouvez désormais créer des instances de bases de données Amazon RDS qui exécutent les versions 10.2.12, 10.1.31 et 10.0.34 de MariaDB. Pour plus d'informations, consultez Versions de MariaDB sur Amazon RDS (p. 544).	21 mars 2018
Prise en charge d'Aurora PostgreSQL pour les nouvelles régions	Aurora PostgreSQL est désormais disponible dans les régions UE(Londres) et Asie Pacifique (Singapour). Pour plus d'informations, consultez Disponibilité pour Amazon Aurora PostgreSQL.	13 mars 2018
MySQL 5.7.21, 5.6.39 et 5.5.59	Vous pouvez désormais créer des instances de bases de données Amazon RDS qui exécutent les versions 5.7.21, 5.6.39 et 5.5.59. de MySQL. Pour plus d'informations, consultez Versions de MySQL sur Amazon RDS (p. 782).	9 mars 2018
Amazon RDS pour Oracle prend désormais en charge les services de données Oracle REST	Amazon RDS pour Oracle prend désormais en charge les services de données Oracle REST dans le cadre de l'option APEX. Pour plus d'informations, consultez Oracle Application Express (APEX) (p. 1026).	9 mars 2018
Amazon Aurora avec compatibilité MySQL disponible dans une nouvelle région AWS	Aurora MySQL est désormais disponible dans la région Asie-Pacifique (Singapour). Pour obtenir la liste complète des régions AWS pour Aurora MySQL, consultez Disponibilité pour Amazon Aurora MySQL.	6 mars 2018
Prise en charge de PostgreSQL 10.1	Amazon RDS prend désormais en charge la version 10.1 de PostgreSQL. Pour plus d'informations, consultez PostgreSQL version 10.1 sur Amazon RDS (p. 1478)	27 février 2018
PSU Oracle Janvier 2018	Amazon RDS pour Oracle a publié les versions 12.1.0.2.v11 et 11.2.0.4.v15 du moteur de base de données pour prendre en charge la mise à jour d'ensemble de correctifs (PSU) Oracle Database de janvier 2018. Pour plus d'informations, consultez Notes de mise à jour pour le moteur de base de données Oracle (p. 1208).	22 février 2018
Les instances de base de données Amazon RDS s'exécutant sur Microsoft SQL Server prennent en charge la capture de données modifiées (CDC)	Les instances de base de données exécutant Amazon RDS pour Microsoft SQL Server prennent à présent en charge la capture de données modifiées (CDC). Pour plus d'informations, consultez Prise en charge de la capture de données modifiées (CDC) pour les instances de base de données Microsoft SQL Server (p. 605).	6 février 2018

Modifier	Description	Date de modification
Aurora MySQL prend en charge une nouvelle version majeure	Vous pouvez désormais créer des clusters de bases de données Aurora MySQL en exécutant la version 5.7 de MySQL. Pour plus d'informations, consultez Amazon Aurora MySQL Database Engine Updates 2018-02-06 Mises à jour de moteur de base de données Amazon Aurora MySQL de 2018-02-06à.	6 février 2018
Prise en charge de PostgreSQL 9.6.6	Amazon RDS PostgreSQL prend désormais en charge la version 9.6.6. Cette édition prend désormais en charge le préfixe et les extensions orafce. Pour plus d'informations, consultez PostgreSQL version 9.6.6 sur Amazon RDS (p. 1481).	19 janvier 2018
Publier des journaux MySQL et MariaDB dans Amazon CloudWatch Logs	Vous pouvez maintenant publier des données de journaux MySQL et MariaDB dans CloudWatch Logs. Pour plus d'informations, consultez Publication des journaux MySQL dans CloudWatch Logs (p. 509) et Publication des journaux MariaDB dans Amazon CloudWatch Logs (p. 496).	17 janvier 2018
Prise en charge de plusieurs zones de disponibilité pour les réplicas en lecture	Vous pouvez désormais créer un réplica en lecture en tant qu'instance de base de données multi-AZ. Amazon RDS crée une instance de secours de votre réplica dans une autre zone de disponibilité pour prendre en charge le basculement du réplica. La création de votre réplica en lecture en tant qu'instance de base de données multi-AZ est indépendante du fait que la base de données source soit ou non une instance de base de données multi-AZ. Pour plus d'informations, consultez Utilisation des réplicas en lecture (p. 275).	11 janvier 2018
Amazon RDS pour MariaDB prend en charge une nouvelle version majeure	Vous pouvez désormais créer des instances de bases de données Amazon RDS qui exécutent la version 10.2 de MariaDB. Pour plus d'informations, consultez Prise en charge de MariaDB 10.2 sur Amazon RDS (p. 547).	3 janvier 2018
Amazon Aurora avec compatibilité PostgreSQL disponible dans une nouvelle région AWS	Aurora PostgreSQL est maintenant disponible dans la région UE (Paris). Pour obtenir la liste complète des régions AWS pour Aurora PostgreSQL, consultez Disponibilité pour Amazon Aurora PostgreSQL.	22 décembre 2017
Aurora PostgreSQL prend en charge de nouveaux types d'instance	Aurora PostgreSQL prend maintenant en charge de nouveaux types d'instance. Pour obtenir la liste complète des types d'instance, consultez Choisir la classe d'instance de base de données.	20 décembre 2017
PSU Oracle d'octobre 2017	Amazon RDS pour Oracle a publié les versions 12.1.0.2.v10 et 11.2.0.4.v14 du moteur de base de données pour prendre en charge la mise à jour d'ensemble de correctifs (PSU) Oracle Database d'octobre 2017. Pour plus d'informations, consultez Notes de mise à jour pour le moteur de base de données Oracle (p. 1208).	19 décembre 2017

Modifier	Description	Date de modification
Amazon Aurora avec compatibilité MySQL disponible dans une nouvelle région AWS	Aurora MySQL est maintenant disponible dans la région UE (Paris). Pour obtenir la liste complète des régions AWS pour Aurora MySQL, consultez Disponibilité pour Amazon Aurora MySQL.	18 décembre 2017
Aurora MySQL prend en charge les jointures par hachage	Cette fonctionnalité peut améliorer les performances de requêtes lorsque vous devez joindre une grande quantité de données au moyen d'une équijointure. Pour plus d'informations, consultez Traitement des raccords de hachage dans Aurora MySQL.	11 décembre 2017
Aurora MySQL prend en charge les fonctions natives pour invoquer les fonctions AWS Lambda	Vous pouvez appeler les fonctions natives `lambda_sync` et `lambda_async` lorsque vous utilisez Aurora MySQL. Pour plus d'informations, consultez Invocation d'une fonction lambda à partir d'un cluster de base de données Amazon Aurora MySQL.	11 décembre 2017
Ajout de l'éligibilité HIPAA à Aurora PostgreSQL	Aurora PostgreSQL prend désormais en charge les applications conformes à la loi HIPAA. Pour plus d'informations, consultez Utilisation de Amazon Aurora PostgreSQL.	6 décembre 2017
Régions AWS supplémentaires disponibles pour Amazon Aurora avec compatibilité PostgreSQL	Amazon Aurora avec compatibilité PostgreSQL est désormais disponible dans quatre nouvelles régions AWS. Pour plus d'informations, consultez Disponibilité pour Amazon Aurora PostgreSQL.	22 novembre 2017
Modification du stockage pour les instances de bases de données Amazon RDS exécutant Microsoft SQL Server	Vous pouvez désormais modifier le stockage de vos instances de bases de données Amazon RDS exécutant SQL Server. Pour de plus amples informations, veuillez consulter Modification d'une instance de base de données Amazon RDS (p. 243).	21 novembre 2017
Amazon RDS prend en charge 16 Tio de stockage pour les moteurs basés sur Linux	Vous pouvez désormais créer des instances de bases de données MySQL, MariaDB, PostgreSQL et Oracle avec un maximum de 16 Tio de stockage. Pour plus d'informations, consultez Stockage d'instance de base de données Amazon RDS (p. 30).	21 novembre 2017
Amazon RDS prend en charge une augmentation rapide du stockage	Vous pouvez désormais ajouter en quelques minutes du stockage aux instances de bases de données MySQL, MariaDB, PostgreSQL et Oracle. Pour plus d'informations, consultez Stockage d'instance de base de données Amazon RDS (p. 30).	21 novembre 2017
Amazon RDS prend en charge MariaDB versions 10.1.26 et 10.0.32	Vous pouvez désormais créer des instances de bases de données Amazon RDS qui exécutent les versions 10.1.26 et 10.0.32 de MariaDB. Pour plus d'informations, consultez Versions de MariaDB sur Amazon RDS (p. 544).	20 novembre 2017

Modifier	Description	Date de modification
Amazon RDS pour Microsoft SQL Server prend désormais en charge de nouvelles classes d'instances de bases de données	Vous pouvez désormais créer des instances de bases de données Amazon RDS exécutant SQL Server qui utilisent les classes d'instances de bases de données db.r4 et db.m4.16xlarge. Pour plus d'informations, consultez Prise en charge de la classe d'instance de base de données pour Microsoft SQL Server (p. 597).	20 novembre 2017
Amazon RDS pour MySQL et MariaDB prend désormais en charge de nouvelles classes d'instances de bases de données	Vous pouvez désormais créer des instances de bases de données Amazon RDS exécutant MySQL et MariaDB qui utilisent les classes d'instances de bases de données db.r4, db.m4.16xlarge, db.t2.xlarge et db.t2.2xlarge. Pour plus d'informations, consultez Classes d'instances de base de données (p. 6).	20 novembre 2017
SQL Server 2017	Vous pouvez désormais créer des instances de bases de données Amazon RDS exécutant Microsoft SQL Server 2017. Vous pouvez également créer des instances de bases de données exécutant SQL Server 2016 SP1 CU5. Pour plus d'informations, consultez Microsoft SQL Server sur Amazon RDS (p. 592).	17 novembre 2017
Restauration des sauvegardes MySQL d'Amazon S3	Vous pouvez désormais créer une sauvegarde de votre base de données sur site, la stocker sur Amazon S3, puis restaurer le fichier de sauvegarde sur une nouvelle instance de base de données Amazon RDS qui exécute MySQL. Pour plus d'informations, consultez Restauration d'une sauvegarde dans une instance de base de données MySQL Amazon RDS (p. 821).	17 novembre 2017
Auto Scaling avec réplicas Aurora	Amazon Aurora MySQL prend désormais en charge l'Auto Scaling Aurora. L'Auto Scaling Aurora ajuste dynamiquement le nombre de réplicas Aurora sur la base des réductions et augmentations de connectivité ou de charge de travail. Pour plus d'informations, consultez Utilisation d'Auto Scaling Amazon Aurora avec des réplicas Aurora.	17 novembre 2017
Prise en charge de l'édition par défaut d'Oracle	Amazon RDS pour les instances de bases de données Oracle prend maintenant en charge la configuration de l'édition par défaut de l'instance de base de données. Pour plus d'informations, consultez Définition de l'édition par défaut d'une instance de base de données (p. 1123).	3 novembre 2017
Validation des fichiers d'instance de base de données Oracle	Amazon RDS pour les instances de bases de données Oracle prend maintenant en charge la validation des fichiers d'instance de base de données avec l'utilitaire de validation logique Oracle Recovery Manager (RMAN). Pour plus d'informations, consultez Validation des fichiers d'instance de base de données (p. 1140).	3 novembre 2017

Modifier	Description	Date de modification
PSU Oracle de juillet 2017	Amazon RDS pour Oracle a publié les versions 12.1.0.2.v9 et 11.2.0.4.v13 du moteur de base de données pour prendre en charge la mise à jour d'ensemble de correctifs (PSU) Oracle Database de juillet 2017. Pour plus d'informations, consultez Notes de mise à jour pour le moteur de base de données Oracle (p. 1208).	3 novembre 2017
Management Agent pour OEM 13c	Les instances de bases de données Oracle Amazon RDS prennent désormais en charge Management Agent pour le contrôle de cloud Oracle Enterprise Manager (OEM) 13c. Pour plus d'informations, consultez Oracle Management Agent pour Enterprise Manager Cloud Control (p. 1042).	1 novembre 2017
PostgreSQL 9.6.5, 9.5.9, 9.4.14 et 9.3.19	Vous pouvez désormais créer des instances de bases de données Amazon RDS exécutant les versions 9.6.5., 9.5.9, 9.4.14 et 9.3.19 de PostgreSQL. Pour plus d'informations, consultez Versions de base de données PostgreSQL prises en charge (p. 1468).	1 novembre 2017
Reconfiguration du stockage pour les instantanés Microsoft SQL Server	Vous pouvez désormais reconfigurer le stockage lorsque vous restaurez un instantané sur une instance de base de données Amazon RDS exécutant Microsoft SQL Server. Pour plus d'informations, consultez Restauration à partir d'un instantané de base de données (p. 329).	26 octobre 2017
Lecture anticipée asynchrone des clés pour Aurora avec compatibilité MySQL	La lecture anticipée asynchrone des clés (AKP) améliore les performances des jointures d'index non mises en cache en récupérant au préalable les clés en mémoire avant qu'elles ne soient nécessaires. Pour plus d'informations, consultez Utilisation de la pré-extraction de clé asynchrone dans Amazon Aurora.	26 octobre 2017
MySQL 5.7.19, 5.6.37 et 5.5.57	Vous pouvez désormais créer des instances de bases de données Amazon RDS qui exécutent les versions 5.7.19, 5.6.37 et 5.5.57 de MySQL. Pour plus d'informations, consultez Versions de MySQL sur Amazon RDS (p. 782).	25 octobre 2017
Disponibilité générale d'Amazon Aurora avec compatibilité PostgreSQL	Amazon Aurora avec compatibilité PostgreSQL permet de configurer, de gérer et de dimensionner de façon simple et économique vos déploiements PostgreSQL nouveaux et existants, vous permettant ainsi de vous concentrer sur votre activité et vos applications. Pour plus d'informations, consultez Utilisation de Amazon Aurora PostgreSQL.	24 octobre 2017
Amazon RDS pour les instances de bases de données Oracle prend en charge les nouvelles classes d'instance de base de données	Amazon RDS pour les instances de bases de données Oracle prend désormais en charge les classes d'instance à mémoire optimisée nouvelle génération (db.r4). Amazon RDS pour les instances de bases de données Oracle prend maintenant également en charge les nouvelles classes d'instance suivantes de la génération actuelle : db.m4.16xlarge, db.t2.xlarge et db.t2.2xlarge. Pour plus d'informations, consultez Classes d'instances de base de données (p. 6) et Prise en charge des classes d'instance de base de données pour Oracle (p. 933).	23 octobre 2017

Modifier	Description	Date de modification
Nouvelle fonction	Vos instances réservées nouvelles et existantes peuvent maintenant couvrir plusieurs tailles dans la même classe d'instance de base de données. Les instances réservées de taille flexible sont disponibles pour les instances de bases de données ayant les mêmes région AWS, moteur de base de données et famille d'instance dans la configuration de zone de disponibilité. Les instances réservées de taille flexible sont disponibles pour les moteurs de base de données suivants : Amazon Aurora, MariaDB, MySQL, Oracle (Réutilisez vos licences), PostgreSQL. Pour plus d'informations, consultez Instances de base de données réservées de taille flexible (p. 49).	11 octobre 2017
Nouvelle fonction	Vous pouvez désormais utiliser l'option Oracle SQLT pour régler une instruction SQL afin d'obtenir des performances optimales. Pour plus d'informations, consultez Oracle SQLT (p. 1080).	22 septembre 2017
Nouvelle fonction	Si vous avez des instantanés de base de données manuels existants de vos instances de bases de données Amazon RDS Oracle, vous pouvez désormais les mettre à niveau vers une version ultérieure du moteur de base de données Oracle. Pour plus d'informations, consultez Mise à niveau d'un instantané de base de données Oracle (p. 988).	20 septembre 2017
Nouvelle fonction	Vous pouvez désormais utiliser Oracle Spatial pour stocker, récupérer, mettre à jour et effectuer des requêtes sur les données spatiales dans vos instances de bases de données Amazon RDS exécutant Oracle. Pour plus d'informations, consultez Oracle Spatial (p. 1077).	15 septembre 2017
Nouvelle fonction	Vous pouvez désormais utiliser Oracle Locator pour prendre en charge les applications basées sur des services sans fil et sur Internet, ainsi que les solutions GIS basées sur le partenariat avec vos instances de bases de données Amazon RDS exécutant Oracle. Pour plus d'informations, consultez Oracle Locator (p. 1057).	15 septembre 2017
Nouvelle fonction	Vous pouvez désormais utiliser Oracle Multimedia pour stocker, gérer et récupérer des images, des fichiers audio et vidéo, ainsi que d'autres données multimédias hétérogènes dans vos instances de bases de données Amazon RDS exécutant Oracle. Pour plus d'informations, consultez Oracle Multimedia (p. 1060).	15 septembre 2017
Nouvelle fonction	Vous pouvez désormais exporter des journaux d'audit depuis vos clusters de bases de données Amazon Aurora MySQL vers Amazon CloudWatch Logs. Pour plus d'informations, consultez Publication des journaux Aurora MySQL vers Amazon CloudWatch Logs.	14 septembre 2017

Modifier	Description	Date de modification
Nouvelle fonction	Amazon RDS prend désormais en charge plusieurs versions d'Oracle Application Express (APEX) pour vos instances de bases de données exécutant Oracle. Pour plus d'informations, consultez Oracle Application Express (APEX) (p. 1026).	13 septembre 2017
Nouvelle fonction	Vous pouvez désormais utiliser Amazon Aurora pour migrer un instantané de base de données chiffré ou non chiffré ou une instance de base de données Amazon RDS MySQL vers un cluster de bases de données Aurora MySQL chiffré. Pour plus d'informations, consultez Migration d'un instantané RDS MySQL vers Aurora et Migration de données à partir d'une instance de base de données MySQL vers un cluster de base de données Amazon Aurora MySQL en utilisant un réplica en lecture Aurora.	5 septembre 2017
Nouvelle fonction	Vous pouvez utiliser Amazon RDS pour les bases de données Microsoft SQL Server afin de développer des applications conformes à la loi HIPAA. Pour plus d'informations, consultez Prise en charge du programme de conformité pour les instances de bases de données Microsoft SQL Server (p. 599).	31 août 2017
Nouvelle fonction	Vous pouvez maintenant utiliser Amazon RDS pour les bases de données MariaDB afin de développer des applications conformes à la loi HIPAA. Pour plus d'informations, consultez MariaDB sur Amazon RDS (p. 542).	31 août 2017
Nouvelle fonction	Vous pouvez désormais créer des instances de bases de données Amazon RDS exécutant Microsoft SQL Server avec un stockage alloué pouvant atteindre 16 Tio et des IOPS allouées pour stocker des plages de 1:1–50:1. Pour plus d'informations, consultez Stockage d'instance de base de données Amazon RDS (p. 30).	22 août 2017
Nouvelle fonction	Vous pouvez désormais utiliser les déploiements Multi-AZ pour les instances de bases de données exécutant Microsoft SQL Server dans la région UE (Francfort). Pour plus d'informations, consultez Déploiements multi-AZ pour Microsoft SQL Server (p. 664).	3 août 2017
Nouvelle fonction	Vous pouvez désormais créer des instances de bases de données Amazon RDS qui exécutent les versions 10.1.23 et 10.0.31 de MariaDB. Pour plus d'informations, consultez Versions de MariaDB sur Amazon RDS (p. 544).	17 juillet 2017
Nouvelle fonction	Amazon RDS prend désormais en charge Microsoft SQL Server Enterprise Edition avec le modèle Licence incluse dans toutes les régions AWS. Pour plus d'informations, consultez Gestion des licences Microsoft SQL Server sur Amazon RDS (p. 617).	13 juillet 2017

Modifier	Description	Date de modification
Nouvelle fonction	Amazon RDS pour Oracle prend désormais en charge les grandes pages du noyau Linux pour obtenir une base de données plus évolutive. L'utilisation de grandes pages se traduit par des tables de page réduites et une réduction du temps UC de gestion de la mémoire, ce qui augmente les performances des instances de bases de données volumineuses. Vous pouvez utiliser les grandes pages avec vos instances de bases de données Amazon RDS qui exécutent toutes les éditions des versions 12.1.0.2 et 11.2.0.4 d'Oracle. Pour plus d'informations, consultez Utilisation de HugePages avec une instance de base de données Oracle (p. 954).	7 juillet 2017
Nouvelle fonction	Mise à jour pour la prise en charge du chiffrement au repos (EAR) pour les classes d'instance de base de données db.t2.small et db.t2.medium pour tous les moteurs de base de données autres qu'Aurora. Pour plus d'informations, consultez Disponibilité du chiffrement Amazon RDS (p. 1523).	27 juin 2017
Nouvelle fonction	Mise à jour pour prendre en charge Amazon Aurora dans la région Europe (Francfort). Pour plus d'informations, consultez Disponibilité pour Amazon Aurora MySQL.	16 juin 2017
Nouvelle fonction	Vous pouvez désormais spécifier un groupe d'options lorsque vous copiez un instantané de base de données d'une région AWS à une autre. Pour plus d'informations, consultez Considérations relatives au groupe d'options (p. 335).	12 juin 2017
Nouvelle fonction	Vous pouvez désormais copier des instantanés de base de données créés à partir d'instances de bases de données spécialisées d'une région AWS à une autre. Vous pouvez copier les instantanés à partir d'instances de bases de données qui utilisent Oracle TDE, Microsoft SQL Server TDE et Multi-AZ avec mise en miroir de Microsoft SQL Server. Pour plus d'informations, consultez Copie d'un instantané de base de données (p. 335).	12 juin 2017
Nouvelle fonction	Amazon Aurora vous permet désormais de copier rapidement et économiquement toutes vos bases de données dans un cluster de bases de données Amazon Aurora. Pour plus d'informations, consultez Clonage de base de données dans un cluster de base de données Aurora.	12 juin 2017
Nouvelle fonction	Amazon RDS prend désormais en charge Microsoft SQL Server 2016 SP1 CU2. Pour plus d'informations, consultez Microsoft SQL Server sur Amazon RDS (p. 592).	7 juin 2017
Nouvelle fonction	Amazon RDS pour Oracle a publié les versions 12.1.0.2.v8 et 11.2.0.4.v12 du moteur de base de données pour prendre en charge la mise à jour d'ensemble de correctifs (PSU) Oracle Database d'avril 2017. Pour plus d'informations, consultez Notes de mise à jour pour le moteur de base de données Oracle (p. 1208).	23 mai 2017

Modifier	Description	Date de modification
Nouvelle fonction	Amazon RDS prend désormais en charge les versions mineures 9.6.2, 9.5.6, 9.4.11 et 9.3.16 de PostgreSQL. Pour plus d'informations, consultez Versions de base de données PostgreSQL prises en charge (p. 1468)	3 mai 2017
Version préliminaire	Version préliminaire publique d'Amazon Aurora avec compatibilité PostgreSQL. Pour plus d'informations, consultez Utilisation de Amazon Aurora PostgreSQL.	19 avril 2017
Nouvelle fonction	Amazon Aurora vous permet désormais d'exécuter une opération ALTER TABLE tbl_name ADD COLUMN col_name column_definition pratiquement instantanément. L'opération s'effectue sans nécessiter la copie de la table et sans impact matériel sur les autres instructions DML. Pour plus d'informations, consultez Modification des tableaux dans Amazon Aurora à l'aide de Fast DDL.	5 avril 2017
Nouvelle fonction	Nous avons ajouté une nouvelle commande de surveillance, SHOW VOLUME STATUS, qui permet d'afficher le nombre de nœuds et de disques dans un volume. Pour plus d'informations, consultez Affichage du statut de volume pour un cluster de base de données Aurora.	5 avril 2017
Nouvelle fonction	Amazon RDS pour Oracle inclut maintenant la mise à jour d'ensemble de correctifs (PSU) Oracle Database de janvier 2017. Celle-ci ajoute la prise en charge pour les versions 12.1.0.2.v7 et 11.2.0.4.v11 du moteur de base de données Pour plus d'informations, consultez Notes de mise à jour pour le moteur de base de données Oracle (p. 1208).	21 mars 2017
Nouvelle fonction	Vous pouvez désormais utiliser votre propre logique personnalisée dans les fonctions de vérification de mot de passe personnalisé pour Oracle sur Amazon RDS. Pour plus d'informations, consultez Création de fonctions personnalisées pour vérifier les mots de passe (p. 1110).	21 mars 2017
Nouvelle fonction	Vous pouvez désormais accéder à vos fichiers de journalisation Redo en ligne et archivés sur vos instances de bases de données Oracle sur Amazon RDS. Pour plus d'informations, consultez Accès aux journaux de transactions (p. 1135).	21 mars 2017
Nouvelle fonction	Vous pouvez désormais copier des instantanés de cluster de bases de données chiffrés et non chiffrés entre les comptes d'une même région. Pour plus d'informations, consultez Copying a DB Cluster Snapshot Across Accounts (Copier une instantané de cluster de base de données entre plusieurs comptes).	7 mars 2017
Nouvelle fonction	Vous pouvez désormais partager des instantanés de cluster de bases de données chiffrés et non chiffrés entre les comptes d'une même région. Pour plus d'informations, consultez Sharing a DB Cluster Snapshot (Partager un instantané de cluster de base de données).	7 mars 2017

Modifier	Description	Date de modification
Nouvelle fonction	Vous pouvez désormais répliquer des clusters de base de données Amazon Aurora MySQL chiffrés pour créer des réplicas Aurora entre régions. Pour plus d'informations, consultez Réplication de clusters de base de données Aurora MySQL entre des régions AWS.	7 mars 2017
Nouvelle fonction	Vous pouvez désormais demander à ce que toutes les connexions de votre instance de base de données exécutant Microsoft SQL Server utilisent SSL (Secure Sockets Layer). Pour plus d'informations, consultez Utilisation de SSL avec une instance DB Microsoft SQL Server (p. 669).	27 février 2017
Nouvelle fonction	Vous pouvez désormais définir votre fuseau horaire local sur l'un 15 fuseaux horaires supplémentaires. Pour plus d'informations, consultez Fuseaux horaires pris en charge (p. 610).	27 février 2017
Nouvelle fonction	Vous pouvez désormais utiliser la procédure Amazon RDS `msdb.dbo.rds_shrink_tempdbfile` pour réduire la base de données tempdb sur vos instances de base de données exécutant Microsoft SQL Server. Pour plus d'informations, consultez Réduction de la base de données tempdb (p. 761).	17 février 2017
Nouvelle fonction	Vous pouvez désormais compresser vos fichiers de sauvegarde lorsque vous exportez votre base de données Microsoft SQL Server Enterprise and Standard Edition d'une instance de base de données Amazon RDS vers Amazon S3. Pour plus d'informations, consultez Compression des fichiers de sauvegarde (p. 650).	17 février 2017
Nouvelle fonction	Amazon RDS prend désormais en charge des serveurs DNS personnalisés pour résoudre des noms DNS utilisés dans l'accès réseau sortant sur vos instances de bases de données Oracle. Pour plus d'informations, consultez Configuration d'un serveur DNS personnalisé (p. 1114).	26 janvier 2017
Nouvelle fonction	Amazon RDS prend désormais en charge la création d'un réplica en lecture chiffré dans une autre région. Pour plus d'informations, consultez Création d'un réplica en lecture dans une autre région AWS (p. 284) et CreateDBInstanceReadReplica.	23 janvier 2017
Nouvelle fonction	Amazon RDS prend désormais en charge la mise à niveau d'un instantané de base de données MySQL de MySQL version 5.1 vers MySQL 5.5. Pour plus d'informations, consultez Mise à niveau d'un instantané de base de données MySQL (p. 813) et ModifyDBSnapshot.	20 janvier 2017

Modifier	Description	Date de modification
Nouvelle fonction	Amazon RDS prend désormais en charge la copie d'un instantané de base de données chiffré vers une autre région pour les moteurs de base de données MariaDB, MySQL, Oracle, PostgreSQL et Microsoft SQL Server. Pour plus d'informations, consultez Copie d'un instantané de base de données (p. 335) et CopyDBSnapshot.	20 décembre 2016
Nouvelle fonction	Amazon RDS prend désormais en charge la migration d'un instantané de base de données Amazon RDS MySQL 5.6 vers une nouvelle instance de base de données exécutant MariaDB 10.1. Pour plus d'informations, consultez Migration des données à partir d'un instantané de base de données MySQL vers une instance de base de données MariaDB (p. 568).	20 décembre 2016
Nouvelle fonction	Amazon Aurora MySQL prend désormais en charge l'indexation spatiale. L'indexation spatiale améliore les performances des requêtes sur des jeux de données volumineux pour les requêtes qui utilisent des données spatiales. Pour plus d'informations, consultez Amazon Aurora MySQL et données spatiales.	14 décembre 2016
Nouvelle fonction	Amazon RDS pour Oracle inclut désormais la mise à jour d'ensemble de correctifs (PSU) Oracle Database d'octobre 2016. Celle-ci ajoute la prise en charge pour les versions 12.1.0.2.v6 et 11.2.0.4.v10 du moteur de base de données Oracle. Pour plus d'informations, consultez Notes de mise à jour pour le moteur de base de données Oracle (p. 1208).	12 décembre 2016
Nouvelle fonction	Amazon RDS prend désormais en charge l'accès réseau sortant sur vos instances de bases de données exécutant Oracle. Vous pouvez utiliser utl_http, utl_tcp et utl_smtp pour vous connecter au réseau à partir de votre instance de base de données. Pour plus d'informations, consultez Utilisation de utl_http, utl_tcp et utl_smtp avec une instance de base de données Oracle (p. 957).	5 décembre 2016
Nouvelle fonction	Amazon RDS a annulé la prise en charge de la version 5.1 de MySQL. Cependant, vous pouvez restaurer des instantanés MySQL 5.1 sur une instance MySQL 5.5. Pour plus d'informations, consultez Moteurs de stockage pris en charge pour MySQL sur Amazon RDS (p. 785).	15 novembre 2016
Nouvelle fonction	Amazon RDS prend désormais en charge la version 9.6.1 de PostgreSQL. Pour plus d'informations, consultez PostgreSQL version 9.6.1 sur Amazon RDS (p. 1482).	11 novembre 2016
Nouvelle fonction	Amazon RDS prend désormais en charge Microsoft SQL Server 2016 RTM CU2. Pour plus d'informations, consultez Microsoft SQL Server sur Amazon RDS (p. 592).	4 novembre 2016

Modifier	Description	Date de modification
Nouvelle fonction	Amazon RDS prend désormais en charge les mises à niveau de version majeure pour les instances de bases de données exécutant Oracle. Vous pouvez désormais mettre à niveau vos instances de bases de données de 11g vers 12c. Pour plus d'informations, consultez Mise à niveau du moteur de base de données Oracle (p. 975).	2 novembre 2016
Nouvelle fonction	Vous pouvez désormais créer des instances de base de données exécutant Microsoft SQL Server 2014 Enterprise Edition. Amazon RDS prend désormais en charge SQL Server 2014 SP2 pour toutes les versions et toutes les régions. Pour plus d'informations, consultez Microsoft SQL Server sur Amazon RDS (p. 592).	25 octobre 2016
Nouvelle fonction	Amazon Aurora MySQL s'intègre désormais à d'autres services AWS : vous pouvez charger du texte ou des données au format XML dans un tableau à partir d'un compartiment Amazon S3 ou appeler une fonction AWS Lambda à partir d'un code de base de données. Pour plus d'informations consultez Intégration de Aurora MySQL avec d'autres services AWS.	18 octobre 2016
Nouvelle fonction	Vous pouvez maintenant accéder à la base de données tempdb sur vos instances de bases de données Amazon RDS exécutant Microsoft SQL Server. Vous pouvez accéder à la base de données tempdb à l'aide de Transact-SQL via Microsoft SQL Server Management Studio (SSMS) ou via toute autre application cliente SQL standard. Pour plus d'informations, consultez Accès à la base de données tempdb sur les instances de base de données Microsoft SQL Server sur Amazon RDS (p. 760).	29 septembre 2016
Nouvelle fonction	Vous pouvez désormais utiliser le package UTL_MAIL avec vos instances de bases de données Amazon RDS qui exécutent Oracle. Pour plus d'informations, consultez Oracle UTL_MAIL (p. 1093).	20 septembre 2016
Nouvelle fonction	Amazon RDS pour Oracle inclut maintenant la mise à jour d'ensemble de correctifs (PSU) Oracle Database de juillet 2016. Cette ajoute la prise en charge pour les versions 12.1.0.2.v5, 12.1.0.1.v6 et 11.2.0.4.v9 du moteur de base de données Oracle. Pour plus d'informations, consultez Notes de mise à jour pour le moteur de base de données Oracle (p. 1208).	20 septembre 2016
Nouvelles fonctions	Vous pouvez maintenant définir le fuseau horaire de vos nouvelles instances de bases de données Microsoft SQL Server sur un fuseau horaire local, correspondant à celui de vos applications. Pour plus d'informations, consultez Fuseau horaire local pour les instances de bases de données Microsoft SQL Server (p. 609).	19 septembre 2016

Modifier	Description	Date de modification
Nouvelles fonctions	Ajout de la prise en charge des nouvelles versions 9.5.4, 9.4.9 et 9.3.14 de PostgreSQL. Ajout également de la prise en charge de la réplication logique PostgreSQL, des déclencheurs d'événements PostgreSQL et du disque RAM pour le paramètre stats_temp_directory de PostgreSQL. Pour plus d'informations, consultez Versions de base de données PostgreSQL prises en charge (p. 1468), Réplication logique pour PostgreSQL sur Amazon RDS (p. 1510), Déclencheurs d'événements pour PostgreSQL sur Amazon RDS (p. 1512) et Disque RAM pour le stats_temp_directory (p. 1513).	14 septembre 2016
Nouvelle fonction	Vous pouvez désormais utiliser l'option Oracle Label Security pour contrôler l'accès aux lignes individuelles des tables dans vos instances de bases de données Amazon RDS exécutant Oracle 12c. Avec Oracle Label Security, vous pouvez garantir la conformité réglementaire à un modèle d'administration basé sur une stratégie et vous assurer que l'accès aux données sensibles est limité aux utilisateurs disposant du niveau d'autorisation approprié. Pour plus d'informations, consultez Oracle Label Security (p. 1054).	8 septembre 2016
Nouvelle fonction	Vous pouvez désormais vous connecter à un cluster de bases de données Amazon Aurora à l'aide du point de terminaison de lecteur, qui équilibre la charge des connexions entre les réplicas Aurora qui sont disponibles dans le cluster de bases de données. À mesure que les clients demandent de nouvelles connexions au point de terminaison de lecteur, Aurora répartit les demandes de connexion entre les réplicas Aurora dans le cluster de bases de données. Cette fonctionnalité peut aider à équilibrer votre charge de travail entre les différents réplicas Aurora de votre cluster de base de données. Pour plus d'informations, consultez Points de terminaison Amazon Aurora.	8 septembre 2016
Nouvelle fonction	Vous pouvez désormais prendre en charge le contrôle du cloud Oracle Enterprise Manager sur vos instances de bases de données Amazon RDS qui exécutent Oracle. Vous pouvez activer l'agent de gestion sur vos instances de bases de données et partager les données avec votre Oracle Management Service (OMS). Pour plus d'informations, consultez Oracle Management Agent pour Enterprise Manager Cloud Control (p. 1042).	1 septembre 2016
Nouvelle fonction	Cette version ajoute la prise en charge permettant d'obtenir un ARN pour une ressource. Pour plus d'informations, consultez Obtention d'un ARN existant (p. 302).	23 août 2016
Nouvelle fonction	Vous pouvez maintenant affecter jusqu'à 50 balises pour chacune des ressources Amazon RDS afin de gérer vos ressources et suivre les coûts. Pour plus d'informations, consultez Balisage de ressources Amazon RDS (p. 293).	19 août 2016

Modifier	Description	Date de modification
Nouvelle fonction	Amazon RDS prend désormais en charge le modèle « Licence incluse » pour Oracle Standard Edition Two. Pour de plus amples informations, veuillez consulter Création d'une instance de base de données Amazon RDS (p. 146). Vous pouvez désormais modifier le modèle de licence de vos instances de bases de données Amazon RDS exécutant Microsoft SQL Server et Oracle. Pour plus d'informations, consultez Gestion des licences Microsoft SQL Server sur Amazon RDS (p. 617) et Options de licence Oracle (p. 930).	5 août 2016
Nouvelle fonction	Vous pouvez désormais utiliser AWS Management Console pour déplacer facilement votre instance de base de données vers un autre VPC, ou un autre groupe de sous-réseaux du même VPC. Pour plus d'informations, consultez Mise à jour du VPC pour une instance de base de données (p. 1627). Si votre instance de base de données n'est pas dans un VPC, vous pouvez désormais utiliser AWS Management Console pour déplacer facilement votre instance de base de données vers un VPC. Pour plus d'informations, consultez Déplacement vers un VPC d'une instance de base de données n'appartenant pas à un VPC (p. 1627).	4 août 2016
Nouvelle fonction	Amazon RDS prend désormais en charge les sauvegarde et restauration natives pour les bases de données Microsoft SQL Server à l'aide de fichiers de sauvegarde complète (fichiers .bak). Vous pouvez désormais facilement migrer les bases de données SQL Server vers Amazon RDS et importer et exporter des bases de données dans un seul fichier facilement transférable, à l'aide de Amazon S3 pour le stockage et de AWS KMS pour le chiffrement. Pour plus d'informations, consultez Importation et exportation de bases de données SQL Server (p. 634).	27 juillet 2016
Nouvelle fonction	Vous pouvez désormais copier les fichiers source à partir d'une base de données MySQL dans un compartiment Amazon Simple Storage Service (Amazon S3), puis restaurer un cluster DB Amazon Aurora à partir de ces fichiers. Cette option peut être considérablement plus rapide que la migration des données à l'aide de `mysqldump`. Pour plus d'informations, consultez Migration des données d'une base de données MySQL externe vers un cluster de bases de données Aurora MySQL.	20 juillet 2016
Nouvelle fonction	Vous pouvez maintenant restaurer un instantané non chiffré de cluster de base de données Amazon Aurora pour créer un cluster de base de données Amazon Aurora chiffré en incluant une clé de chiffrement AWS Key Management Service (AWS KMS) au cours de l'opération de restitution. Pour plus d'informations, consultez Chiffrer des ressources Amazon RDS.	30 juin 2016

Modifier	Description	Date de modification
Nouvelle fonction	Amazon RDS pour Oracle inclut maintenant la mise à jour d'ensemble de correctifs (PSU) Oracle Database d'avril 2016. Cette PSU ajoute la prise en charge pour les versions 12.1.0.2.v4, 12.1.0.1.v5 et 11.2.0.4.v8 du moteur de base de données Oracle. Pour plus d'informations, consultez Notes de mise à jour pour le moteur de base de données Oracle (p. 1208).	17 juin 2016
Nouvelle fonction	Vous pouvez employer l'utilitaire Oracle Repository Creation Utility (RCU) pour créer un référentiel sur Amazon RDS pour Oracle. Pour plus d'informations, consultez Utilisation de l'utilitaire Oracle Repository Creation Utility sur Amazon RDS pour Oracle (p. 1200).	17 juin 2016
Nouvelle fonction	Ajout de la prise en charge des réplicas en lecture PostgreSQL entre régions. Pour plus d'informations, consultez Création d'un réplica en lecture dans une autre région AWS (p. 284).	16 juin 2016
Nouvelle fonction	Vous pouvez désormais utiliser AWS Management Console pour ajouter facilement Multi-AZ avec la mise en miroir à une instance de base de données Microsoft SQL Server. Pour plus d'informations, consultez Ajout d'un déploiement multi-AZ à une instance de base de données Microsoft SQL Server (p. 665).	9 juin 2016
Nouvelle fonction	Vous pouvez désormais utiliser les déploiements Multi-AZ à l'aide de la mise en miroir SQL Server dans les régions supplémentaires suivantes : Asie-Pacifique (Sydney), Asie-Pacifique (Tokyo) et Amérique du Sud (Sao Paulo). Pour plus d'informations, consultez Déploiements multi-AZ pour Microsoft SQL Server (p. 664).	9 juin 2016
Nouvelle fonction	Mis à jour pour prendre en charge la version 10.1 de MariaDB. Pour plus d'informations, consultez MariaDB sur Amazon RDS (p. 542).	1 juin 2016
Nouvelle fonction	Mise à jour pour prendre en charge les clusters de bases de données Amazon Aurora entre régions qui sont des réplicas en lecture. Pour plus d'informations, consultez Réplication de clusters de base de données Aurora MySQL entre des régions AWS.	1 juin 2016
Nouvelle fonction	La surveillance améliorée est disponible pour les instances de bases de données Oracle. Pour plus d'informations, consultez Surveillance améliorée (p. 394) et Modification d'une instance de base de données Amazon RDS (p. 243).	27 mai 2016
Nouvelle fonction	Mise à jour pour prendre en charge le partage manuel d'instantanés pour les instantanés de cluster DB Amazon Aurora. Pour plus d'informations, consultez Sharing a DB Cluster Snapshot (Partager un instantané de cluster de base de données).	18 mai 2016

Modifier	Description	Date de modification
Nouvelle fonction	Vous pouvez désormais utiliser le plug-in d'audit MariaDB pour vous connecter à l'activité de base de données sur les instances de bases de données MariaDB et MySQL. Pour plus d'informations, consultez Options pour le moteur de base de données MariaDB (p. 581) et Options pour les instances de base de données MySQL (p. 873).	27 avril 2016
Nouvelle fonction	Les mises à niveau de version majeure sur place sont désormais disponibles pour la mise à niveau de la version 5.6 vers la version 5.7 de MySQL. Pour plus d'informations, consultez Mise à niveau du moteur de base de données MySQL (p. 804).	26 avril 2016
Nouvelle fonction	La supervision améliorée est disponible pour les instances de bases de données Microsoft SQL Server. Pour plus d'informations, consultez Surveillance améliorée (p. 394).	22 avril 2016
Nouvelle fonction	Ajout de la prise en charge des versions 9.5.2, 9.4.7 et 9.3.12 de PostgreSQL. Pour plus d'informations, consultez Versions de base de données PostgreSQL prises en charge (p. 1468).	8 avril 2016
Nouvelle fonction	Mise à jour pour prendre en charge la base de données Oracle versions 11.2.0.4.v7, 12.1.0.1.v4 et 12.1.0.2.v3 avec les mises à jour d'ensemble de correctifs (PSU) Oracle de janvier 2016. Pour plus d'informations, consultez Notes de mise à jour pour le moteur de base de données Oracle (p. 1208).	1 avril 2016
Nouvelle fonction	Mis à jour pour fournir un affichage Amazon Aurora Clusters dans la console Amazon RDS. Pour plus d'informations, consultez Affichage d'un cluster de base de données Aurora.	1 avril 2016
Nouvelle fonction	Mise à jour pour prendre en charge SQL Server Multi-AZ avec la mise en miroir dans la région Asie-Pacifique (Séoul). Pour plus d'informations, consultez Déploiements multi-AZ pour Microsoft SQL Server (p. 664).	31 mars 2016
Nouvelle fonction	Mise à jour pour prendre en charge Amazon Aurora Multi-AZ avec la mise en miroir dans la région Asie-Pacifique (Séoul). Pour plus d'informations, consultez Disponibilité pour Amazon Aurora MySQL.	31 mars 2016
Nouvelle fonction	Les instances de bases de données PostgreSQL peuvent exiger des connexions pour utiliser SSL. Pour plus d'informations, consultez Utilisation de SSL avec une instance de base de données PostgreSQL (p. 1515).	25 mars 2016
Nouvelle fonction	La supervision améliorée est disponible pour les instances de bases de données PostgreSQL. Pour plus d'informations, consultez Surveillance améliorée (p. 394).	25 mars 2016

Modifier	Description	Date de modification
Nouvelle fonction	Les instances de bases de données Microsoft SQL Server peuvent désormais utiliser l'authentification Windows pour l'authentification utilisateur. Pour plus d'informations, consultez Utilisation de l'authentification Windows avec une instance de base de données Amazon RDS pour SQL Server (p. 676).	23 mars 2016
Nouvelle fonction	La supervision améliorée est disponible dans la région Asie-Pacifique (Séoul). Pour plus d'informations, consultez Surveillance améliorée (p. 394).	16 mars 2016
Nouvelle fonction	Vous pouvez désormais personnaliser l'ordre dans lequel les réplicas Aurora sont promus sur l'instance principale lors d'un basculement. Pour plus d'informations, consultez Tolérance aux pannes d'un cluster de base de données Aurora.	14 mars 2016
Nouvelle fonction	Mise à jour pour prendre en charge le chiffrement lors de la migration vers un cluster DB Aurora. Pour plus d'informations, consultez Migration de données à partir d'un cluster de base de données Aurora.	2 mars 2016
Nouvelle fonction	Mise à jour pour prendre en charge le fuseau horaire local pour les clusters de bases de données Aurora. Pour plus d'informations, consultez Fuseau horaire local pour les clusters de base de données Aurora.	1 mars 2016
Nouvelle fonction	Mise à jour pour ajouter la prise en charge pour MySQL version 5.7 pour les classes d'instance de base de données Amazon RDS de la génération actuelle.	22 février 2016
Nouvelle fonction	Mis à jour pour prendre en charge les classes d'instance de base de données db.r3 et db.t2 dans la région AWS GovCloud (US-West).	11 février 2016
Nouvelle fonction	Mise à jour pour prendre en charge le chiffrement des copies de snapshots DB et le partage des snapshots DB chiffrés. Pour plus d'informations, consultez Copie d'un instantané (p. 332) et Partage d'un instantané de de base de données (p. 342).	11 février 2016
Nouvelle fonction	Mise à jour pour prendre en charge Amazon Aurora dans la région Asie-Pacifique (Sydney). Pour plus d'informations, consultez Disponibilité pour Amazon Aurora MySQL.	11 février 2016
Nouvelle fonction	Mise à jour pour prendre en charge SSL pour les instances de bases de données Oracle. Pour plus d'informations, consultez Utilisation de SSL avec une instance de base de données Oracle (p. 937).	9 février 2016
Nouvelle fonction	Mise à jour pour prendre en charge le fuseau horaire local pour les instances de bases de données MySQL et MariaDB. Pour plus d'informations, consultez Fuseau horaire local pour les instances de bases de données MySQL (p. 791) et Fuseau horaire local pour les instances de base de données MariaDB (p. 554).	21 décembre 2015

Modifier	Description	Date de modification
Nouvelle fonction	Mise à jour pour prendre en charge la surveillance améliorée des métriques du système d'exploitation pour les instances de bases de données MySQL et MariaDB et les clusters de bases de données Aurora. Pour plus d'informations, consultez Affichage des métriques d'instances de base de données (p. 384).	18 décembre 2015
Nouvelle fonction	Mise à jour pour prendre en charge Oracle Standard Edition Two avec le modèle avec apport de sa propre licence (BYOL). Ajout également de la prise en charge pour Oracle versions 11.2.0.4.v5, 12.1.0.1.v3 et 12.1.0.2.v2. Pour plus d'informations, consultez Notes de mise à jour pour le moteur de base de données Oracle (p. 1208).	14 décembre 2015
Nouvelle fonction	Mis à jour pour prendre en charge les classes d'instance de base de données db.t2, db.r3 et db.m4 pour la version 5.5 de MySQL. Pour plus d'informations, consultez Classes d'instances de base de données (p. 6).	4 décembre 2015
Nouvelle fonction	Mise à jour pour prendre en charge la modification du port de base de données pour une instance de base de données existante.	3 décembre 2015
Nouvelle fonction	Mise à jour pour prendre en charge trois nouvelles extensions pour les instances de bases de données PostgreSQL versions 9.3.10 et 9.4.5. Pour plus d'informations, consultez Versions de base de données PostgreSQL prises en charge (p. 1468).	1 décembre 2015
Nouvelle fonction	Mise à jour pour prendre en charge les instances de bases de données PostgreSQL versions 9.3.10 et 9.4.5. Pour plus d'informations, consultez Versions de base de données PostgreSQL prises en charge (p. 1468).	27 novembre 2015
Nouvelle fonction	Mise à jour pour prendre en charge les mises à niveau de version majeure du moteur de base de données pour les instances PostgreSQL. Pour plus d'informations, consultez Mise à niveau du moteur de base de données PostgreSQL pour Amazon RDS (p. 1373).	19 novembre 2015
Nouvelle fonction	Mise à jour pour prendre en charge la modification de l'accessibilité publique d'une instance de base de données existante. Mise à jour pour prendre en charge les classes d'instance de base de données standard db.m4.	11 novembre 2015
Nouvelle fonction	Mise à jour pour prendre en charge le partage manuel d'un instantané de base de données. Pour plus d'informations, consultez Partage d'un instantané de de base de données (p. 342).	28 octobre 2015
Nouvelle fonction	Mise à jour pour prendre en charge Microsoft SQL Server 2014 pour les éditions Web, Express et Standard.	26 octobre 2015

Modifier	Description	Date de modification
Nouvelle fonction	Mise à jour pour prendre en charge le moteur de base de données MariaDB basé sur MySQL. Pour plus d'informations, consultez MariaDB sur Amazon RDS (p. 542).	7 octobre 2015
Nouvelle fonction	Mise à jour pour prendre en charge Amazon Aurora dans la région Asie-Pacifique (Tokyo). Pour plus d'informations, consultez Disponibilité pour Amazon Aurora MySQL.	7 octobre 2015
Nouvelle fonction	Mise à jour pour prendre en charge les classes d'instance de base de données avec capacité de transmission en rafales db.t2 pour tous les moteurs DB et l'ajout de la classe d'instance de base de données db.t2.large. Pour plus d'informations, consultez Classes d'instances de base de données (p. 6).	25 septembre 2015
Nouvelle fonction	Mise à jour pour prendre en charge les instances de bases de données Oracle sur les classes d'instance de base de données R3 et T2. Pour plus d'informations, consultez Classes d'instances de base de données (p. 6).	5 août 2015
Nouvelle fonction	Mise à jour pour prendre en charge PostgreSQL versions 9.4.4 et 9.3.9. Pour plus d'informations, consultez Versions de base de données PostgreSQL prises en charge (p. 1468).	30 juillet 2015
Nouvelle fonction	Microsoft SQL Server Enterprise Edition est désormais disponible avec le modèle de service « License Included » (licence incluse). Pour plus d'informations, consultez Gestion des licences Microsoft SQL Server sur Amazon RDS (p. 617).	29 juillet 2015
Nouvelle fonction	Amazon Aurora est officiellement disponible. Le moteur DB Amazon Aurora prend en charge plusieurs instances de bases de données dans un cluster DB. Pour plus d'informations, consultez Qu'est-ce qu'Amazon Aurora ?	27 juillet 2015
Nouvelle fonction	Mise à jour pour prendre en charge la copie des balises vers des snapshots DB.	20 juillet 2015
Nouvelle fonction	Mise à jour pour prendre en charge la base de données Oracle 12c version « 12.1.0.2 », dont l'option In-Memory, les correctifs PSU d'avril Oracle 11g et l'intégration améliorée avec AWS CloudHSM.	20 juillet 2015
Nouvelle fonction	Mise à jour pour prendre en charge les augmentations du volume de stockage pour tous les moteurs DB et une hausse des IOPS provisionnées pour SQL Server.	18 juin 2015
Nouvelle fonction	Mise à jour des options pour les instances de bases de données réservées.	15 juin 2015
Nouvelle fonction	Mise à jour pour prendre en charge Oracle version 12c.	2 avril 2015
Nouvelle fonction	Mise à jour pour prendre en charge PostgreSQL versions 9.3.6 et 9.4.1.	18 mars 2015

Modifier	Description	Date de modification
Nouvelle fonction	Mise à jour pour prendre en charge l'utilisation d'Amazon CloudHSM avec les instances de bases de données Oracle grâce à TDE.	8 janvier 2015
Nouvelle fonction	Mise à jour pour prendre en charge le chiffrement des données au repos et la nouvelle version de l'API 2014-10-31.	6 janvier 2015
Nouvelle fonction	Mise à jour pour prendre en charge Oracle version 11.2.0.4.v3 qui inclut la PSU publiée en octobre 2014.	20 novembre 2014
Nouvelle fonction	Mise à jour pour inclure le nouveau moteur DB Amazon : Aurora. Le moteur de base de données Amazon Aurora prend en charge plusieurs instances de base de données dans un cluster de base de données. Amazon Aurora est actuellement en pré-édition et est susceptible de changer. Pour plus d'informations, consultez Qu'est-ce qu'Amazon Aurora ?	12 novembre 2014
Nouvelle fonction	Mise à jour pour prendre en charge les réplicas en lecture PostgreSQL.	10 novembre 2014
Nouvelles fonctions	Mise à jour pour prendre en charge Oracle 11.2.0.4v2.	16 octobre 2014
Nouvelles API et fonctions	Mise à jour pour prendre en charge le type de stockage GP2 et la nouvelle version de l'API 2014-09-01. Mise à jour pour prendre en charge la copie d'une option existante ou d'un groupe de paramètres pour créer une nouvelle option ou un groupe de paramètres.	7 octobre 2014
Nouvelle fonction	Mise à jour pour prendre en charge la préparation du cache InnoDB pour les instances de bases de données exécutant MySQL version 5.6.19 et ultérieure.	3 septembre 2014
Nouvelle fonction	Mise à jour pour prendre en charge la vérification du certificat SSL lors de la connexion aux moteurs de base de données MySQL (version 5.6), SQL Server et PostgreSQL.	5 août 2014
Nouvelle fonction	Mise à jour pour prendre en charge les classes d'instance de base de données avec capacité de transmission en rafales db.t2.	4 août 2014
Nouvelle fonction	Mise à jour pour prendre en charge les classes d'instance de base de données optimisées pour la mémoire db.r3 à utiliser avec les moteurs de base de données MySQL (version 5.6), SQL Server et PostgreSQL.	28 mai 2014
Nouvelle fonction	Mise à jour pour prendre en charge les déploiements multi-AZ SQL Server grâce à la mise en miroir SQL Server.	19 mai 2014
Nouvelle fonction	Mise à jour pour prendre en charge les mises à niveau MySQL version 5.5 à 5.6.	23 avril 2014
Nouvelle fonction	Mise à jour pour prendre en charge Oracle 11.2.0.4.	23 avril 2014
Nouvelle fonction	Mise à jour pour prendre en charge Oracle GoldenGate.	3 avril 2014

Modifier	Description	Date de modification
Nouvelle fonction	Mise à jour pour prendre en charge les classes d'instances de bases de données M3.	20 février 2014
Nouvelle fonction	Mise à jour pour prendre en charge l'option Oracle Timezone.	13 janvier 2014
Nouvelle fonction	Mise à jour pour prendre en charge la réplication entre les instances de bases de données MySQL Amazon RDS dans différentes régions.	26 novembre 2013
Nouvelle fonction	Mise à jour pour prendre en charge le moteur DB PostgreSQL.	14 novembre 2013
Nouvelle fonction	Mise à jour pour prendre en charge le chiffrement TDE (Transparent Data Encryption) SQL Server.	7 novembre 2013
Nouvelles API et fonction	Mise à jour pour prendre en charge les copies d'instantané de base de données entre régions ; la nouvelle version de l'API 2013-09-09.	31 octobre 2013
Nouvelles fonctions	Mise à jour pour prendre en charge Oracle Statspack.	26 septembre 2013
Nouvelles fonctions	Mis à jour pour prendre en charge l'usage de la réplication d'importation ou d'exportation de données entre des instances de MySQL s'exécutant dans Amazon RDS et des instances de MySQL s'exécutant sur site ou sur Amazon EC2.	5 septembre 2013
Nouvelles fonctions	Mise à jour pour prendre en charge la classe d'instance de base de données db.cr1.8xlarge pour MySQL 5.6.	4 septembre 2013
Nouvelle fonction	Mise à jour pour prendre en charge la réplication des réplicas en lecture.	28 août 2013
Nouvelle fonction	Mise à jour pour prendre en charge la création parallèle de réplicas en lecture.	22 juillet 2013
Nouvelle fonction	Mise à jour pour prendre en charge les autorisations et le balisage précis pour toutes les ressources Amazon RDS.	8 juillet 2013
Nouvelle fonction	Mise à jour pour prendre en charge MySQL 5.6 pour de nouvelles instances, dont la prise en charge pour l'interface memcached MySQL 5.6 et l'accès au journal binaire.	1 juillet 2013
Nouvelle fonction	Mise à jour pour prendre en charge les mises à niveau de version majeure MySQL 5.1 à 5.5.	20 juin 2013
Nouvelle fonction	Mise à jour des groupes de paramètres de base de données pour autoriser des expressions pour des valeurs de paramètres.	20 juin 2013
Nouvelles API et fonction	Mise à jour pour prendre en charge le statut du réplica en lecture, et nouvelle version d'API, 2013-05-15.	23 mai 2013
Nouvelles fonctions	Mise à jour pour prendre en charge les fonctions Oracle Advanced Security pour le chiffrement réseau natif et Oracle TDE.	18 avril 2013

Modifier	Description	Date de modification
Nouvelles fonctions	Mise à jour pour prendre en charge les mises à niveau de version majeure pour SQL Server et une fonctionnalité supplémentaire pour les IOPS provisionnées.	13 mars 2013
Nouvelle fonction	Mise à jour pour prendre en charge VPC par défaut pour RDS.	11 mars 2013
Nouvelles API et fonction	Mise à jour pour prendre en charge l'accès au journal ; la nouvelle version de l'API 2013-02-12	4 mars 2013
Nouvelle fonction	Mise à jour pour prendre en charge les abonnements aux notifications d'événements RDS.	4 février 2013
Nouvelles API et fonction	Mise à jour pour prendre en charge le renommage d'une instance de base de données et la migration des membres du groupe de sécurité DB d'un VPC vers un groupe de sécurité VPC.	14 janvier 2013
Nouvelle fonction	Mise à jour pour prendre en charge la région AWS GovCloud (US-West).	17 décembre 2012
Nouvelle fonction	Mise à jour pour prendre en charge les classes d'instance de base de données m1.medium et m1.xlarge.	6 novembre 2012
Nouvelle fonction	Mise à jour pour prendre en charge la promotion des réplicas en lecture.	11 octobre 2012
Nouvelle fonction	Mise à jour pour prendre en charge SSL dans les instances de bases de données Microsoft SQL Server.	10 octobre 2012
Nouvelle fonction	Mise à jour pour prendre en charge les micro-instances de bases de données Oracle.	27 septembre 2012
Nouvelle fonction	Mise à jour pour prendre en charge SQL Server 2012.	26 septembre 2012
Nouvelles API et fonction	Mise à jour pour prendre en charge les IOPS provisionnées. Version de l'API 2012-09-17.	25 septembre 2012
Nouvelles fonctions	Mise à jour pour prendre en charge SQL Server pour les instances de bases de données dans VPC et Oracle pour Data Pump.	13 septembre 2012
Nouvelle fonction	Mise à jour pour prendre en charge SQL Server Agent.	22 août 2012
Nouvelle fonction	Mise à jour pour prendre en charge le balisage des instances de bases de données.	21 août 2012
Nouvelles fonctions	Mise à jour pour prendre en charge Oracle APEX et XML DB, les fuseaux horaires Oracle et les instances de bases de données Oracle dans un VPC.	16 août 2012
Nouvelles fonctions	Mise à jour pour prendre en charge SQL Server Database Engine Tuning Advisor et les instances de bases de données Oracle dans VPC.	18 juillet 2012
Nouvelle fonction	Mise à jour pour prendre en charge les groupes d'options et la première option, Oracle Enterprise Manager Database Control.	29 mai 2012

Modifier	Description	Date de modification
Nouvelle fonction	Mise à jour pour prendre en charge les réplicas en lecture dans Amazon Virtual Private Cloud.	17 mai 2012
Nouvelle fonction	Mise à jour pour prendre en charge Microsoft SQL Server.	8 mai 2012
Nouvelles fonctions	Mise à jour pour prendre en charge le basculement forcé, le déploiement multi-AZ des instances de bases de données Oracle et les jeux de caractères personnalisés pour les instances de bases de données Oracle.	2 mai 2012
Nouvelle fonction	Mise à jour pour prendre en charge Amazon Virtual Private Cloud (VPC).	13 février 2012
Contenu mis à jour	Mise à jour pour de nouveaux types d'instance réservée.	19 décembre 2011
Nouvelle fonction	Mise à jour pour prendre en charge le moteur Oracle.	23 mai 2011
Contenu mis à jour	Mises à jour de la console.	13 mai 2011
Contenu mis à jour	Contenu modifié pour une sauvegarde et des fenêtres de maintenance plus courtes.	28 février 2011
Nouvelle fonction	Ajout de la prise en charge pour MySQL 5.5.	31 janvier 2011
Nouvelle fonction	Ajout de la prise en charge des réplicas en lecture.	4 octobre 2010
Nouvelle fonction	Ajout de la prise en charge pour AWS Identity and Access Management (IAM).	2 septembre 2010
Nouvelle fonction	Ajout de la gestion de version du moteur DB.	16 août 2010
Nouvelle fonction	Ajout d'instances de bases de données réservées.	16 août 2010
Nouvelle fonction	Amazon RDS prend désormais en charge les connexions SSL vers les instances de bases de données.	28 juin 2010
Nouveau Guide	Il s'agit de la première version du manuel Amazon RDS Guide de l'utilisateur.	7 juin 2010

Glossaire AWS

Pour la terminologie AWS la plus récente, consultez le Glossaire AWS dans le document AWS General Reference.