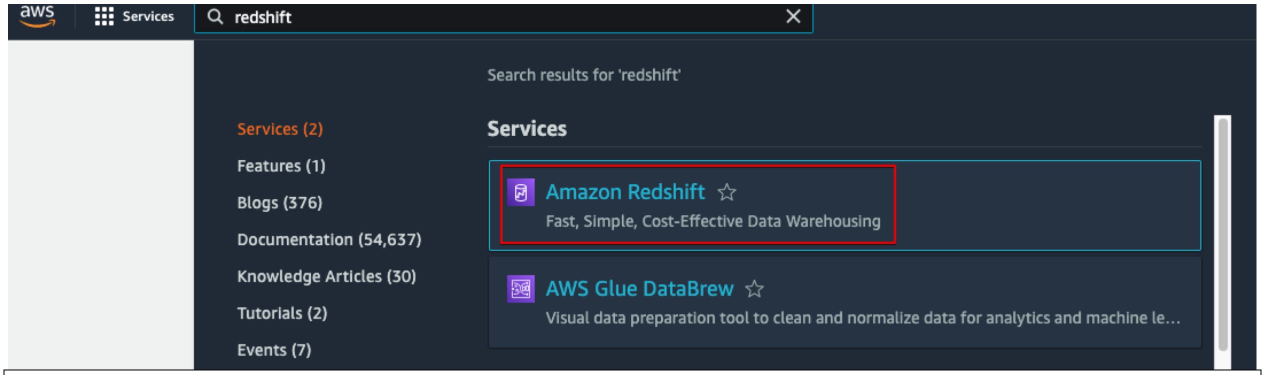
Now give the role S3 Full Access:

```
aws iam attach-role-policy --policy-arn
arn:aws:iam::aws:policy/AmazonS3FullAccess --role-name my-
redshift-service-role
```

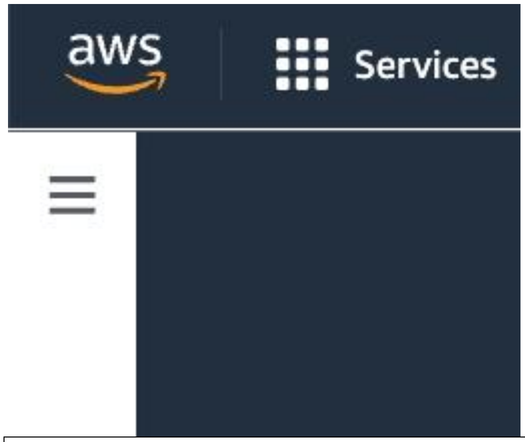
1. Open the AWS console by clicking on the **Launch Cloud Gateway** button followed the **Open Cloud Console** button in the classroom.

2. Search **Redshift** in the search bar, and then click on **Amazon Redshift**.


aws
Services
redshift
Search results for 'redshift'
Services (2)
Features (1)
Blogs (376)
Documentation (54,637)
Knowledge Articles (30)
Tutorials (2)
Events (7)
Services
Amazon Redshift
Fast, Simple, Cost-Effective Data Warehousing
AWS Glue DataBrew
Visual data preparation tool to clean and normalize data for analytics and machine le...

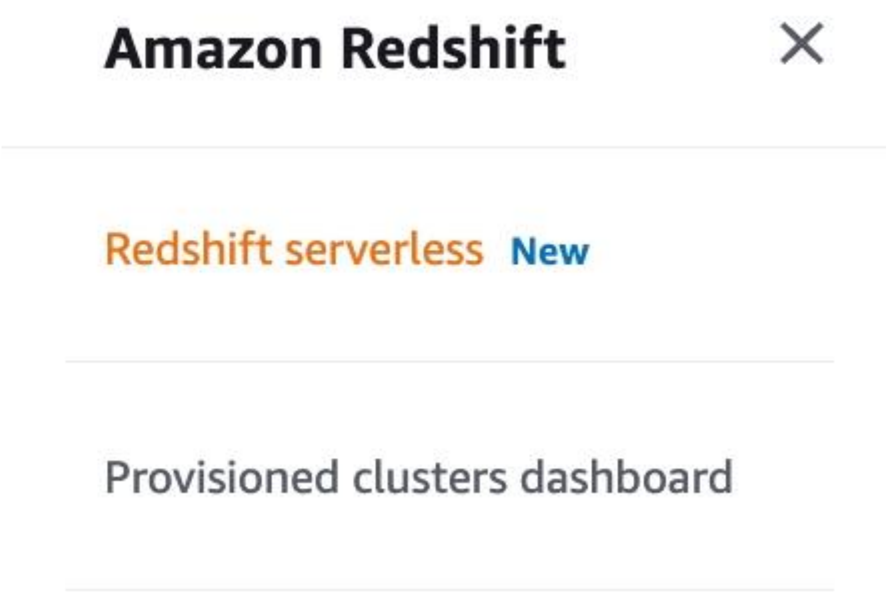
Select Amazon Redshift

3. On the left click the hamburger menu



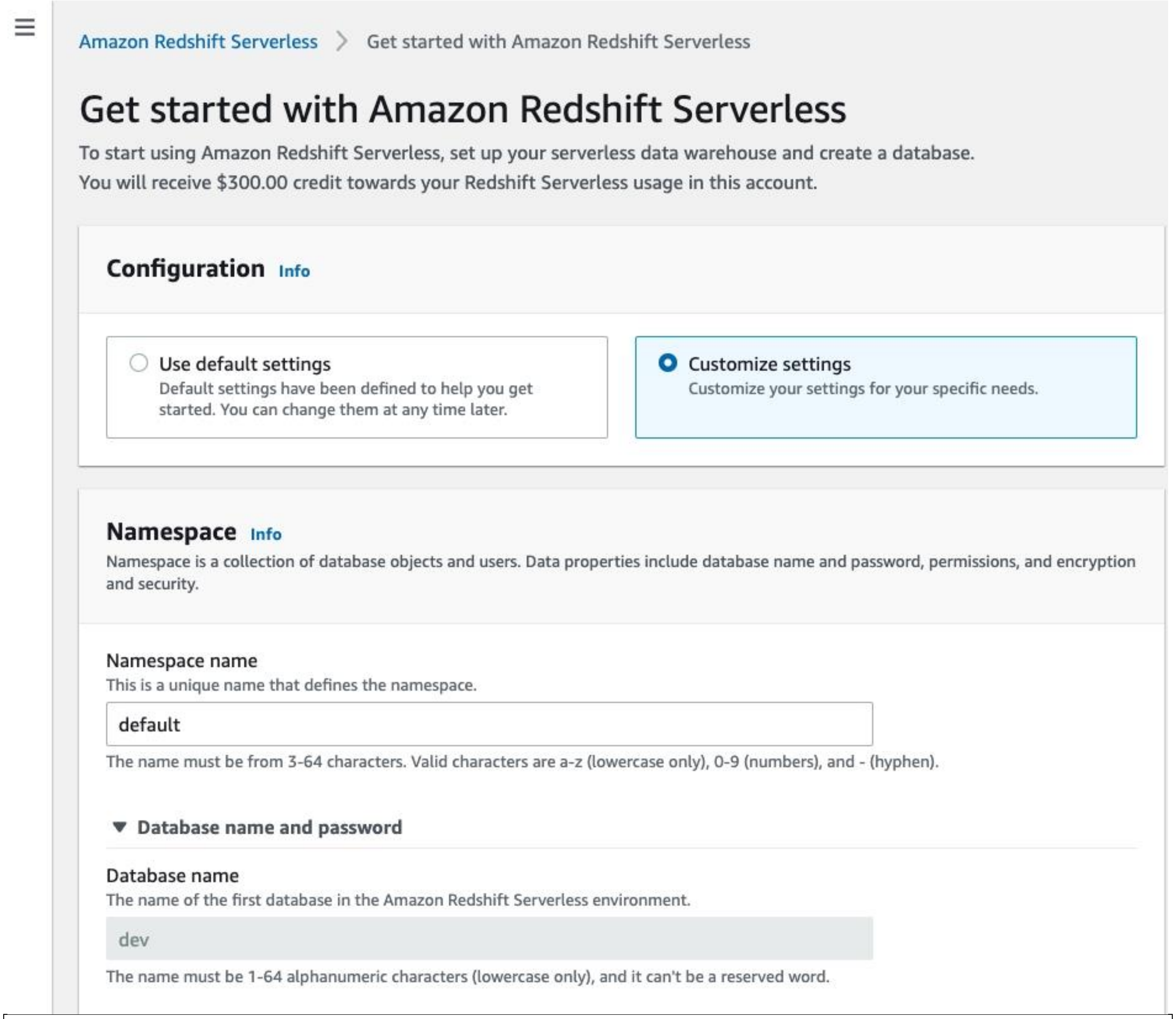
Hamburger menu

4. Click **Redshift Serverless**



From the Amazon Redshift menu on the left, Click Redshift serverless

5. Click **Customize settings**



Amazon Redshift Serverless > Get started with Amazon Redshift Serverless

Get started with Amazon Redshift Serverless

To start using Amazon Redshift Serverless, set up your serverless data warehouse and create a database.
You will receive $300.00 credit towards your Redshift Serverless usage in this account.

Configuration Info

○ Use default settings
Default settings have been defined to help you get started. You can change them at any time later.

● Customize settings
Customize your settings for your specific needs.

Namespace Info

Namespace is a collection of database objects and users. Data properties include database name and password, permissions, and encryption and security.

Namespace name
This is a unique name that defines the namespace.

default

The name must be from 3-64 characters. Valid characters are a-z (lowercase only), 0-9 (numbers), and - (hyphen).

▼ Database name and password

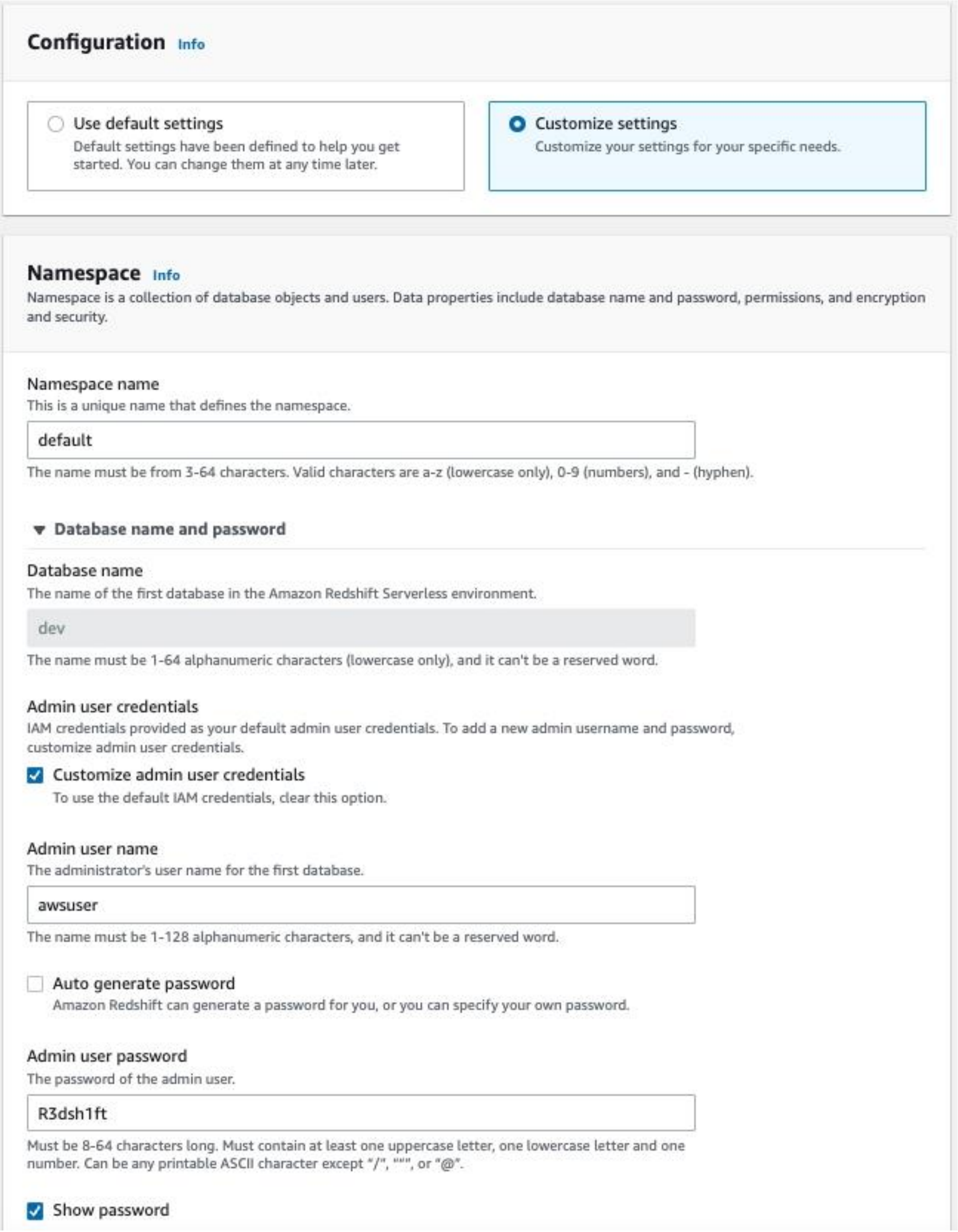
Database name
The name of the first database in the Amazon Redshift Serverless environment.

dev

The name must be 1-64 alphanumeric characters (lowercase only), and it can't be a reserved word.

Customize settings

6. Go with the **default** namespace name
7. Check the box **Customize admin user credentials**
8. Enter **awsuser** for the Admin user name
9. Enter a password (save this for later)



Configuration Info

○ Use default settings
Default settings have been defined to help you get started. You can change them at any time later.

● Customize settings
Customize your settings for your specific needs.

Namespace Info

Namespace is a collection of database objects and users. Data properties include database name and password, permissions, and encryption and security.

Namespace name
This is a unique name that defines the namespace.

default

The name must be from 3-64 characters. Valid characters are a-z (lowercase only), 0-9 (numbers), and - (hyphen).

▼ Database name and password

Database name
The name of the first database in the Amazon Redshift Serverless environment.

dev

The name must be 1-64 alphanumeric characters (lowercase only), and it can't be a reserved word.

Admin user credentials
IAM credentials provided as your default admin user credentials. To add a new admin username and password, customize admin user credentials.

☑ Customize admin user credentials
To use the default IAM credentials, clear this option.

Admin user name
The administrator's user name for the first database.

awsuser

The name must be 1-128 alphanumeric characters, and it can't be a reserved word.

□ Auto generate password
Amazon Redshift can generate a password for you, or you can specify your own password.

Admin user password
The password of the admin user.

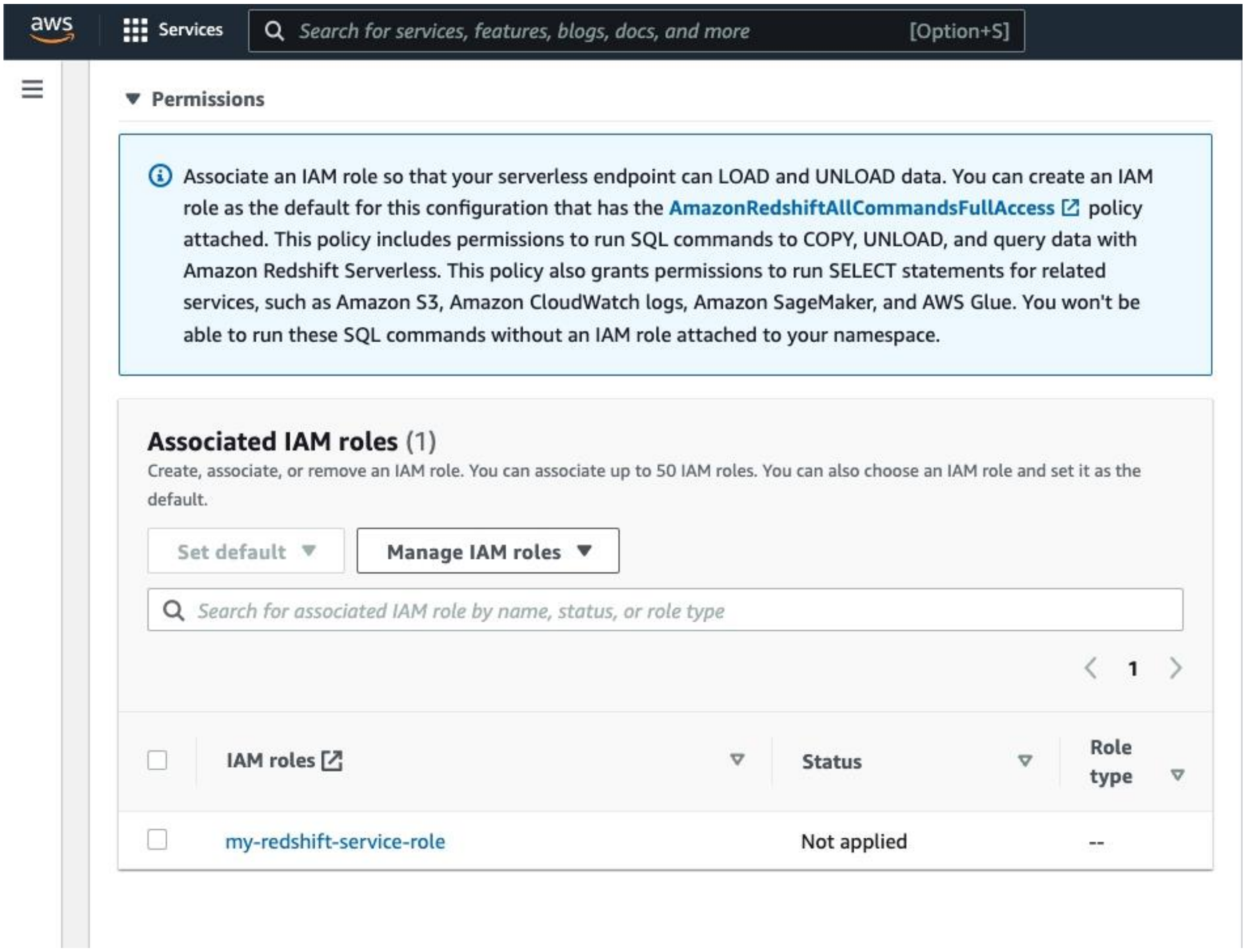
R3dsh1ft

Must be 8-64 characters long. Must contain at least one uppercase letter, one lowercase letter and one number. Can be any printable ASCII character except "/", """, or "@".

☑ Show password

10. Associate the my-redshift-service-role you created with Redshift **(Hint:** If the role you created didn't show up, refresh the page)

11. This will enable Redshift Serverless to connect with S3



▼ Permissions

Associate an IAM role so that your serverless endpoint can LOAD and UNLOAD data. You can create an IAM role as the default for this configuration that has the AmazonRedshiftAllCommandsFullAccess policy attached. This policy includes permissions to run SQL commands to COPY, UNLOAD, and query data with Amazon Redshift Serverless. This policy also grants permissions to run SELECT statements for related services, such as Amazon S3, Amazon CloudWatch logs, Amazon SageMaker, and AWS Glue. You won't be able to run these SQL commands without an IAM role attached to your namespace.

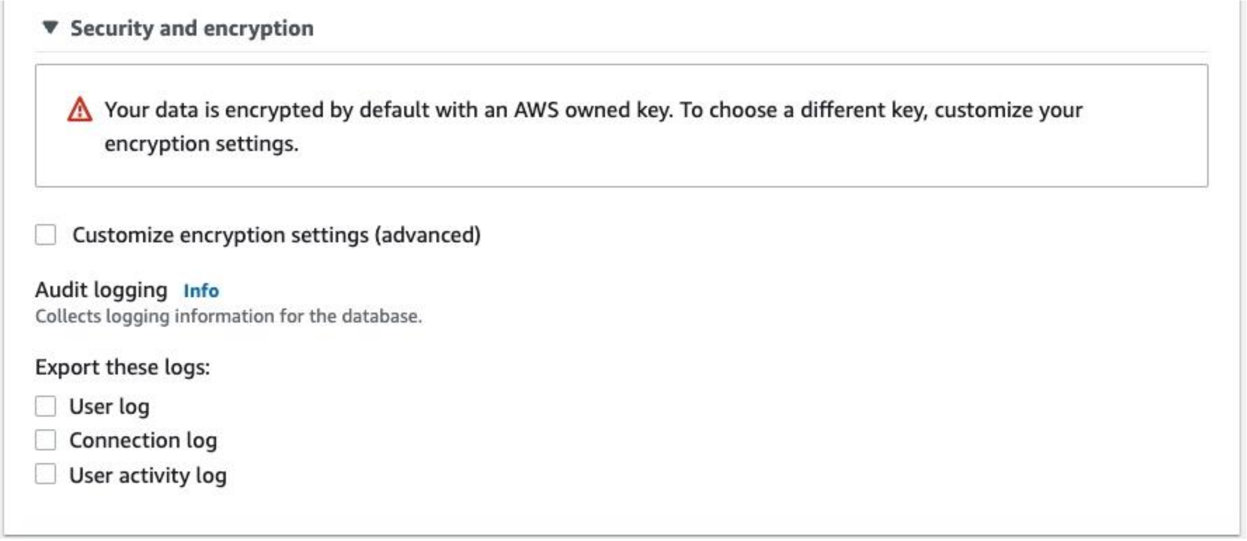
Associated IAM roles (1)

Create, associate, or remove an IAM role. You can associate up to 50 IAM roles. You can also choose an IAM role and set it as the default.

Set default ▼
Manage IAM roles ▼
Search for associated IAM role by name, status, or role type
1

□	IAM roles	Status	Role type
□	my-redshift-service-role	Not applied	--

13. Accept the defaults for **Security and encryption**



▼ Security and encryption

Your data is encrypted by default with an AWS owned key. To choose a different key, customize your encryption settings.

□ Customize encryption settings (advanced)

Audit logging Info

Collects logging information for the database.

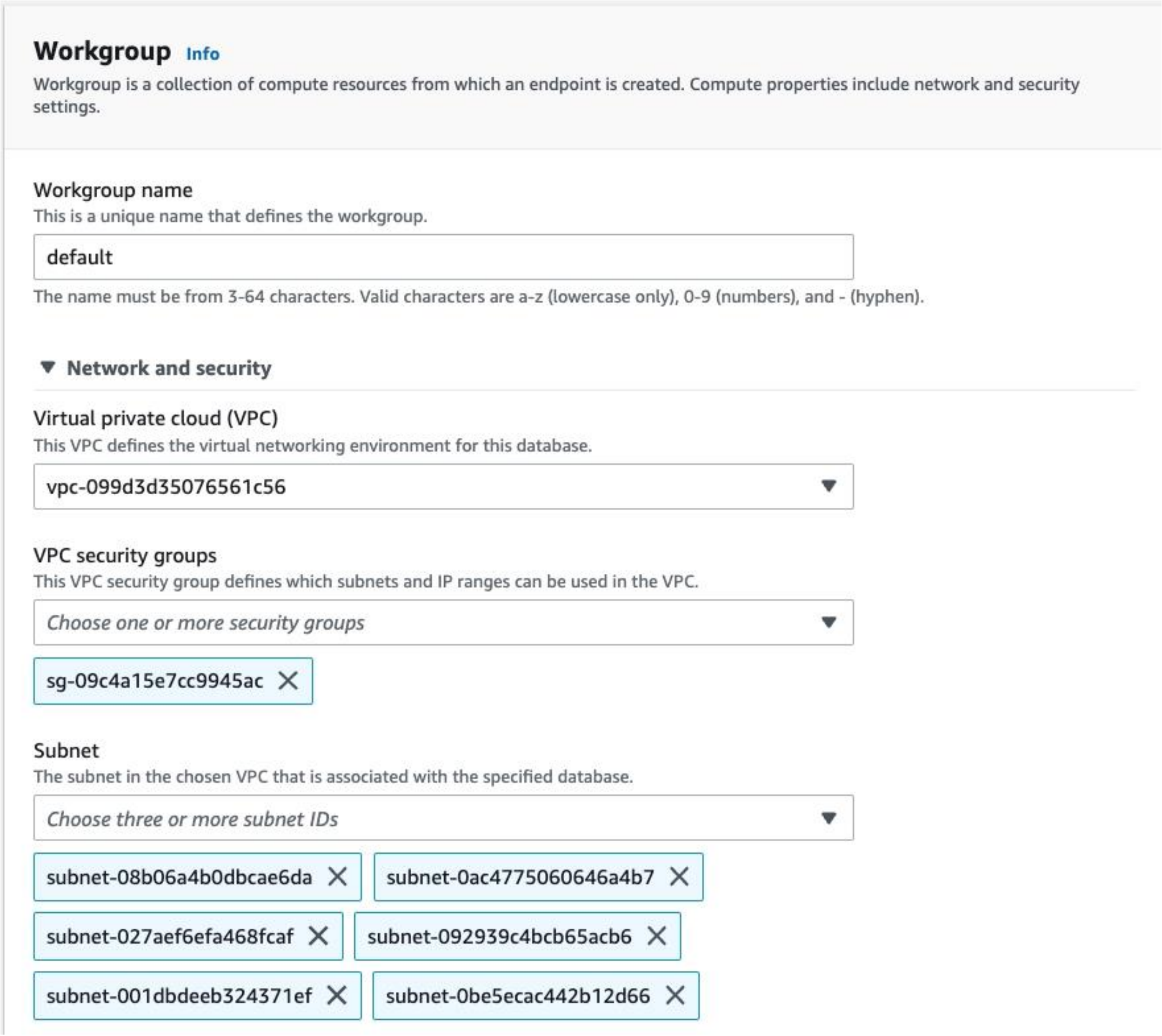
Export these logs:

□ User log

□ Connection log

□ User activity log

14. Accept the default	**Workgroup**	settings



Workgroup

Workgroup is a collection of compute resources from which an endpoint is created. Compute properties include network and security settings.

Workgroup name

This is a unique name that defines the workgroup.

default

The name must be from 3-64 characters. Valid characters are a-z (lowercase only), 0-9 (numbers), and - (hyphen).

▼ Network and security

Virtual private cloud (VPC)

This VPC defines the virtual networking environment for this database.

vpc-099d3d35076561c56 ▼

VPC security groups

This VPC security group defines which subnets and IP ranges can be used in the VPC.

Choose one or more security groups ▼

sg-09c4a15e7cc9945ac ✕

Subnet

The subnet in the chosen VPC that is associated with the specified database.

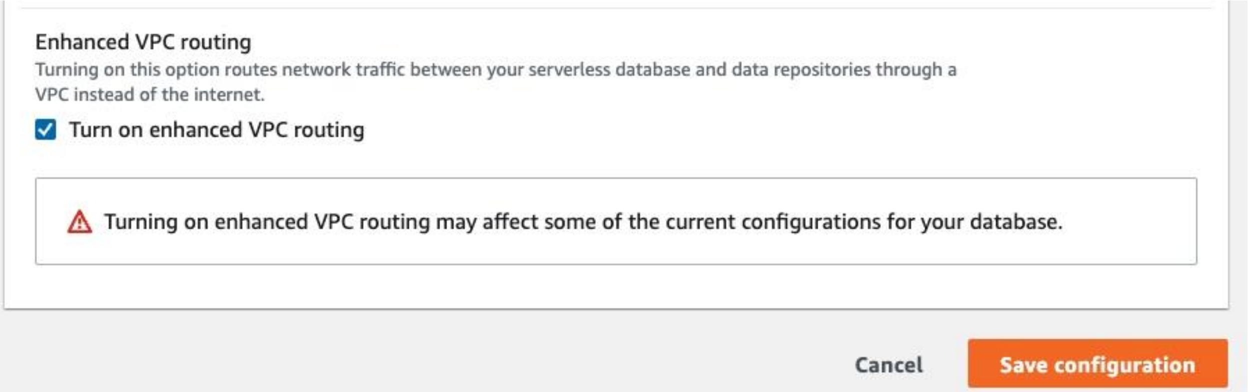
Choose three or more subnet IDs ▼

subnet-08b06a4b0dbcae6da ✕ subnet-0ac4775060646a4b7 ✕

subnet-027aef6efa468fcaf ✕ subnet-092939c4bcb65acb6 ✕

subnet-001dbdeeb324371ef ✕ subnet-0be5ecac442b12d66 ✕

15. Select **Turn on enhanced VPC routing** and click **Save**



Enhanced VPC routing

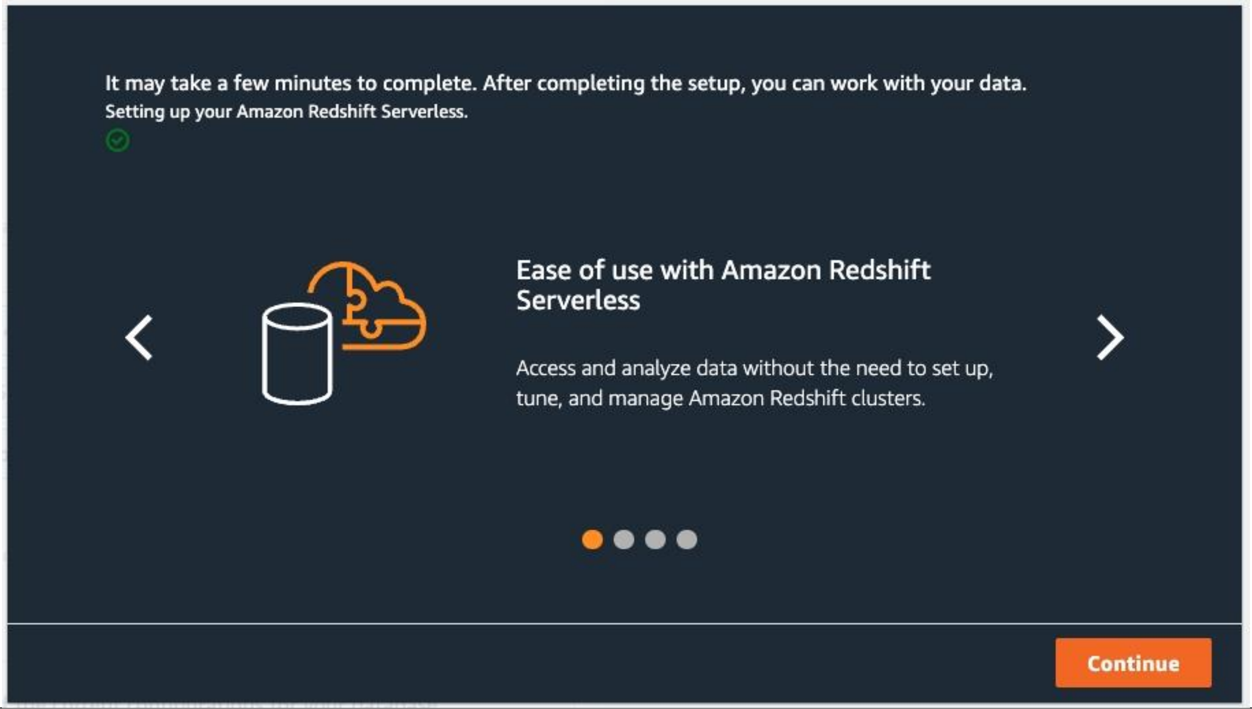
Turning on this option routes network traffic between your serverless database and data repositories through a VPC instead of the internet.

☑ Turn on enhanced VPC routing

⚠ Turning on enhanced VPC routing may affect some of the current configurations for your database.

Turn on enhanced VPC routing

16. Click **Continue** and wait for **Redshift Serverless** setup to finish



It may take a few minutes to complete. After completing the setup, you can work with your data.

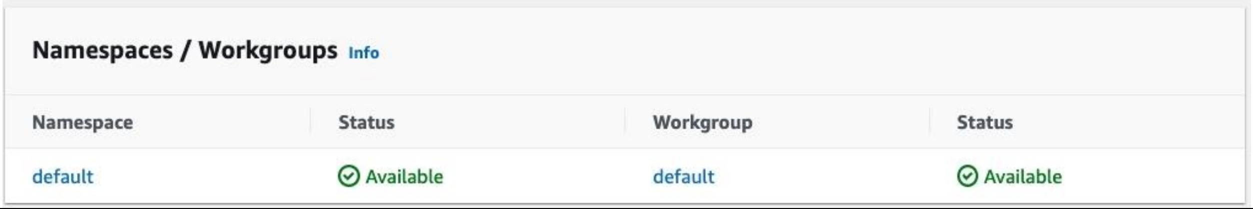
Setting up your Amazon Redshift Serverless.

Ease of use with Amazon Redshift Serverless

Access and analyze data without the need to set up, tune, and manage Amazon Redshift clusters.

Wait for setup to finish

17. On succesful completion, you will see Status Available, as shown below:

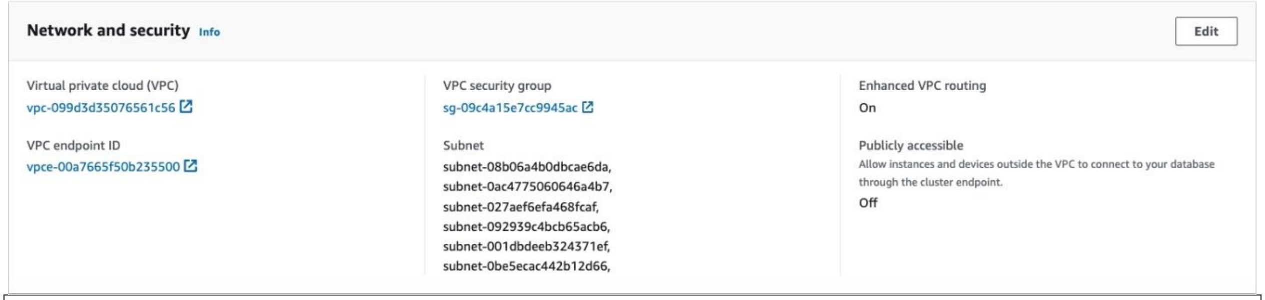


Namespaces / Workgroups Info

Namespace	Status	Workgroup	Status
default	✓ Available	default	✓ Available

Available Status

18. Click the **default** Workgroup.
19. Next, we are going to make this cluster publicly accessible as we would like to connect to this cluster via Airflow.
20. Click **Edit**



Virtual private cloud (VPC)
vpc-099d3d35076561c56

VPC endpoint ID
vpce-00a7665f50b235500

VPC security group
sg-09c4a15e7cc9945ac

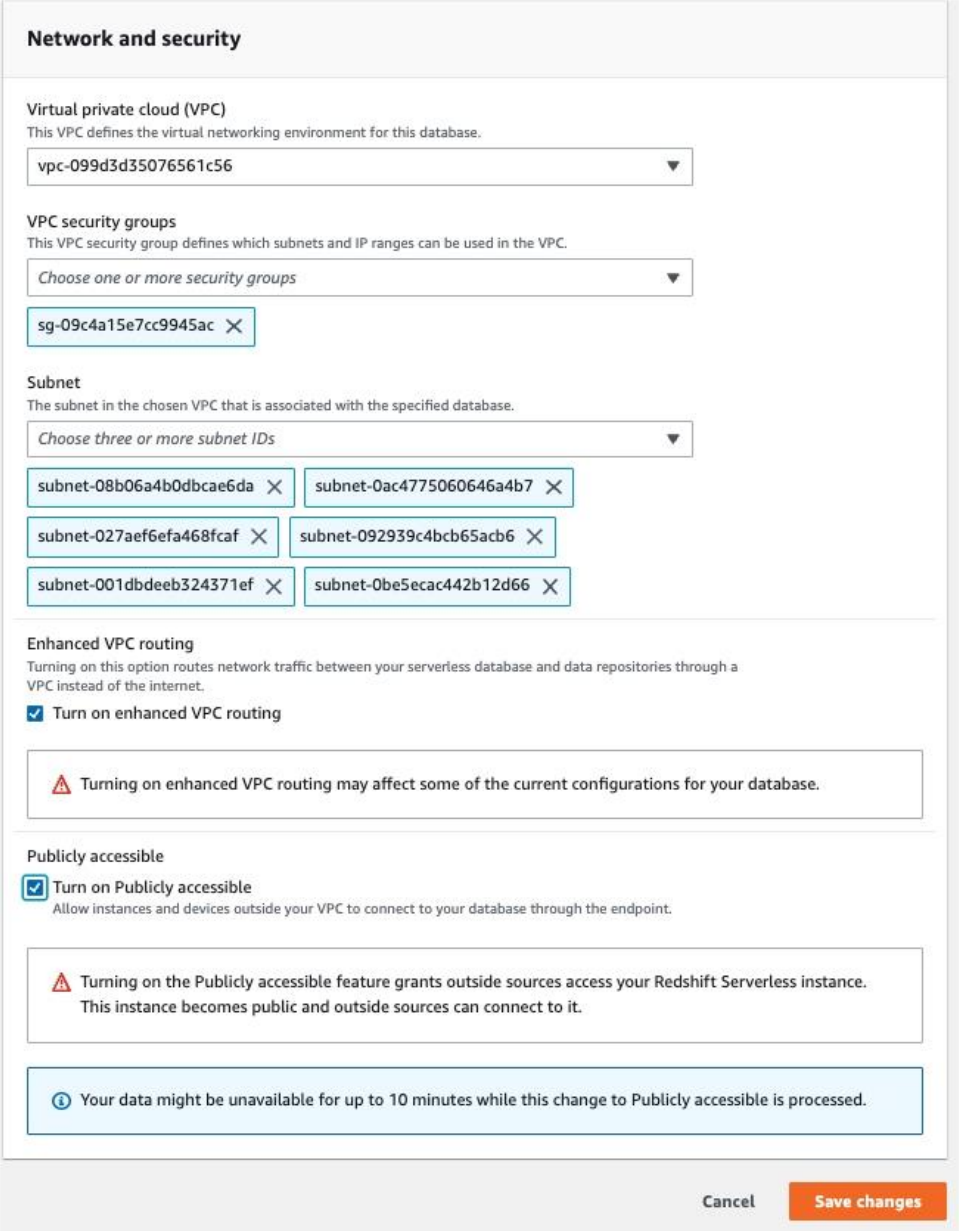
Subnet
subnet-08b06a4b0dbcae6da,
subnet-0ac4775060646a4b7,
subnet-027aef6efa468fcaf,
subnet-092939c4bcb65acb6,
subnet-001dbdeeb324371ef,
subnet-0be5ecac442b12d66,

Enhanced VPC routing
On

Publicly accessible
Allow instances and devices outside the VPC to connect to your database through the cluster endpoint.
Off

Click Edit

21. Select **Turn on Publicly accessible**
22. Click **Save**



Network and security

Virtual private cloud (VPC)

This VPC defines the virtual networking environment for this database.

vpc-099d3d35076561c56 ▼

VPC security groups

This VPC security group defines which subnets and IP ranges can be used in the VPC.

Choose one or more security groups ▼

sg-09c4a15e7cc9945ac ✕

Subnet

The subnet in the chosen VPC that is associated with the specified database.

Choose three or more subnet IDs ▼

subnet-08b06a4b0dbcae6da ✕ subnet-0ac4775060646a4b7 ✕

subnet-027aef6efa468fcaf ✕ subnet-092939c4bcb65acb6 ✕

subnet-001dbdeeb324371ef ✕ subnet-0be5ecac442b12d66 ✕

Enhanced VPC routing

Turning on this option routes network traffic between your serverless database and data repositories through a VPC instead of the internet.

☑ Turn on enhanced VPC routing

⚠ Turning on enhanced VPC routing may affect some of the current configurations for your database.

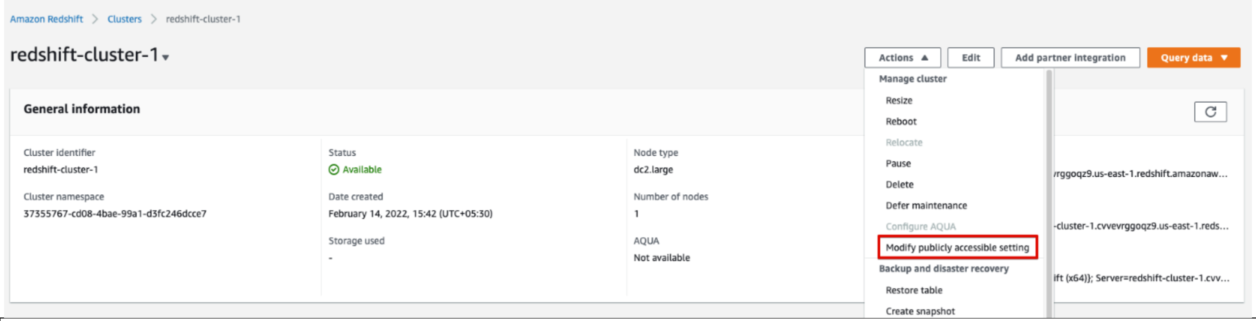
Publicly accessible

☑ Turn on Publicly accessible

Allow instances and devices outside your VPC to connect to your database through the endpoint.

⚠ Turning on the Publicly accessible feature grants outside sources access your Redshift Serverless instance. This instance becomes public and outside sources can connect to it.

ⓘ Your data might be unavailable for up to 10 minutes while this change to Publicly accessible is processed.



Amazon Redshift > Clusters > redshift-cluster-1

redshift-cluster-1

General information

Cluster identifier
redshift-cluster-1

Cluster namespace
37355767-cd08-4bae-99a1-d3fc246dcce7

Status
Available

Date created
February 14, 2022, 15:42 (UTC+05:30)

Storage used
-

Node type
dc2.large

Number of nodes
1

AQUA
Not available

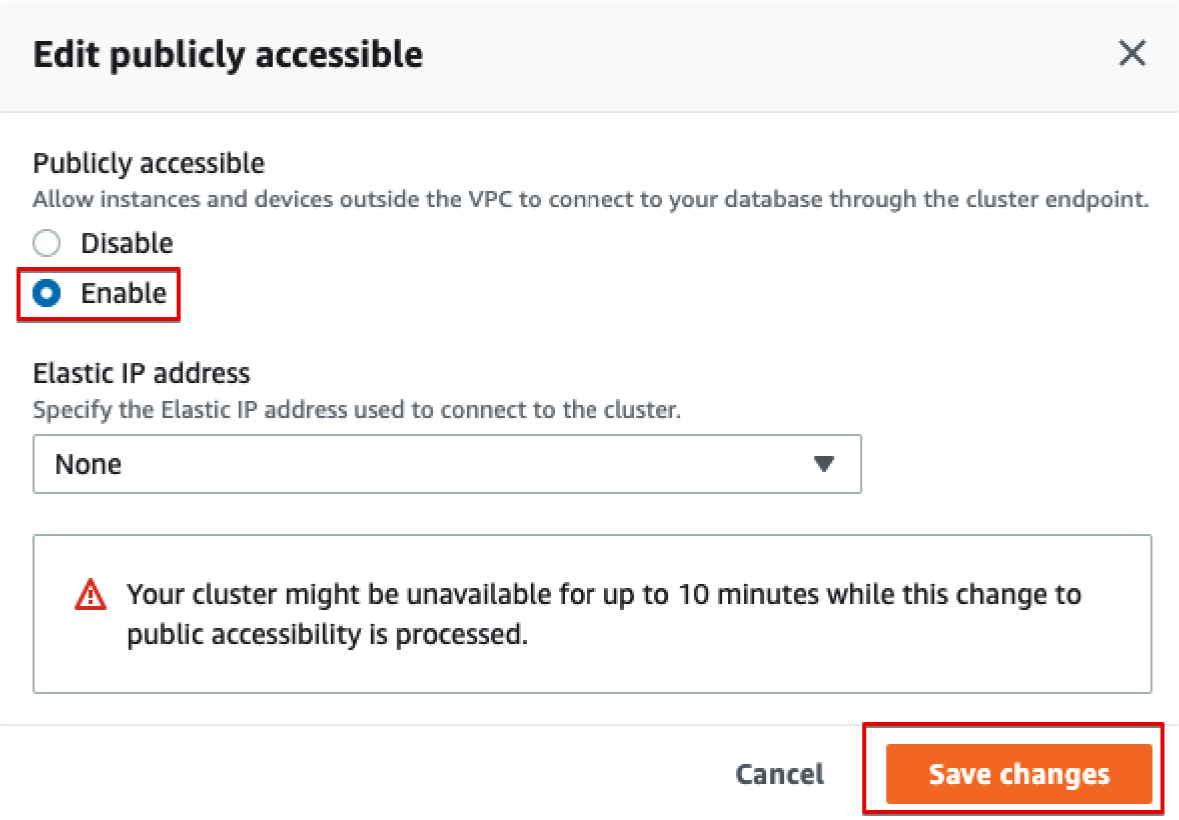
vrggoqz9.us-east-1.redshift.amazonaw…

-cluster-1.cvvevrggoqz9.us-east-1.reds…

ift (x64)}; Server=redshift-cluster-1.cvv…

Modify public accessibility

23. Click on **Enable** and **Save changes**.



Edit publicly accessible

Publicly accessible
Allow instances and devices outside the VPC to connect to your database through the cluster endpoint.

○ Disable

● Enable

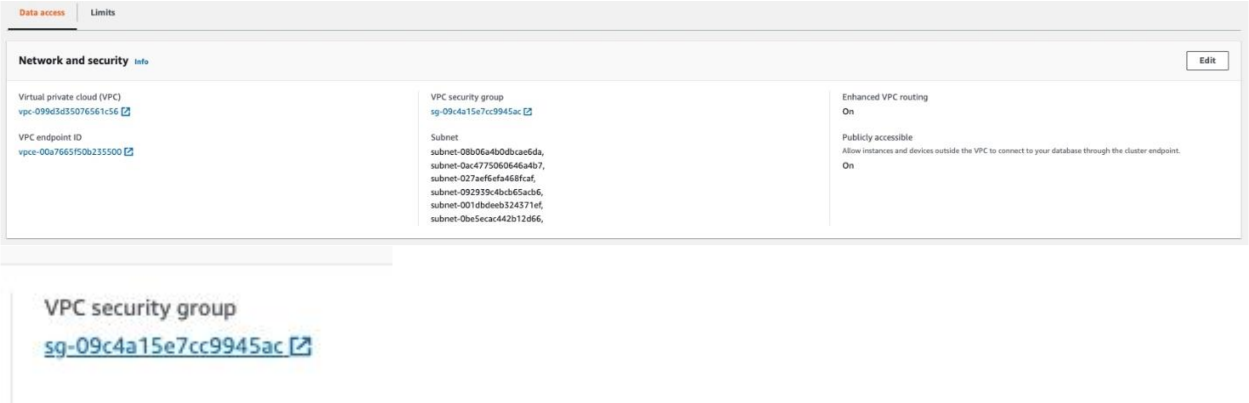
Elastic IP address
Specify the Elastic IP address used to connect to the cluster.

None

Your cluster might be unavailable for up to 10 minutes while this change to public accessibility is processed.

Enable public accessibility

24. Choose the link labeled **VPC security group** to open the Amazon Elastic Compute Cloud (Amazon EC2) console.



Network and security Info

Virtual private cloud (VPC)
vpc-099d3d35076561c56

VPC endpoint ID
vpce-00a7665f50b235500

VPC security group
sg-09c4a15e7cc9945ac

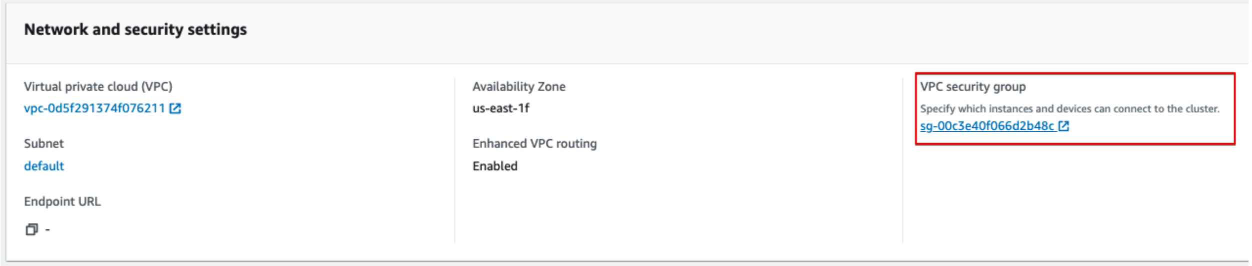
Subnet
subnet-08b06a4b0dbcae6da,
subnet-0ac4775060646a4b7,
subnet-027aef6efa468fcaf,
subnet-092939c4bcb65acb6,
subnet-001dbdeeb324371ef,
subnet-0be5ecac442b12d66,

Enhanced VPC routing
On

Publicly accessible
Allow instances and devices outside the VPC to connect to your database through the cluster endpoint.
On

VPC security group
sg-09c4a15e7cc9945ac

VPC Security group link



Network and security settings

Virtual private cloud (VPC)
vpc-0d5f291374f076211

Subnet
default

Endpoint URL
-

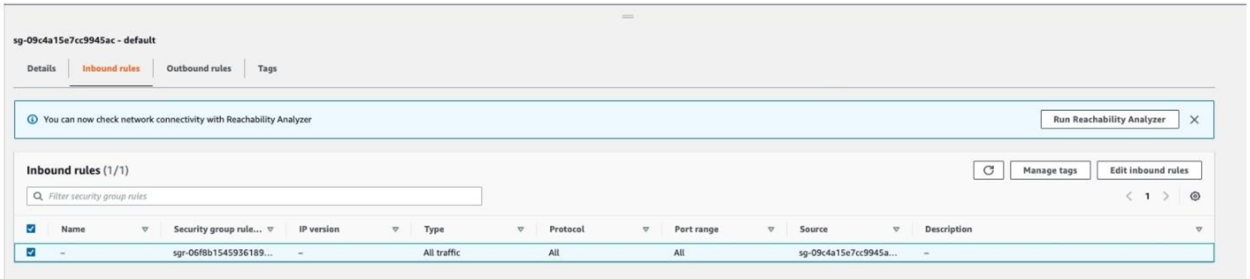
Availability Zone
us-east-1f

Enhanced VPC routing
Enabled

VPC security group
Specify which instances and devices can connect to the cluster.
sg-00c3e40f066d2b48c

Open VPC security group

25. Go to **Inbound Rules** tab and click on **Edit inbound rules**.



sg-09c4a15e7cc9945ac - default

You can now check network connectivity with Reachability Analyzer

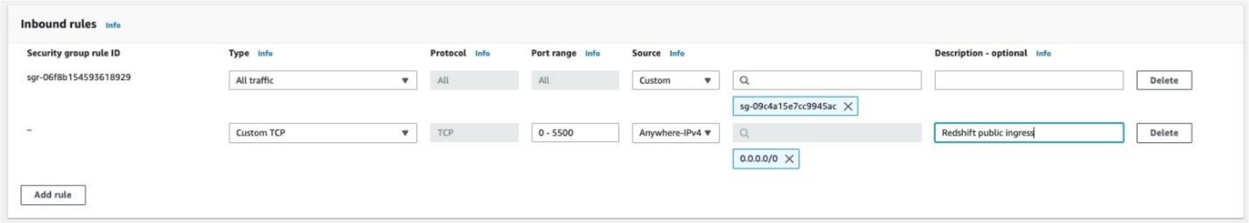
Inbound rules (1/1)

☑	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
☑	–	sgr-06f8b1545936189...	–	All traffic	All	All	sg-09c4a15e7cc9945a...	–

Edit Inbound Rules

26. Add an inbound rule, as shown in the image below.

- Type = Custom TCP
- Port range = 0 - 5500
- Source = Anywhere-iPv4



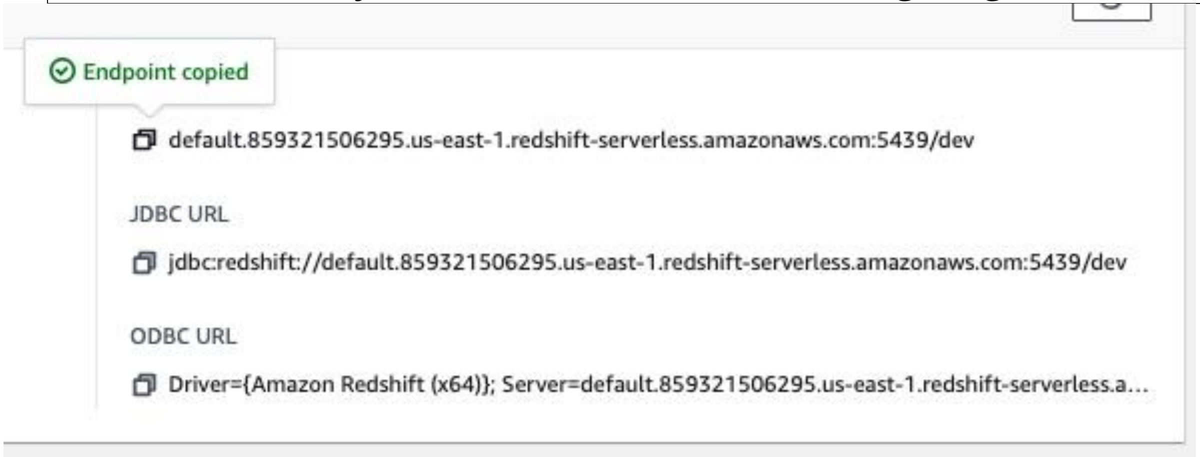
Inbound rules

Security group rule ID	Type	Protocol	Port range	Source		Description - optional	
sgr-06f8b154593618929	All traffic	All	All	Custom	sg-09c4a15e7cc9945ac		Delete
–	Custom TCP	TCP	0 - 5500	Anywhere-IPv4	0.0.0.0/0	Redshift public ingress	Delete

Add inbound rule

27. Now Redshift Serverless should be accessible from Airflow.
28. Go back to the Redshift Workgroup and copy the endpoint.

Store this locally as we will need this while configuring Airflow.



Endpoint copied

default.859321506295.us-east-1.redshift-serverless.amazonaws.com:5439/dev

JDBC URL

jdbc:redshift://default.859321506295.us-east-1.redshift-serverless.amazonaws.com:5439/dev

ODBC URL

Driver={Amazon Redshift (x64)}; Server=default.859321506295.us-east-1.redshift-serverless.a...

Copy the redshift cluster endpoint