ATTACK DEFENSE

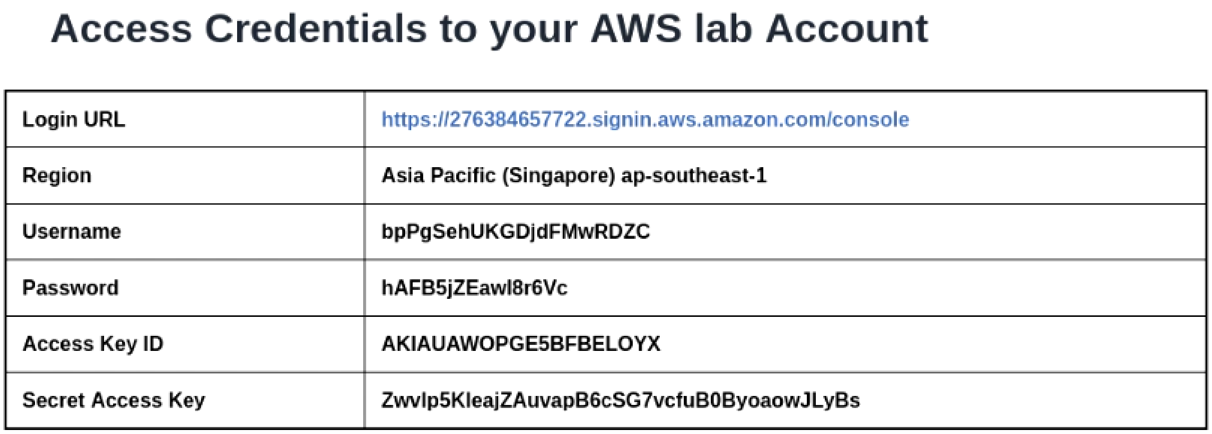
by PentesterAcademy

Name	Database Enumeration
URL	https://attackdefense.com/challengedetails?cid=2297
Type	AWS Cloud Security : Databases

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

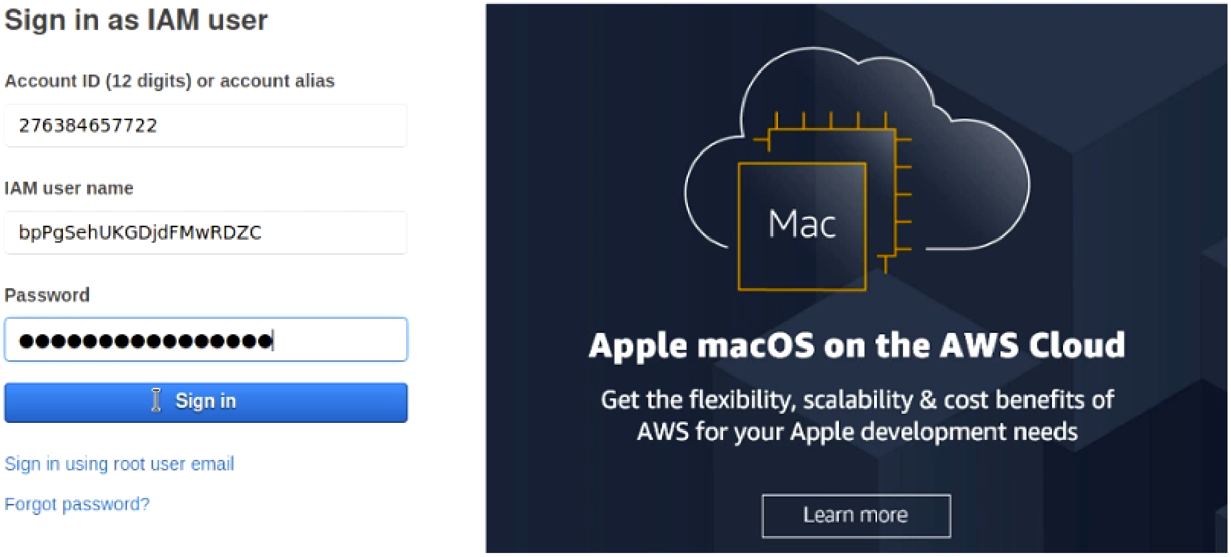
Solution:

Step 1: Sign in into AWS console with AWS access credentials



Access Credentials to your AWS lab Account

Login URL	https://276384657722.signin.aws.amazon.com/console
Region	Asia Pacific (Singapore) ap-southeast-1
Username	bpPgSehUKGDjdFMwRDZC
Password	hAFB5jZEawl8r6Vc
Access Key ID	AKIAUAWOPGE5BFBELOYX
Secret Access Key	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



Sign in as IAM user

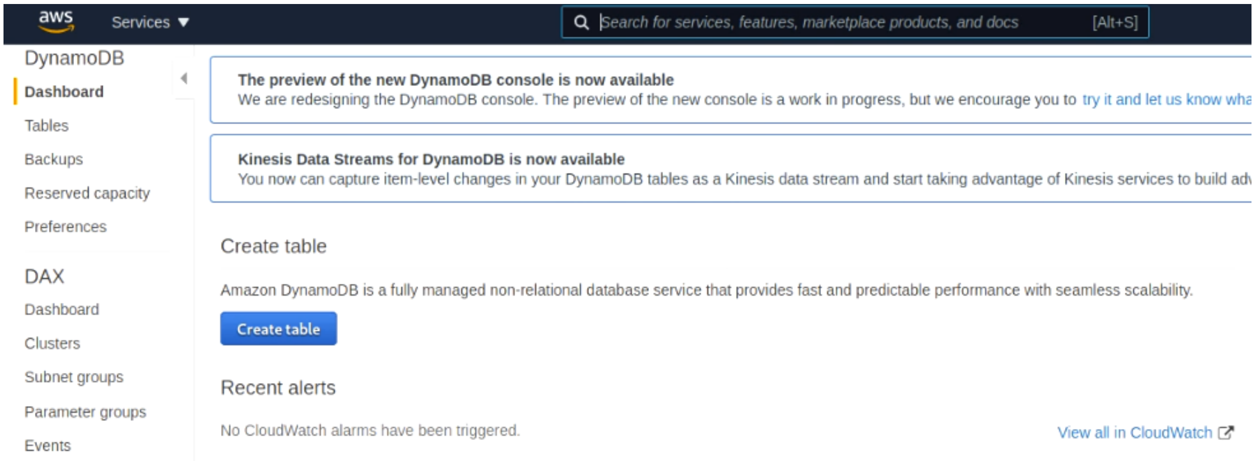
Account ID (12 digits) or account alias: 276384657722

IAM user name: bpPgSehUKGDjdFMwRDZC

Password: ●●●●●●●●●●●●●●●●

Sign in
Sign in using root user email
Forgot password?
Mac
Apple macOS on the AWS Cloud
Get the flexibility, scalability & cost benefits of AWS for your Apple development needs
Learn more

Step 2: Navigate to DynamoDB dashboard.



The preview of the new DynamoDB console is now available
We are redesigning the DynamoDB console. The preview of the new console is a work in progress, but we encourage you to try it and let us know wha

Kinesis Data Streams for DynamoDB is now available
You now can capture item-level changes in your DynamoDB tables as a Kinesis data stream and start taking advantage of Kinesis services to build adv

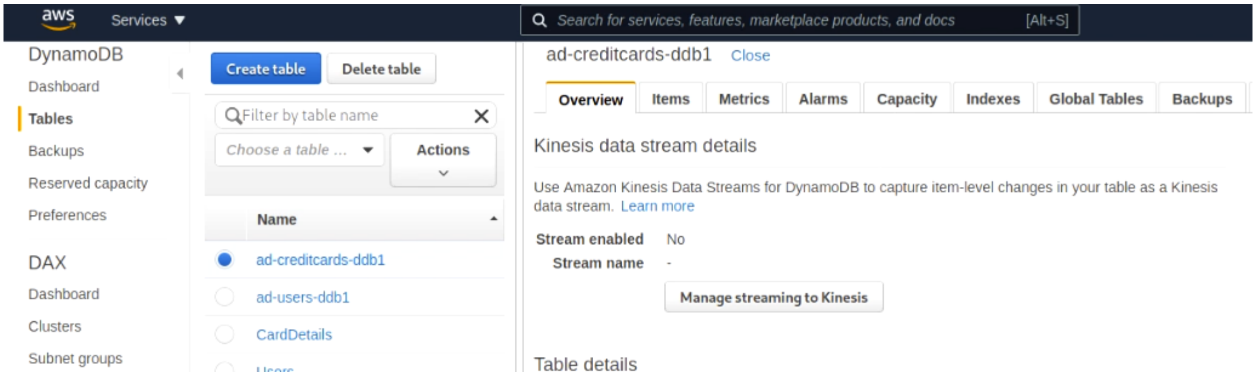
Create table

Amazon DynamoDB is a fully managed non-relational database service that provides fast and predictable performance with seamless scalability.

Recent alerts

No CloudWatch alarms have been triggered.

Click on Tables present in the left pane.



Kinesis data stream details

Use Amazon Kinesis Data Streams for DynamoDB to capture item-level changes in your table as a Kinesis data stream. Learn more

Stream enabled	No
Stream name	-

Table details

Check table details.

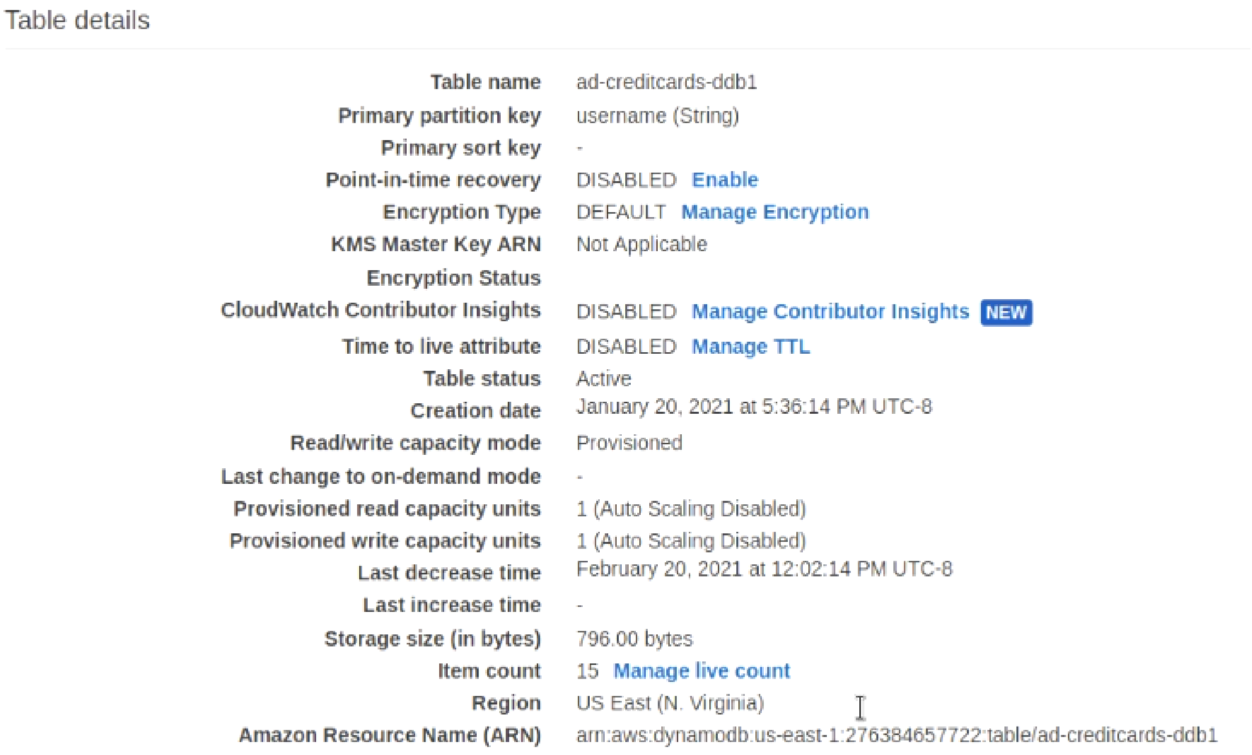
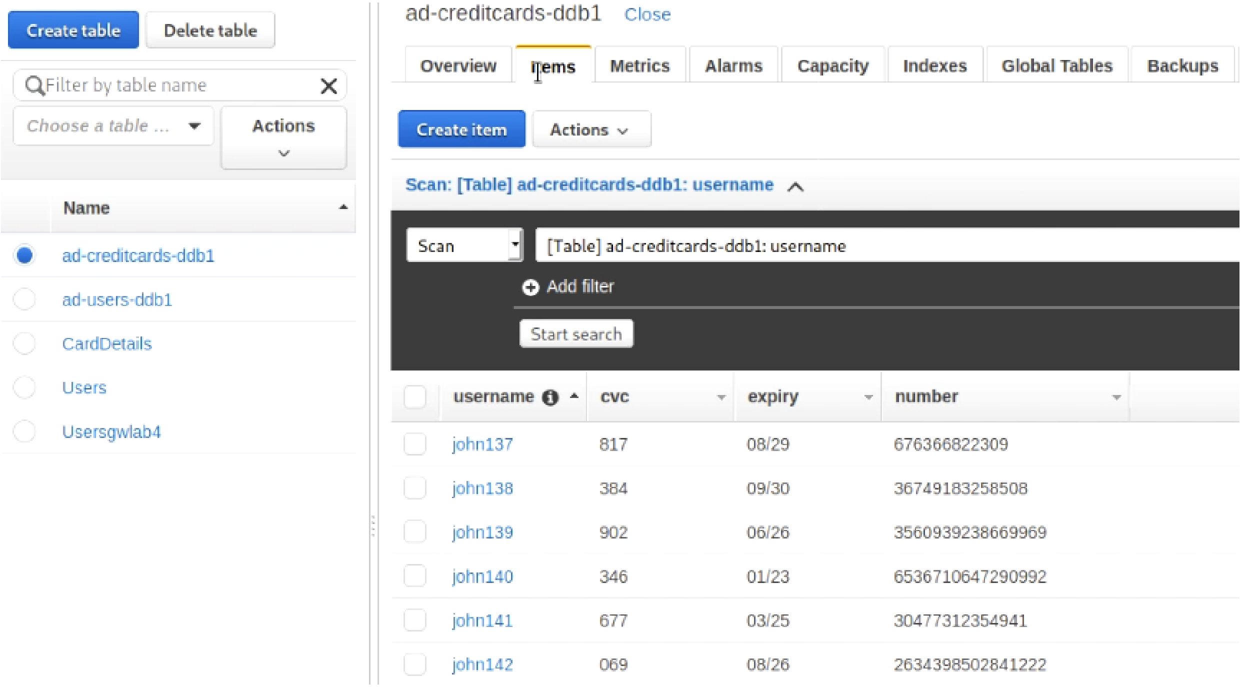


Table details

Table name	ad-creditcards-ddb1
Primary partition key	username (String)
Primary sort key	-
Point-in-time recovery	DISABLED Enable
Encryption Type	DEFAULT Manage Encryption
KMS Master Key ARN	Not Applicable
Encryption Status	
CloudWatch Contributor Insights	DISABLED Manage Contributor Insights NEW
Time to live attribute	DISABLED Manage TTL
Table status	Active
Creation date	January 20, 2021 at 5:36:14 PM UTC-8
Read/write capacity mode	Provisioned
Last change to on-demand mode	-
Provisioned read capacity units	1 (Auto Scaling Disabled)
Provisioned write capacity units	1 (Auto Scaling Disabled)
Last decrease time	February 20, 2021 at 12:02:14 PM UTC-8
Last increase time	-
Storage size (in bytes)	796.00 bytes
Item count	15 Manage live count
Region	US East (N. Virginia)
Amazon Resource Name (ARN)	arn:aws:dynamodb:us-east-1:276384657722:table/ad-creditcards-ddb1

Step 3: Click on Items tab to see table items.



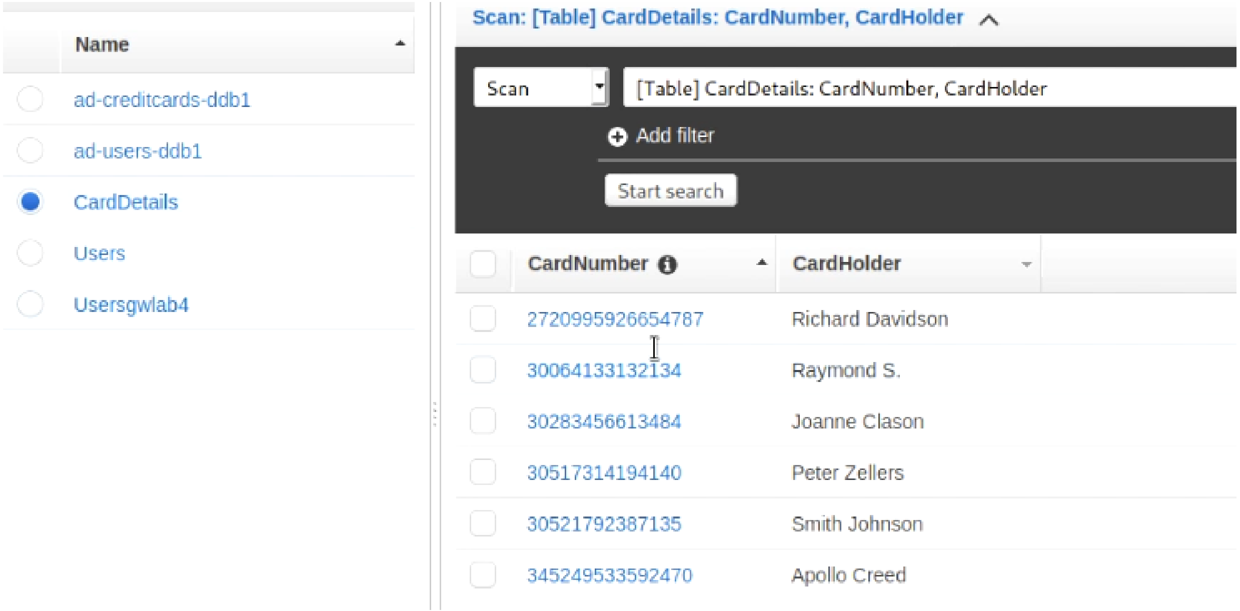
Name
● ad-creditcards-ddb1
○ ad-users-ddb1
○ CardDetails
○ Users
○ Usersgwlab4

ad-creditcards-ddb1

Scan: [Table] ad-creditcards-ddb1: username

Scan [Table] ad-creditcards-ddb1: username

username	cvc	expiry	number
john137	817	08/29	676366822309
john138	384	09/30	36749183258508
john139	902	06/26	3560939238669969
john140	346	01/23	6536710647290992
john141	677	03/25	30477312354941
john142	069	08/26	2634398502841222

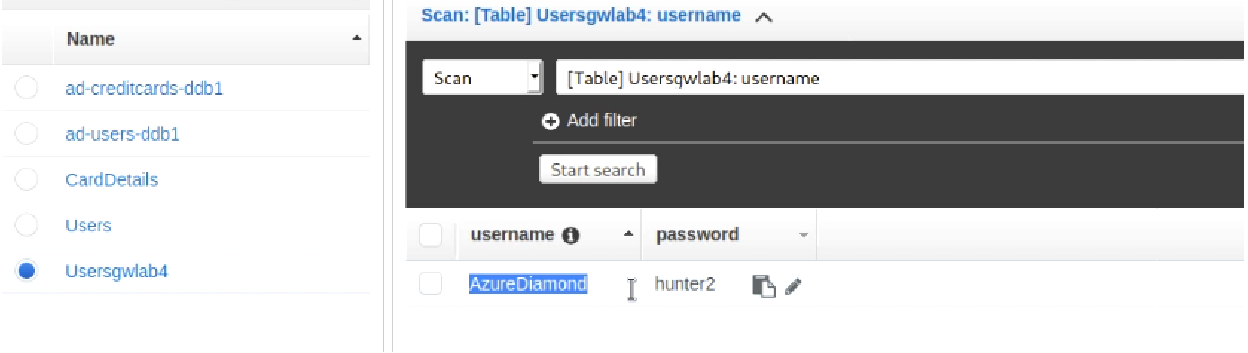


Name
○ ad-creditcards-ddb1
○ ad-users-ddb1
● CardDetails
○ Users
○ Usersgwlab4

Scan: [Table] CardDetails: CardNumber, CardHolder

Scan [Table] CardDetails: CardNumber, CardHolder

CardNumber	CardHolder
2720995926654787	Richard Davidson
30064133132134	Raymond S.
30283456613484	Joanne Clason
30517314194140	Peter Zellers
30521792387135	Smith Johnson
345249533592470	Apollo Creed

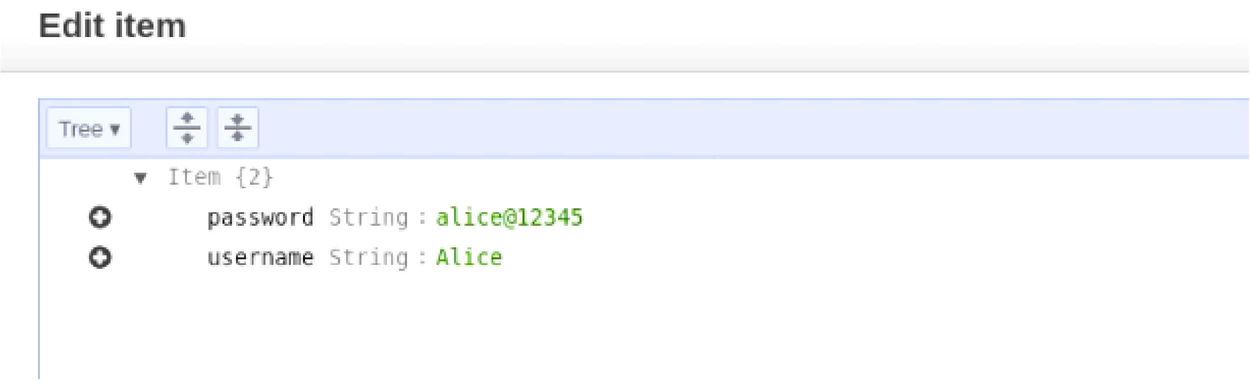


Name
○ ad-creditcards-ddb1
○ ad-users-ddb1
○ CardDetails
○ Users
● Usersgwlab4

Scan: [Table] Usersgwlab4: username

username	password
AzureDiamond	hunter2

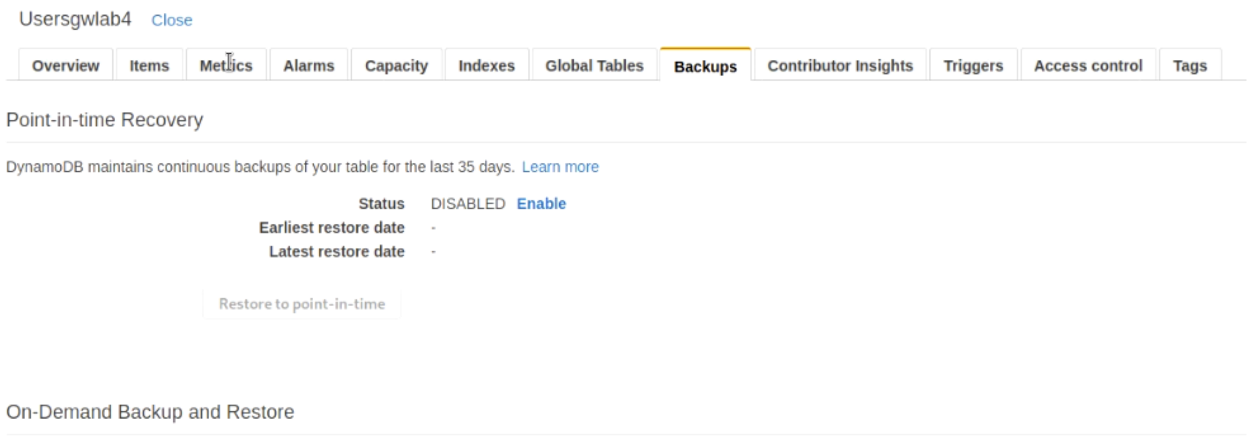
Step 4: Click on the item to check item details.



Edit item

```
▾ Item {2}
    password String : alice@12345
    username String : Alice
```

Step 5: Check for table backup.



Usersgwlab4 Close

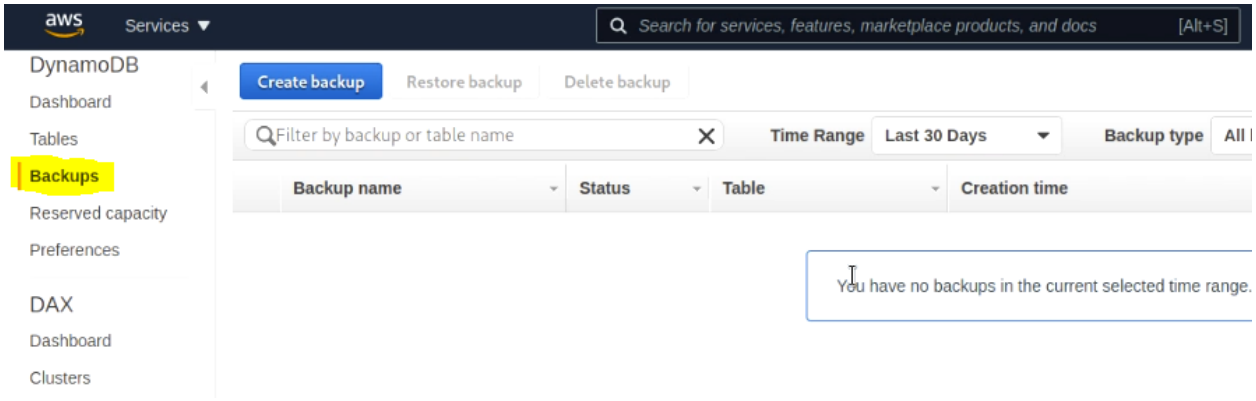
Point-in-time Recovery

DynamoDB maintains continuous backups of your table for the last 35 days. Learn more

Status	DISABLED Enable
Earliest restore date	-
Latest restore date	-

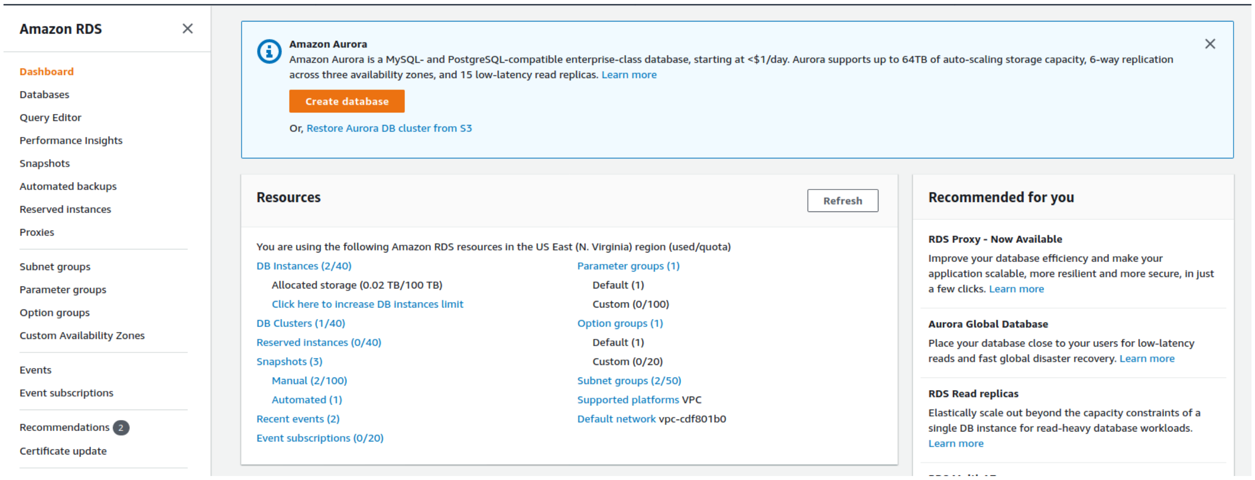
On-Demand Backup and Restore

Step 6: Click on the Backups button on the left pane to check DB backups.



You have no backups in the current selected time range.

Step 7: Navigate to amazon RDS dashboard.



Amazon Aurora

Amazon Aurora is a MySQL- and PostgreSQL-compatible enterprise-class database, starting at <$1/day. Aurora supports up to 64TB of auto-scaling storage capacity, 6-way replication across three availability zones, and 15 low-latency read replicas. Learn more

Or, Restore Aurora DB cluster from S3

Resources

You are using the following Amazon RDS resources in the US East (N. Virginia) region (used/quota)

DB Instances (2/40)	Parameter groups (1)
Allocated storage (0.02 TB/100 TB)	Default (1)
Click here to increase DB instances limit	Custom (0/100)
DB Clusters (1/40)	Option groups (1)
Reserved instances (0/40)	Default (1)
Snapshots (3)	Custom (0/20)
Manual (2/100)	Subnet groups (2/50)
Automated (1)	Supported platforms VPC
Recent events (2)	Default network vpc-cdf801b0
Event subscriptions (0/20)	

Recommended for you

RDS Proxy - Now Available

Improve your database efficiency and make your application scalable, more resilient and more secure, in just a few clicks. Learn more

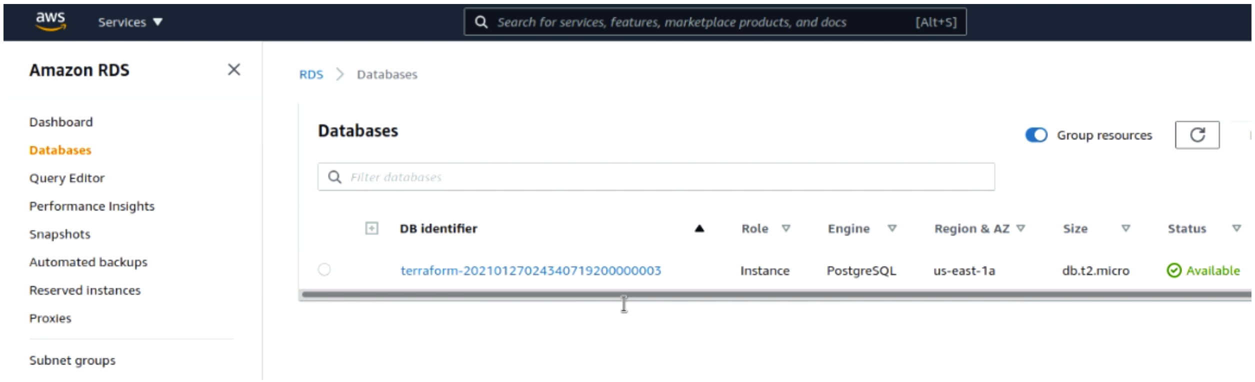
Aurora Global Database

Place your database close to your users for low-latency reads and fast global disaster recovery. Learn more

RDS Read replicas

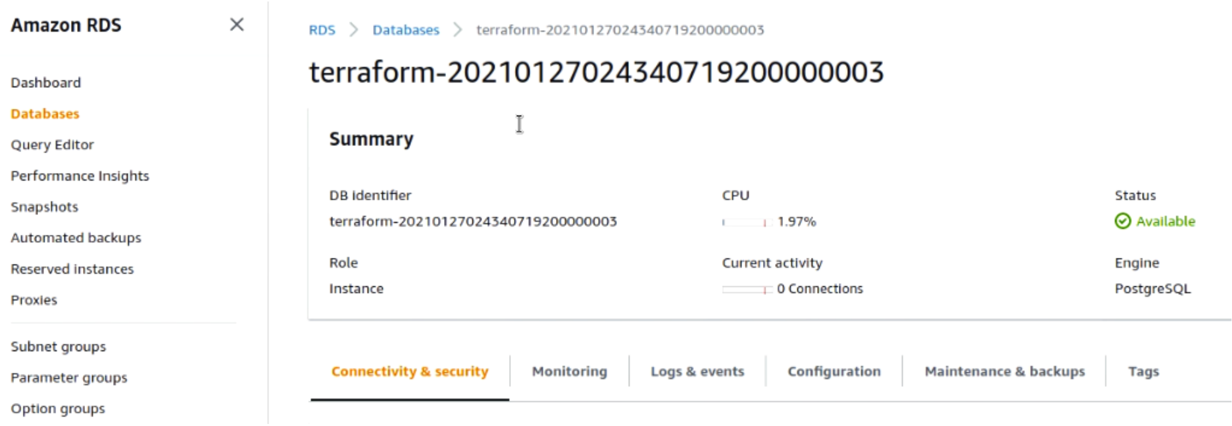
Elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. Learn more

Step 8: Click on Databases option present in left pane.



DB identifier	Role	Engine	Region & AZ	Size	Status
terraform-20210127024340719200000003	Instance	PostgreSQL	us-east-1a	db.t2.micro	Available

Step 9: Click on DB identifier to check more details.

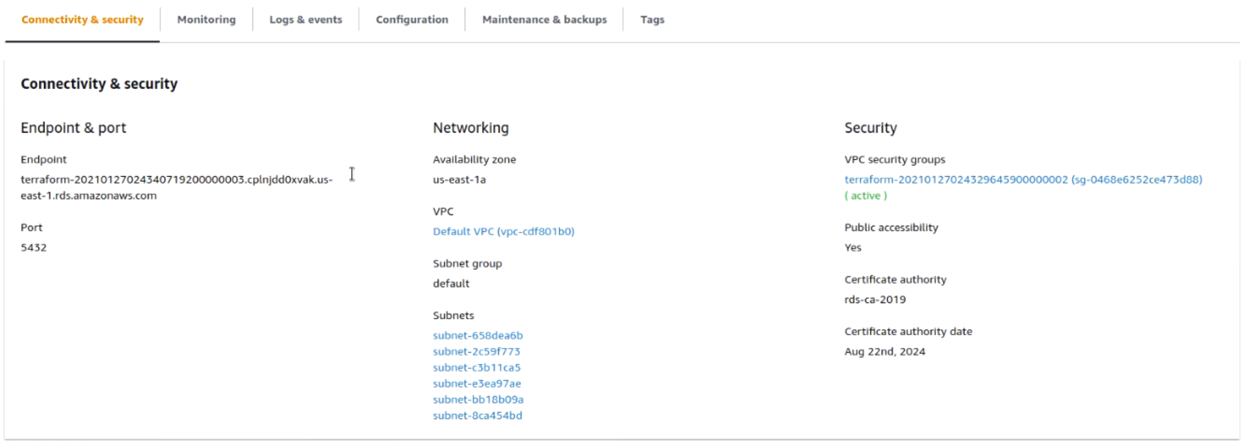


terraform-20210127024340719200000003

Summary

DB identifier: terraform-20210127024340719200000003
CPU: 1.97%
Status: Available
Role: Instance
Current activity: 0 Connections
Engine: PostgreSQL

Check connectivity configurations.



Connectivity & security

Endpoint & port

Endpoint
terraform-20210127024340719200000003.cplnjdd0xvak.us-east-1.rds.amazonaws.com

Port
5432

Networking

Availability zone
us-east-1a

VPC
Default VPC (vpc-cdf801b0)

Subnet group
default

Subnets
subnet-658dea6b
subnet-2c59f773
subnet-c3b11ca5
subnet-e3ea97ae
subnet-bb18b09a
subnet-8ca454bd

Security

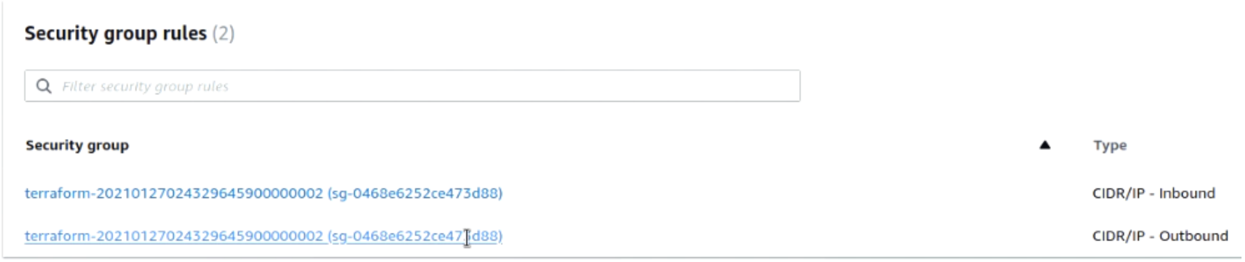
VPC security groups
terraform-20210127024329645900000002 (sg-0468e6252ce473d88)
(active)

Public accessibility
Yes

Certificate authority
rds-ca-2019

Certificate authority date
Aug 22nd, 2024

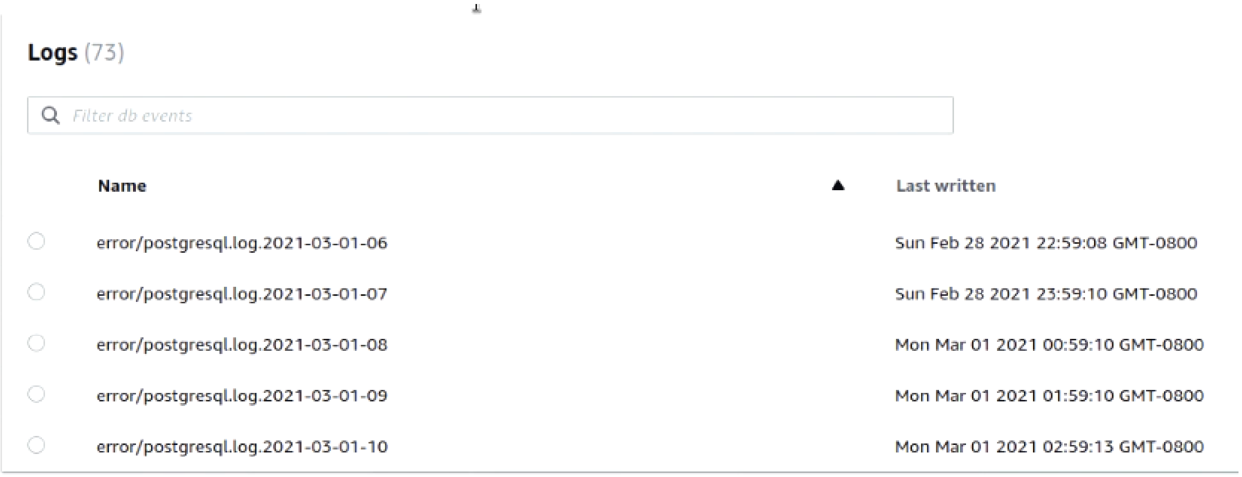
Check security groups.



Security group rules (2)

Security group	Type
terraform-20210127024329645900000002 (sg-0468e6252ce473d88)	CIDR/IP - Inbound
terraform-20210127024329645900000002 (sg-0468e6252ce473d88)	CIDR/IP - Outbound

Check log details by switching to ‘Logs & events’ tab.

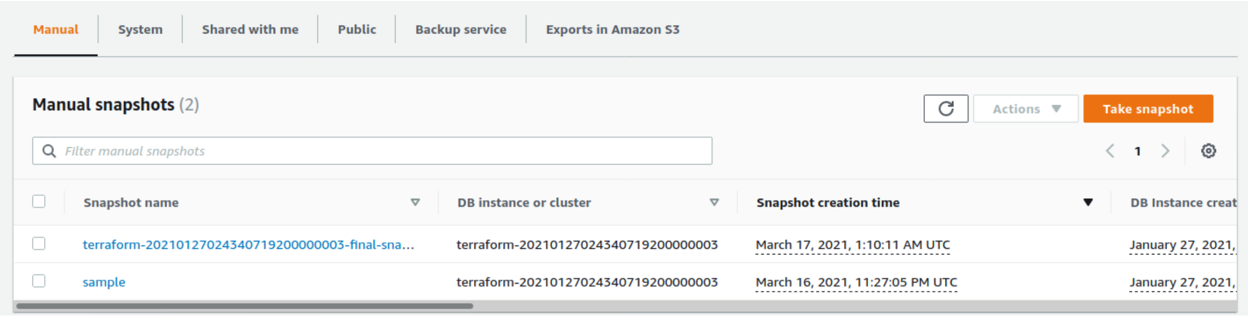


Logs (73)

Filter db events

	Name	Last written
○	error/postgresql.log.2021-03-01-06	Sun Feb 28 2021 22:59:08 GMT-0800
○	error/postgresql.log.2021-03-01-07	Sun Feb 28 2021 23:59:10 GMT-0800
○	error/postgresql.log.2021-03-01-08	Mon Mar 01 2021 00:59:10 GMT-0800
○	error/postgresql.log.2021-03-01-09	Mon Mar 01 2021 01:59:10 GMT-0800
○	error/postgresql.log.2021-03-01-10	Mon Mar 01 2021 02:59:13 GMT-0800

Step 10: Click on Snapshots on the left pane to check snapshots.

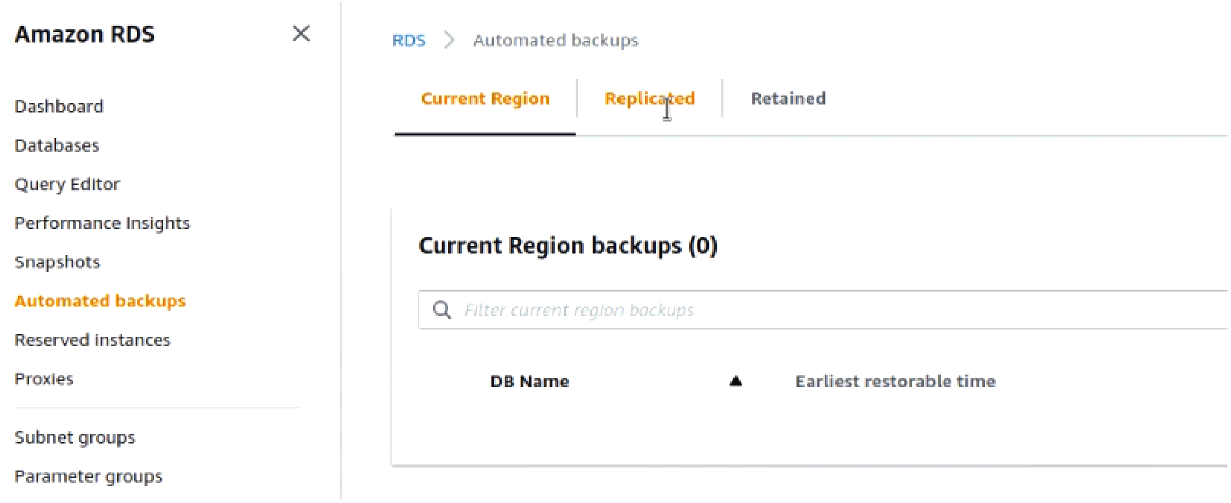


Manual snapshots (2)

Filter manual snapshots

□	Snapshot name	DB instance or cluster	Snapshot creation time	DB Instance creat
□	terraform-20210127024340719200000003-final-sna...	terraform-20210127024340719200000003	March 17, 2021, 1:10:11 AM UTC	January 27, 2021,
□	sample	terraform-20210127024340719200000003	March 16, 2021, 11:27:05 PM UTC	January 27, 2021,

Step 11: Check backups for RDS (by clicking on Automated backups on the left pane).

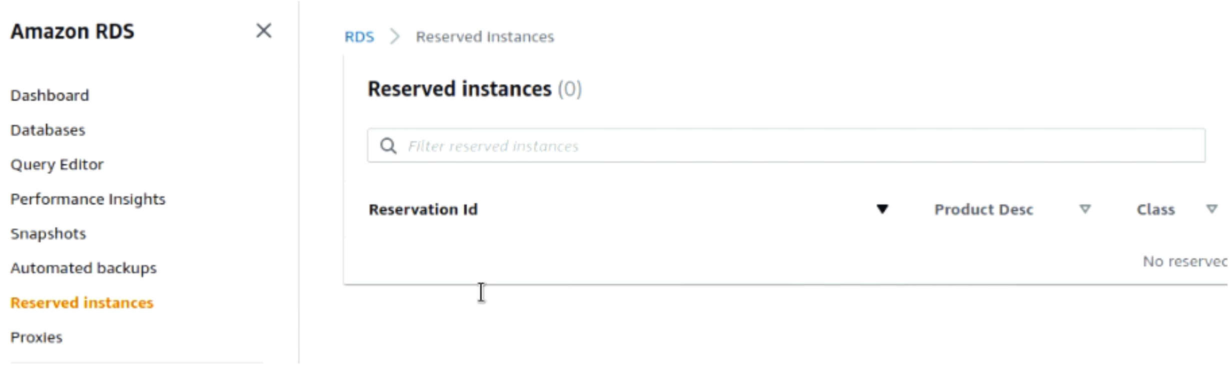


Current Region backups (0)

Filter current region backups

DB Name	Earliest restorable time

Step 12: Check proxies and reserved instances.

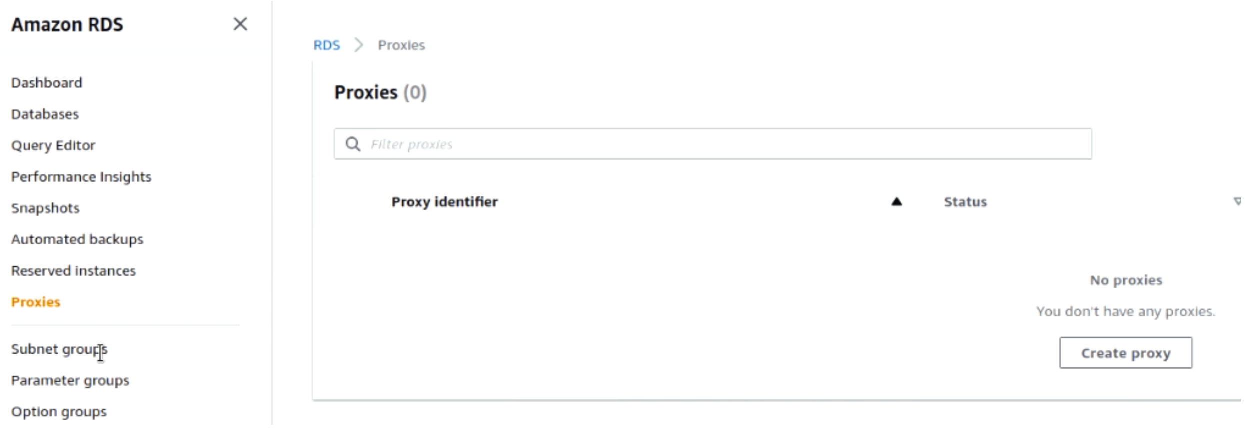


Reserved instances (0)

Filter reserved instances

Reservation Id	Product Desc	Class

No reservec



Proxies (0)

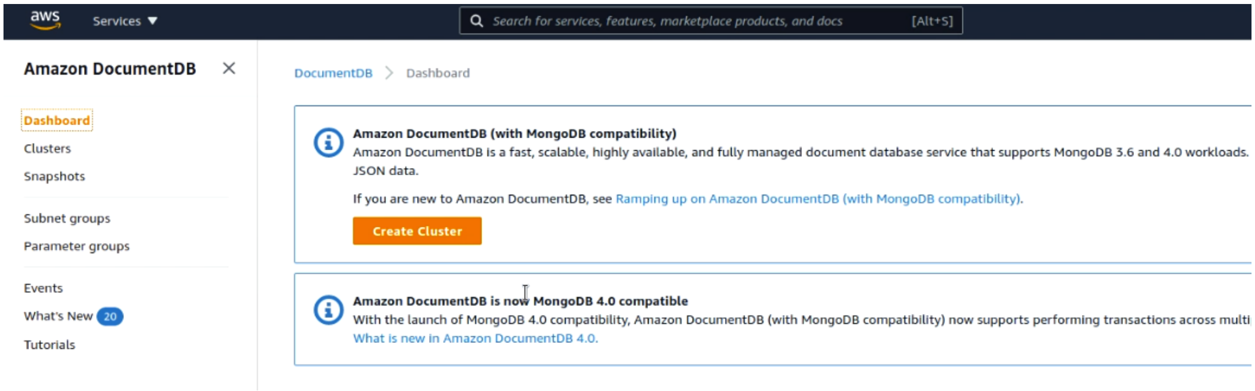
Filter proxies

Proxy identifier	Status

No proxies

You don't have any proxies.

Step 13: Navigate to Amazon DocumentDB dashboard.

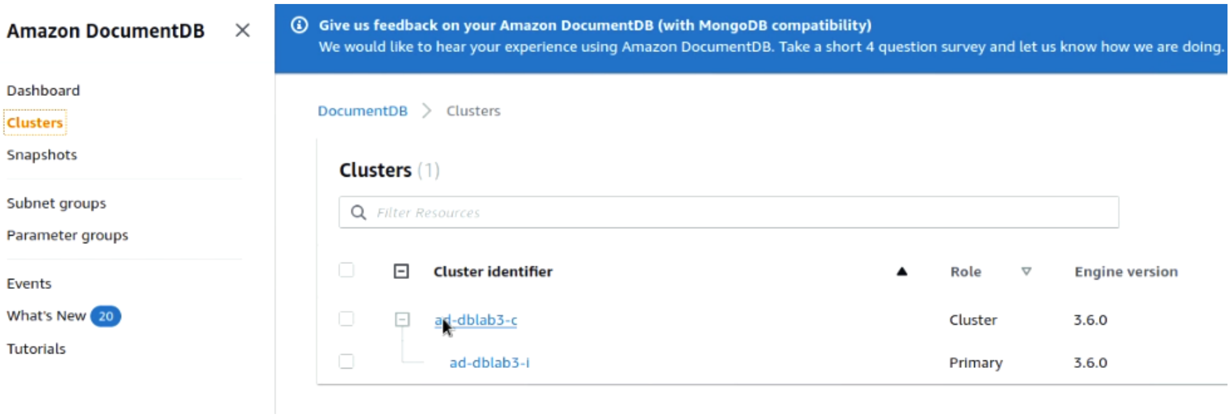


Amazon DocumentDB (with MongoDB compatibility)
Amazon DocumentDB is a fast, scalable, highly available, and fully managed document database service that supports MongoDB 3.6 and 4.0 workloads. JSON data.

If you are new to Amazon DocumentDB, see Ramping up on Amazon DocumentDB (with MongoDB compatibility).

Amazon DocumentDB is now MongoDB 4.0 compatible
With the launch of MongoDB 4.0 compatibility, Amazon DocumentDB (with MongoDB compatibility) now supports performing transactions across multi
What is new in Amazon DocumentDB 4.0.

Step 14: Click on clusters on the left pane to see db clusters.



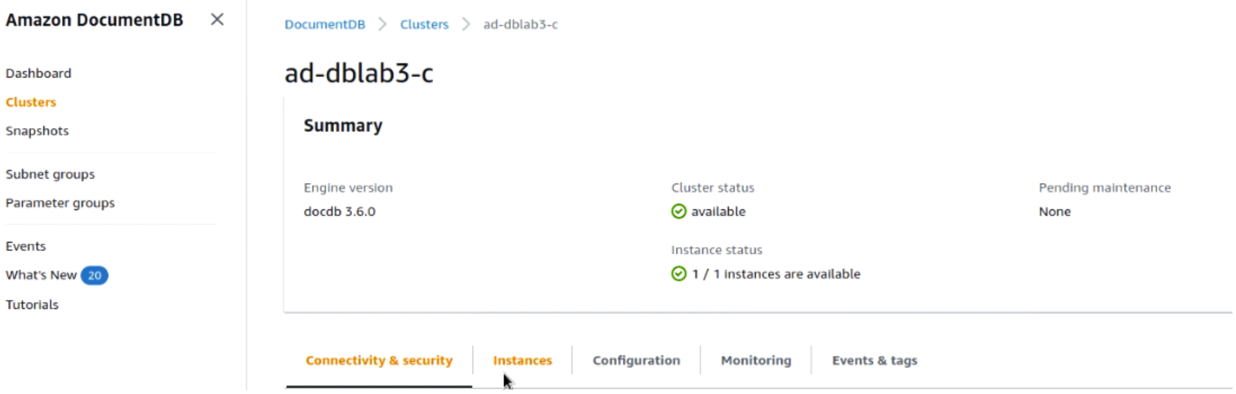
Give us feedback on your Amazon DocumentDB (with MongoDB compatibility)
We would like to hear your experience using Amazon DocumentDB. Take a short 4 question survey and let us know how we are doing.

DocumentDB > Clusters

Clusters (1)

Cluster identifier	Role	Engine version
ad-dblab3-c	Cluster	3.6.0
ad-dblab3-i	Primary	3.6.0

Click on cluster name to check cluster details.



DocumentDB > Clusters > ad-dblab3-c

ad-dblab3-c

Summary

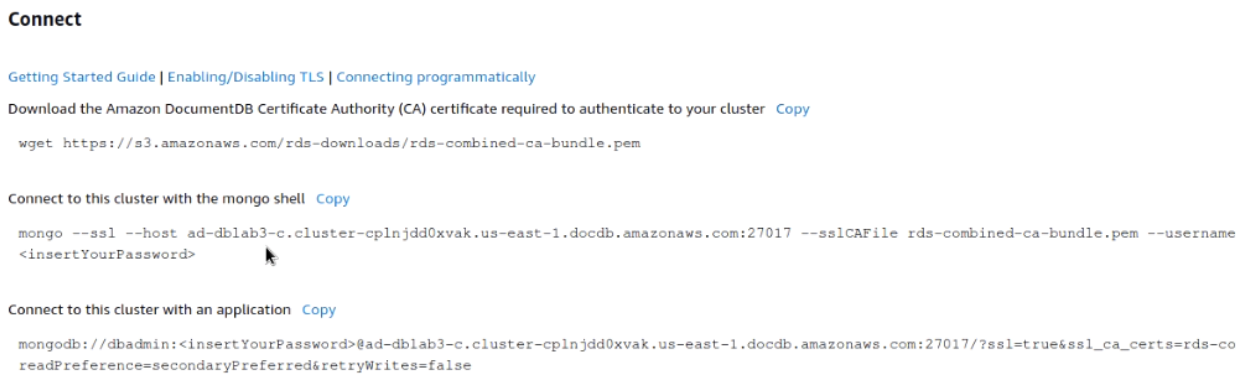
Engine version: docdb 3.6.0

Cluster status: available

Instance status: 1 / 1 instances are available

Pending maintenance: None

Check connection commands.



Connect

Getting Started Guide | Enabling/Disabling TLS | Connecting programmatically

Download the Amazon DocumentDB Certificate Authority (CA) certificate required to authenticate to your cluster Copy

```
wget https://s3.amazonaws.com/rds-downloads/rds-combined-ca-bundle.pem
```

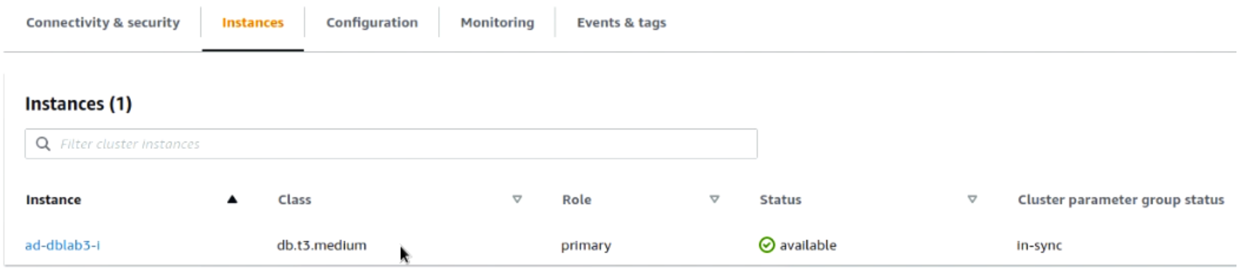
Connect to this cluster with the mongo shell Copy

```
mongo --ssl --host ad-dblab3-c.cluster-cplnjdd0xvak.us-east-1.docdb.amazonaws.com:27017 --sslCAFile rds-combined-ca-bundle.pem --username
<insertYourPassword>
```

Connect to this cluster with an application Copy

```
mongodb://dbadmin:<insertYourPassword>@ad-dblab3-c.cluster-cplnjdd0xvak.us-east-1.docdb.amazonaws.com:27017/?ssl=true&ssl_ca_certs=rds-co
readPreference=secondaryPreferred&retryWrites=false
```

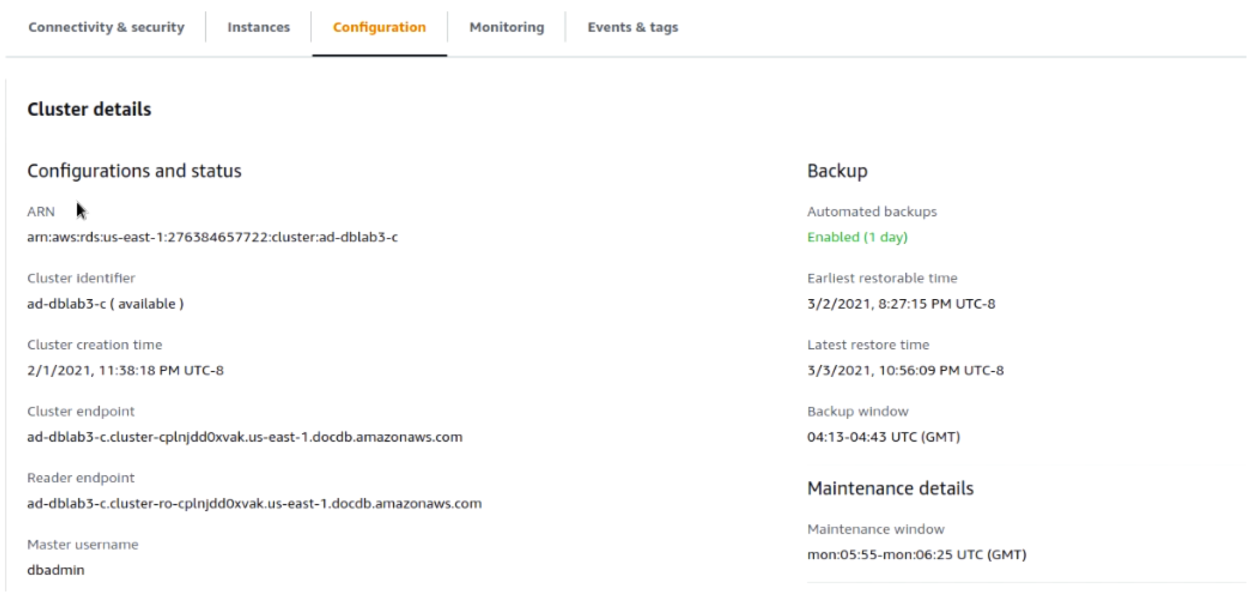
Check instances.



Instances (1)

Instance	Class	Role	Status	Cluster parameter group status
ad-dblab3-i	db.t3.medium	primary	✓ available	in-sync

Check configurations.



Cluster details

Configurations and status

ARN
arn:aws:rds:us-east-1:276384657722:cluster:ad-dblab3-c

Cluster identifier
ad-dblab3-c (available)

Cluster creation time
2/1/2021, 11:38:18 PM UTC-8

Cluster endpoint
ad-dblab3-c.cluster-cplnjdd0xvak.us-east-1.docdb.amazonaws.com

Reader endpoint
ad-dblab3-c.cluster-ro-cplnjdd0xvak.us-east-1.docdb.amazonaws.com

Master username
dbadmin

Backup

Automated backups
Enabled (1 day)

Earliest restorable time
3/2/2021, 8:27:15 PM UTC-8

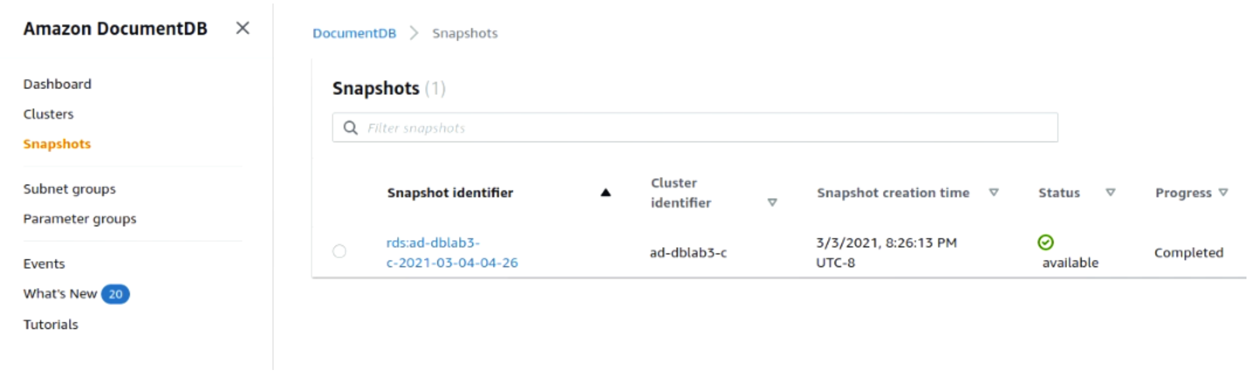
Latest restore time
3/3/2021, 10:56:09 PM UTC-8

Backup window
04:13-04:43 UTC (GMT)

Maintenance details

Maintenance window
mon:05:55-mon:06:25 UTC (GMT)

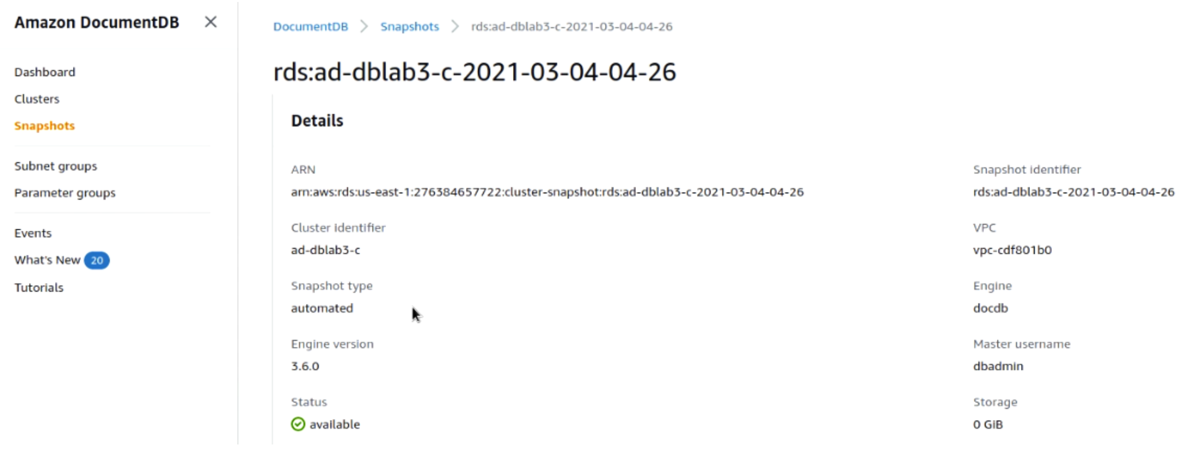
Step 15: Click on Snapshots on left pane to check snapshots.



Snapshots (1)

	Snapshot identifier	Cluster identifier	Snapshot creation time	Status	Progress
○	rds:ad-dblab3-c-2021-03-04-04-26	ad-dblab3-c	3/3/2021, 8:26:13 PM UTC-8	✓ available	Completed

Click on the snapshot name to get more details of the snapshot.



rds:ad-dblab3-c-2021-03-04-04-26

Details

ARN
arn:aws:rds:us-east-1:276384657722:cluster-snapshot:rds:ad-dblab3-c-2021-03-04-04-26

Snapshot identifier
rds:ad-dblab3-c-2021-03-04-04-26

Cluster identifier
ad-dblab3-c

VPC
vpc-cdf801b0

Snapshot type
automated

Engine
docdb

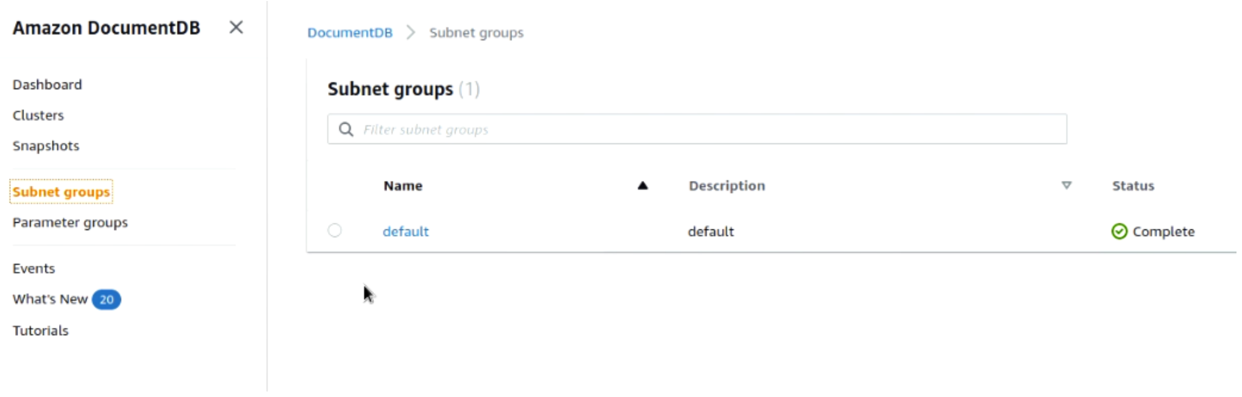
Engine version
3.6.0

Master username
dbadmin

Status
✓ available

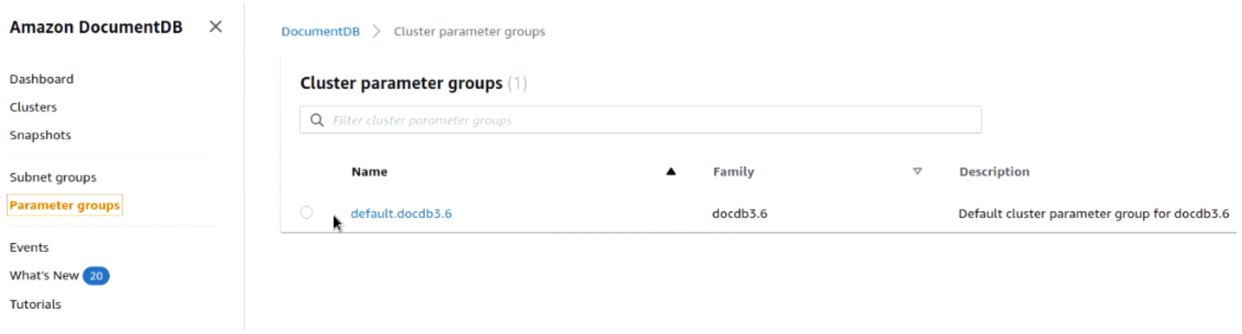
Storage
0 GiB

Step 16: Enumerate subnet groups and parameter groups.



Subnet groups (1)

	Name	Description	Status
○	default	default	✓ Complete



Cluster parameter groups (1)

	Name	Family	Description
○	default.docdb3.6	docdb3.6	Default cluster parameter group for docdb3.6