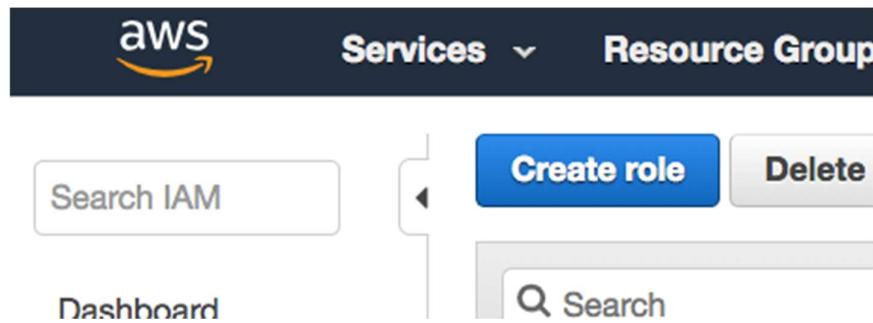


CLOUD Data Warehouse Setup

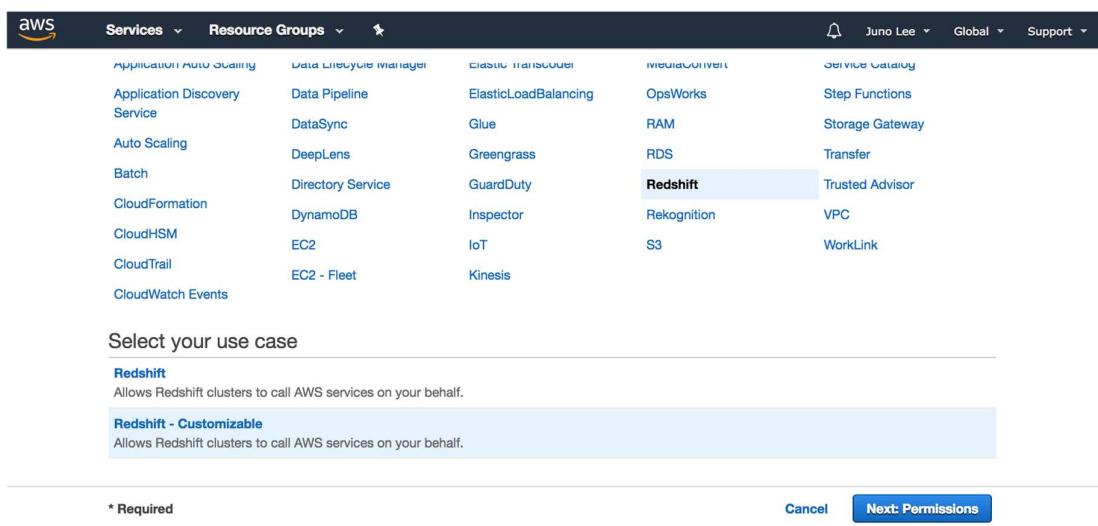
Create an IAM Role

Here, you'll create an IAM role that you will later attach to your Redshift cluster to enable your cluster to load data from Amazon S3 buckets. Read more about IAM roles and Redshift [here](#).

1. Sign in to the AWS Management Console and open the IAM console at <https://console.aws.amazon.com/iam/>.
2. In the left navigation pane, choose **Roles**.
3. Choose **Create role**.



4. In the AWS Service group, choose **Redshift**.
5. Under **Select your use case**, choose **Redshift - Customizable**, and then **Next: Permissions**.



6. On the **Attach permissions policies** page, choose **AmazonS3ReadOnlyAccess**, and then choose **Next: Tags**.
7. Skip this page and choose **Next: Review**.

The screenshot shows the 'Create role' wizard at Step 2, titled 'Attach permissions policies'. A search bar filters results for 's3'. The table lists four policies:

	Policy name	Used as	Description
<input type="checkbox"/>	AmazonDMSRedshiftS3Role	None	Provides access to manage S3 settings f...
<input type="checkbox"/>	AmazonS3FullAccess	Permissions policy (3)	Provides full access to all buckets via th...
<input checked="" type="checkbox"/>	AmazonS3ReadOnlyAccess	Permissions policy (4)	Provides read only access to all buckets ...
<input type="checkbox"/>	QuickSightAccessForS3StorageManagement...	None	Policy used by QuickSight team to acce...

* Required Cancel Previous Next: Tags

8. For **Role name**, enter `myRedshiftRole`, and then choose **Create Role**.

The screenshot shows the 'Create role' wizard at Step 3, titled 'Review'. The role name is 'myRedshiftRole'. The 'Role description' field contains: 'Allows Redshift clusters to call AWS services on your behalf.' Below it, a note says: 'Maximum 1000 characters. Use alphanumeric and '+-=,@-_' characters.'

Trusted entities: AWS service: redshift.amazonaws.com

Policies: [AmazonS3ReadOnlyAccess](#)

Permissions boundary: Permissions boundary is not set

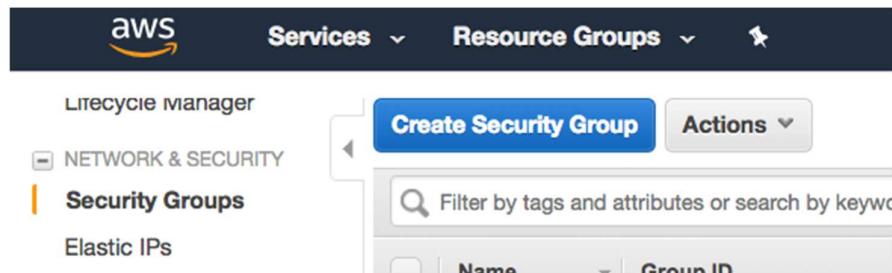
* Required Cancel Previous Create role

You can now attach this role when you launch a new cluster or attach it to an existing cluster. In the next page, you'll attach the role to a new cluster.

Create Security Group

Here, you'll create a security group you will later use to authorize access to your Redshift cluster.

1. Go to your [Amazon EC2 console](#) and under **Network and Security** in the left navigation pane, select **Security Groups**.
2. Choose the **Create Security Group** button.



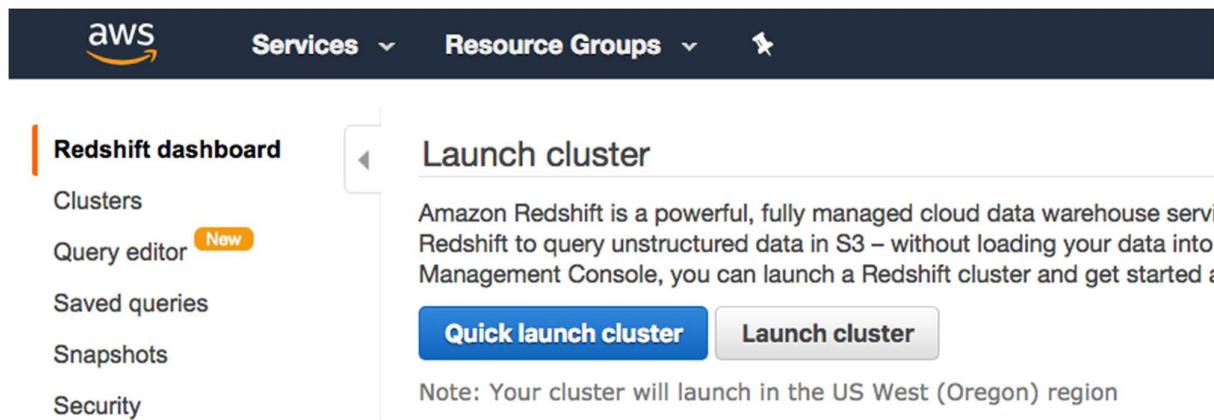
3. Enter `redshift_security_group` for **Security group name**.
4. Enter "authorize redshift cluster access" for **Description**.
5. Select the **Inbound** tab under **Security group rules**.
6. Click on **Add Rule** and enter the following values:
 - **Type:** Custom TCP Rule.
 - **Protocol:** TCP.
 - **Port Range:** `5439`. The default port for Amazon Redshift is 5439, but your port might be different. See note on determining your firewall rules on the earlier "AWS Setup Instructions" page in this lesson.
 - **Source:** select Custom IP, then type `0.0.0.0/0`.
- Important: Using `0.0.0.0/0` is not recommended for anything other than demonstration purposes because it allows access from any computer on the internet. In a real environment, you would create inbound rules based on your own network settings.
7. Choose **Create**.

A detailed screenshot of the "Create Security Group" dialog box. At the top, there are fields for "Security group name" (set to "redshift_security_group"), "Description" (set to "authorize redshift cluster access"), and "VPC" (set to "vpc-3924fa41 (default)"). Below these, the "Security group rules" section is shown. The "Inbound" tab is selected. Under "Inbound", there is a table with columns: Type, Protocol, Port Range, Source, and Description. A new rule is being added: Type is "Custom TCP", Protocol is "TCP", Port Range is "5439", Source is "Custom" with value "0.0.0.0/0", and Description is "e.g. SSH for Admin". There is also an "Add Rule" button. At the bottom right of the dialog is a "Cancel" button and a prominent blue "Create" button.

Launch a Redshift Cluster

WARNING: The cluster that you are about to launch will be live, and you will be charged the standard Amazon Redshift usage fees for the cluster until you delete it. **Make sure to delete your cluster each time you're finished working to avoid large, unexpected costs for yourself.** Instructions on deleting your cluster are included on the last page in this lesson. You can always launch a new cluster, so don't leave your Redshift cluster running overnight or throughout the week if you don't need to.

1. Sign in to the AWS Management Console and open the Amazon Redshift console at <https://console.aws.amazon.com/redshift/>.
2. On the Amazon Redshift Dashboard, choose **Launch cluster**.



3. On the Cluster details page, enter the following values and then choose Continue:
 - **Cluster identifier:** Enter `redshift-cluster`.
 - **Database name:** Enter `dev`.
 - **Database port:** Enter `5439`.
 - **Master user name:** Enter `awsuser`.
 - **Master user password** and **Confirm password**: Enter a password for the master user account.

Please note: We strongly advise you to keep these passwords closely guarded, including not putting them in your GitHub public repo, etc.

Launch your Amazon Redshift cluster - Advanced settings | [Switch to quick launch](#)

CLUSTER DETAILS NODE CONFIGURATION ADDITIONAL CONFIGURATION REVIEW

Provide the details of your cluster. Fields marked with * are required.

Cluster identifier*

This is the unique key that identifies a cluster. This parameter is stored as a lowercase string. (e.g. my-dw-instance)

Database name

Optional. A default database named dev is created for the cluster. Optionally, specify a custom database name (e.g. mydb) to create an additional database.

Database port*

Port number on which the database accepts connections.

Master user name*

Name of master user for your cluster. (e.g. awsuser)

Master user password*

Password must contain 8 to 64 printable ASCII characters excluding: /, ', \, and @. It must contain 1 uppercase letter, 1 lowercase letter, and 1 number.

Confirm password*

Confirm master user password

[Cancel](#)

[Continue](#)

- On the Node Configuration page, accept the default values and choose **Continue**.

Launch your Amazon Redshift cluster - Advanced settings | [Switch to quick launch](#)

CLUSTER DETAILS NODE CONFIGURATION ADDITIONAL CONFIGURATION REVIEW

Choose a number of nodes and node type below. Number of Compute Nodes is required for multi-node clusters.

The ds2 and dc2 node types replace the ds1 and dc1 node types, respectively. The newer ds2 and dc2 node types provide higher performance than ds1 and dc1 at no extra cost. [Learn more](#).

Node type

Specifies the compute, memory, storage, and I/O capacity of the cluster's nodes.

CPU 7 EC2 Compute Units (2 virtual cores) per node

Memory 15.25 GiB per node

Storage 160GB SSD storage per node

I/O performance Moderate

Cluster type

Number of compute nodes*

Single Node clusters consist of a single node which performs both leader and compute functions.

Maximum 1

Minimum 1

[Cancel](#)

[Previous](#)

[Continue](#)

- On the Additional Configuration page, enter the following values:

- **VPC security groups:** redshift_security_group
 - **Available IAM roles:** myRedshiftRole
- Choose Continue.

Publicly accessible Yes No Select Yes if you want the cluster to be accessible from the public internet. Select No if you want it to be accessible only from within your private VPC network.

Choose a public IP address Yes No Select Yes if you want to select your own public IP address from a list of elastic IP (EIP) addresses that are already configured for your cluster's VPC. Select No if you want Amazon Redshift to provide an EIP for you instead.

Enhanced VPC Routing Yes No Select Yes if you want to enable Enhanced VPC Routing. [Learn more](#)

Availability zone The EC2 Availability Zone that the cluster will be created in.

Associate your cluster with one or more security groups.

VPC security groups List of VPC security groups to associate with this cluster.

Optionally, create a basic alarm for this cluster.

Create CloudWatch Alarm Yes No Create a CloudWatch alarm to monitor the disk usage of your cluster.

Optionally, select your maintenance track for this cluster.

Maintenance Track Current Trailing Select Current to apply the latest certified maintenance release including features and bug-fixes. Select Trailing to apply the previously certified maintenance release.

Optionally, associate up to 10 IAM roles with this cluster.

Available IAM roles

6. Review your Cluster configuration and choose **Launch cluster**.

Launch your Amazon Redshift cluster - Advanced settings | [Switch to quick launch](#)

CLUSTER DETAILS NODE CONFIGURATION ADDITIONAL CONFIGURATION REVIEW

You are about to launch a cluster with following the following specifications:

Cluster properties

These attributes specify the name of your cluster, what type of virtual hardware it will run on, how many nodes it will contain, and the availability zone in which it will be located.

Cluster identifier: redshift-cluster

Node type: dc2.large

Number of compute nodes: 1 (leader and compute run on a single node)

Availability zone: No preference

Database configuration

Database name: dev
Database port: 5439

Master user name: awsuser

Cluster parameter group: default.redshift-1.0

Security, access, and encryption

These settings control whether your cluster will be created in an existing VPC to allow for simpler integration with other AWS Services, and the security groups which define access rules to your cluster.

Virtual private cloud: vpc-3924fa41

Cluster subnet group:

Publicly accessible: Yes

Elastic IP: Not used

VPC security groups: redshift_security_group (sg-0eafe91b9bd584f51)

Enhanced VPC Routing: No

Encrypt database: No

CloudWatch alarms

CloudWatch alarms are used to notify if metrics for your cluster are within a certain threshold. All recipients under the SNS topic specified for your alarm will receive notifications once an alarm is triggered.

Basic alarms will not be created for this cluster

[Cancel](#)

[Previous](#)

[Launch cluster](#)

7. A confirmation page will appear and the cluster will take a few minutes to finish. Choose **Clusters** in the left navigation pane to return to the list of clusters.

The screenshot shows the AWS Redshift dashboard. At the top, there's a navigation bar with the AWS logo, 'Services' dropdown, 'Resource Groups' dropdown, and a star icon. Below the navigation, there's a sidebar with links: 'Redshift dashboard', 'Clusters' (which is highlighted in orange), 'Query editor' (with a 'New' badge), 'Saved queries', 'Schemas', and 'Security'. On the right side, a large green-bordered box displays a confirmation message: 'Cluster redshift-cluster-1 is being created'. It includes a checkmark icon, a link to 'Amazon Redshift Pricing and Costs', and a note about accruing charges starting immediately. There's also a link to 'Applicable charges' and a note about the on-demand hourly rate being \$0 for now.

8. On the Clusters page, look at the cluster that you just launched and review the **Cluster Status** information. Make sure that the **Cluster Status** is **available** and the **Database Health** is **healthy** before you try to connect to the database later. You can expect this to take 5-10 minutes.

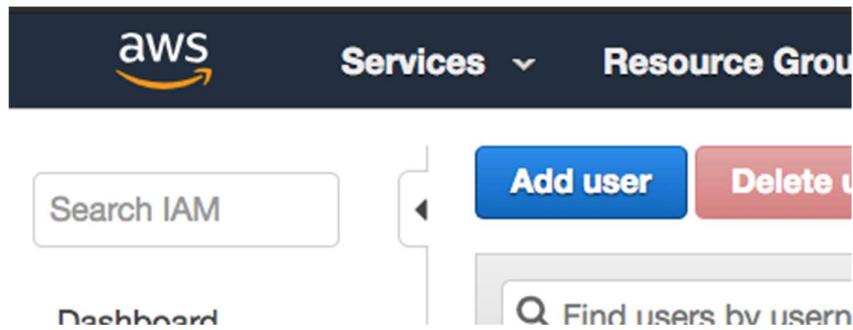
Cluster	Cluster Status	DB Health	Release Status	In Maintenance	Recent Events	Config timeline
redshift-cluster-1	creating	unknown	Not found	unknown	8	View timeline

Cluster	Cluster Status	DB Health	Release Status	In Maintenance	Recent Events	Config timeline
redshift-cluster-1	available	healthy	Up to date	no	9	View timeline

Create an IAM User

Here, you'll create an IAM user that you will use to access your Redshift cluster.

1. Sign in to the AWS Management Console and open the IAM console at <https://console.aws.amazon.com/iam/>.
2. In the left navigation pane, choose **Users**.
3. Choose **Add User**.



4. Enter a name for your user (e.g. `airflow_redshift_user`)
5. Choose **Programmatic access**, then choose **Next: Permissions**.

The screenshot shows the 'Set user details' step of the 'Add user' wizard. At the top, it says 'Add user' and shows a progress bar with step 1 highlighted in blue. Below that, there's a section titled 'Set user details' with a note: 'You can add multiple users at once with the same access type and permissions.' A 'User name*' field contains 'airflow_redshift_user'. There's also a link to 'Learn more' and a blue 'Add another user' button.

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type* **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

AWS Management Console access
Enables a **password** that allows users to sign-in to the AWS Management Console.

* Required Cancel **Next: Permissions**

6. Choose **Attach existing policies directly**.
7. Search for redshift and select **AmazonRedshiftFullAccess**. Then, search for S3 and select **AmazonS3ReadOnlyAccess**. After selecting both policies, choose **Next: Tags**.
8. Skip this page and choose **Next: Review**.

▼ Set permissions

Add user to group Copy permissions from existing user **Attach existing policies directly**

Create policy

	Policy name ▾	Type	Used as	Description
<input type="checkbox"/>	AmazonDMSRedshi...	AWS managed	None	Provides access to manage S3 settings for ...
<input type="checkbox"/>	AmazonMachineLe...	AWS managed	None	Allows Machine Learning to configure and u...
<input checked="" type="checkbox"/>	AmazonRedshiftFull...	AWS managed	Permissions policy (1)	Provides full access to Amazon Redshift via...
<input type="checkbox"/>	AmazonRedshiftQu...	AWS managed	Permissions policy (1)	Provides full access to the Amazon Redshift...
<input type="checkbox"/>	AmazonRedshiftRe...	AWS managed	Permissions policy (1)	Provides read only access to Amazon Reds...
<input type="checkbox"/>	AWSQuickSightDes...	AWS managed	None	Allow QuickSight to describe Redshift resou...

Showing 6 results

Cancel **Previous** **Next: Tags**

▼ Set permissions

Add user to group Copy permissions from existing user **Attach existing policies directly**

Create policy

	Policy name ▾	Type	Used as	Description
<input type="checkbox"/>	AmazonDMSRedshi...	AWS managed	None	Provides access to manage S3 settings for ...
<input type="checkbox"/>	AmazonS3FullAccess	AWS managed	Permissions policy (3)	Provides full access to all buckets via the A...
<input checked="" type="checkbox"/>	AmazonS3ReadOnl...	AWS managed	Permissions policy (5)	Provides read only access to all buckets via...
<input type="checkbox"/>	QuickSightAccessF...	AWS managed	None	Policy used by QuickSight team to access c...

Showing 4 results

Cancel **Previous** **Next: Tags**

9. Review your choices and choose **Create user**.

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	airflow_redshift_user
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	AmazonRedshiftFullAccess
Managed policy	AmazonS3ReadOnlyAccess

Tags

No tags were added.

[Cancel](#)

[Previous](#)

[Create user](#)

10. **Save your credentials!** This is the only time you can view or download these credentials on AWS. Choose **Download .csv** to download these credentials and then save this file to a safe location. You'll need to copy and paste this **Access key ID** and **Secret access key** in the next step. We **strongly advise** you to keep this **Access key ID** and **Secret access key** closely guarded, including not putting them in a GitHub public repo, etc.

Add user

1 2 3 4 5



Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://junolee.signin.aws.amazon.com/console>

[Download .csv](#)

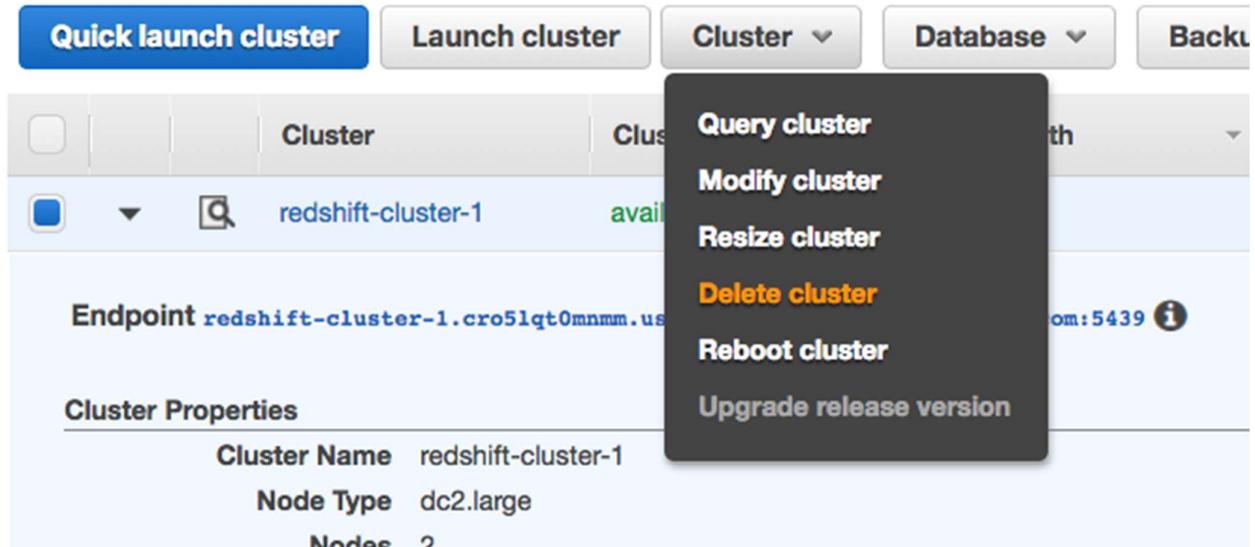
	User	Access key ID	Secret access key
▶	✓ airflow_redshift_user	AKIAJBGNV3NT4NVHNDKA	***** Show

[Close](#)

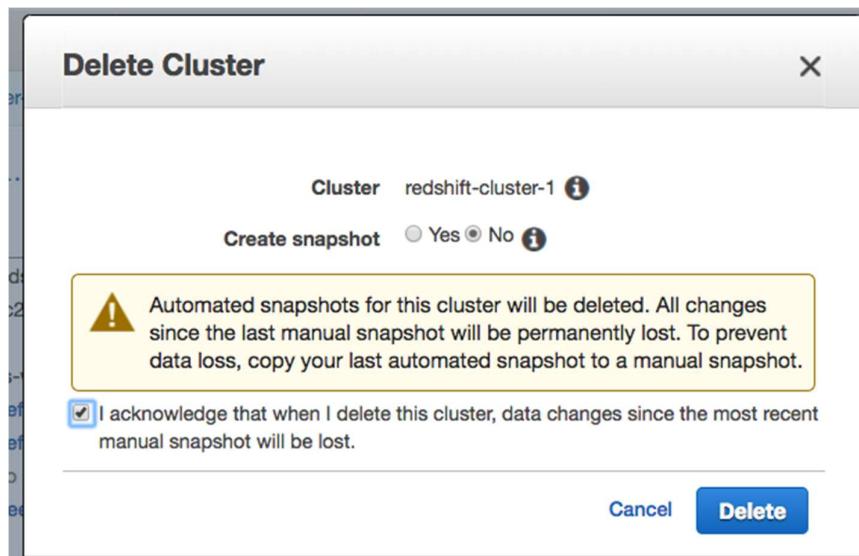
Delete a Redshift Cluster

Make sure to delete your cluster each time you're finished working to avoid large, unexpected costs. You can always launch a new cluster, so don't leave it running overnight or throughout the week if you don't need to.

1. On the **Clusters** page of your Amazon Redshift console, click on the box next to your cluster to select it, and then click on **Cluster > Delete cluster**.



2. You can choose No for **Create snapshot**, check the box that you acknowledge this, and then choose **Delete**.



3. Your cluster will change its status to **deleting**, and then disappear from your Cluster list once it's finished deleting. You'll no longer be charged for this cluster.

Cluster	Cluster Status	DB Health	Release Status	In Maintenance	Recent Events	Config timeline
redshift-cluster-1	deleting	healthy	Up to date	no	9	<input checked="" type="checkbox"/> View timeline

Create an S3 Bucket

1. Go to the [Amazon S3 Console](#) and select Create bucket.

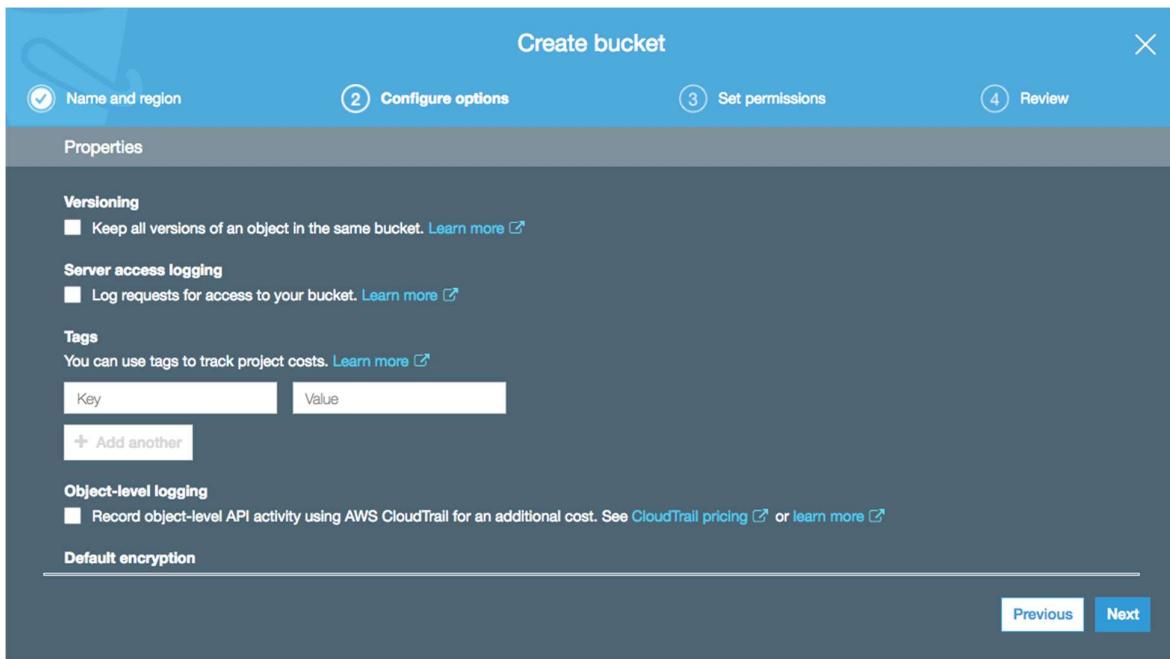
The screenshot shows the Amazon S3 console interface. On the left, there's a sidebar with 'Amazon S3' at the top, followed by 'Buckets', 'Public access settings for this account', and 'Feature spotlight'. The main area is titled 'S3 buckets' and contains a search bar with 'Search for buckets'. Below the search bar are four buttons: '+ Create bucket' (highlighted in blue), 'Edit public access settings', 'Empty', and 'Delete'. At the bottom, there's a dropdown menu labeled 'Bucket name' and a link 'Access' with a help icon.

2. Enter a name for your bucket and select the region you'd like to create it in.

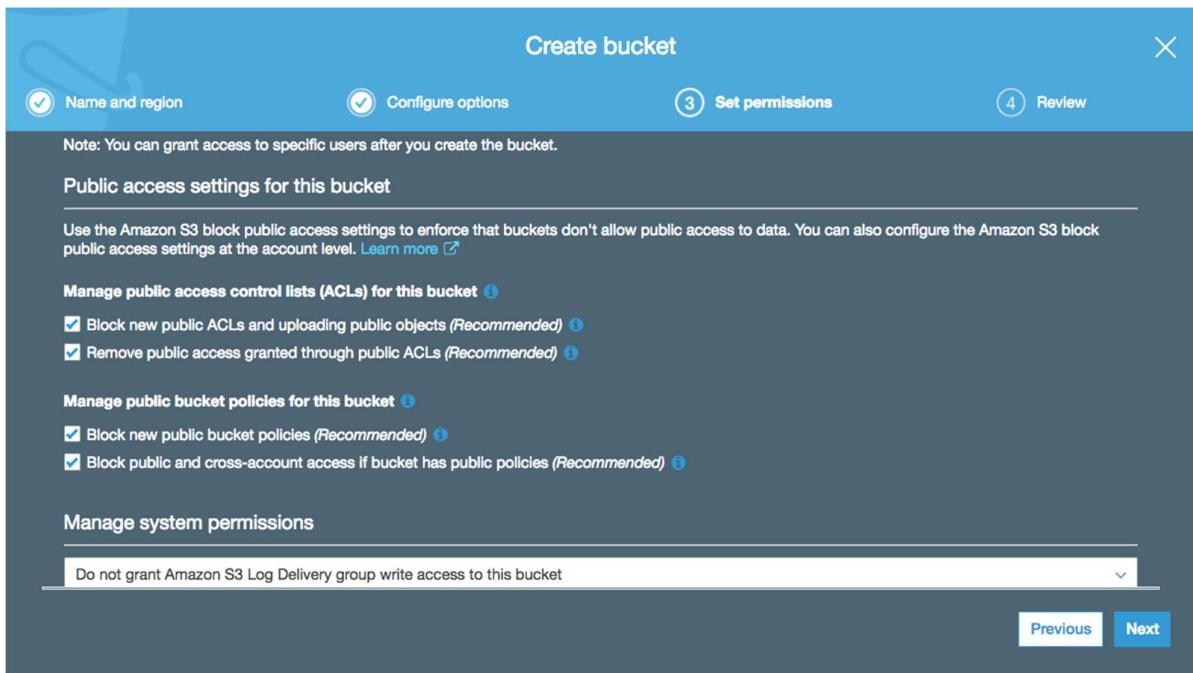
You won't be able to use the same name entered in the screenshot below - the names of all existing buckets on Amazon S3 are unique. You won't be able to change this name later, so choose one that makes sense for the content you'll have in it. This bucket name will be included in any URLs pointing to objects you add in your bucket.

The screenshot shows the 'Create bucket' wizard. The top navigation bar has four steps: 1) Name and region (highlighted in blue), 2) Configure options, 3) Set permissions, and 4) Review. The main section is titled 'Name and region'. It includes fields for 'Bucket name' (containing 'dend-bucket-demo'), 'Region' (set to 'US West (Oregon)'), and 'Copy settings from an existing bucket' (with a dropdown menu showing 'Select bucket (optional) 1 Buckets'). At the bottom, there are 'Create' and 'Next' buttons.

3. Keep the default settings and select Next.



4. Specify **public access settings** for this bucket. For example, unchecking all of these boxes would allow anyone to be able to access this bucket. Be careful with this - you may end up having to pay lots of fees in data transfers from your bucket if you share this link and many people access large amounts of data with it. For this demo, we will leave all of these boxes checked.



5. Review your settings and select **Create bucket**.

Create bucket

X

4 Review

Name and region Configure options Set permissions

Name and region Edit

Bucket name dend-bucket-demo **Region** US West (Oregon)

Options Edit

Versioning	Disabled
Server access logging	Disabled
Tagging	0 Tags
Object-level logging	Disabled
Default encryption	None
CloudWatch request metrics	Disabled
Object lock	Disabled

Permissions Edit

Block new public ACLs and True

[Previous](#) Create bucket

6. You should now see your bucket in your list. Any buckets you've made public will be labeled so here.

S3 buckets Discover the console

Search for buckets All access types

[+ Create bucket](#) [Edit public access settings](#) [Empty](#) [Delete](#) 2 Buckets 1 Regions

<input type="checkbox"/> Bucket name	Access	Region	Date created
<input type="checkbox"/> dend	Public	US West (Oregon)	Dec 20, 2018 5:53:57 PM GMT-0700
<input checked="" type="checkbox"/> dend-bucket-demo	Bucket and objects not public	US West (Oregon)	Feb 20, 2019 10:15:44 AM GMT-0700

Delete S3 Bucket

To delete the bucket, select the bucket and click **Delete**.

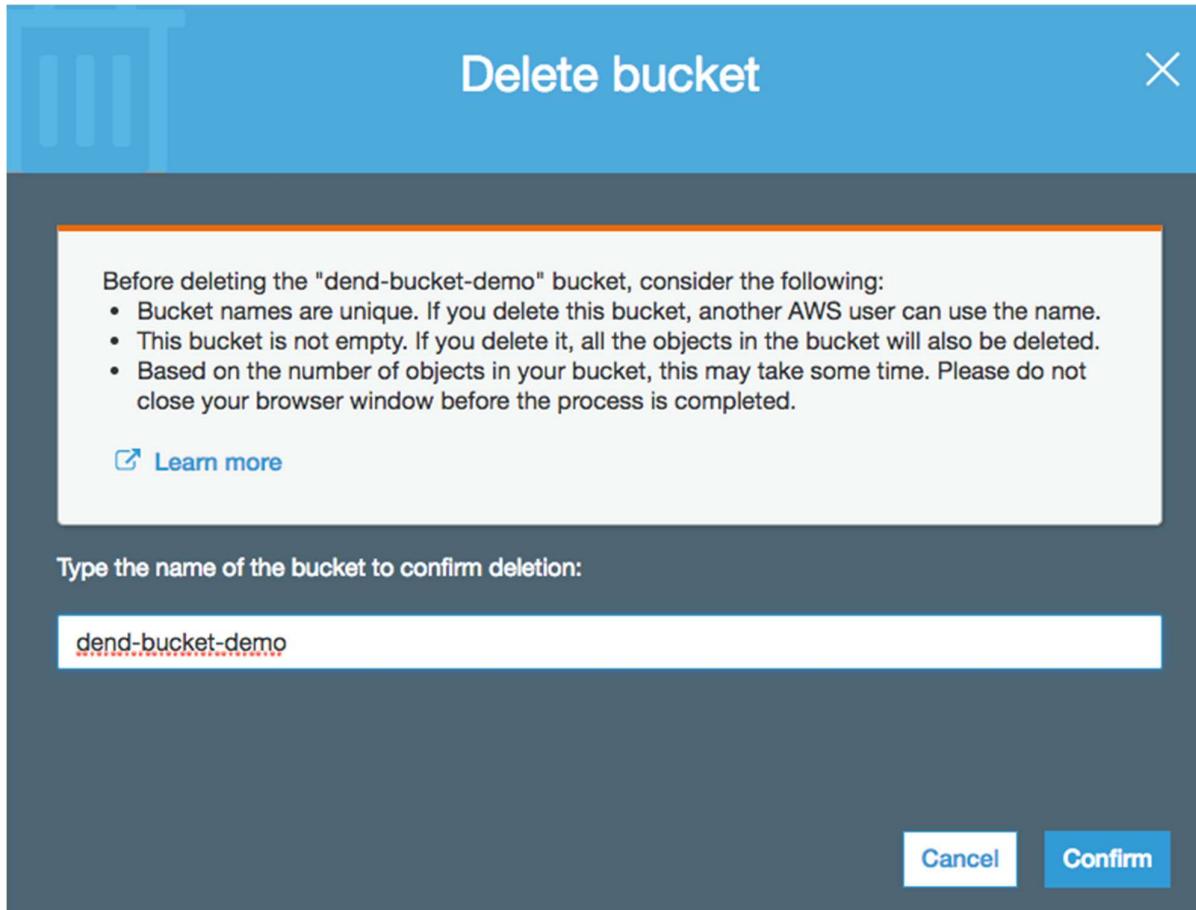
[+ Create bucket](#) [Edit public access settings](#) [Empty](#) [Delete](#)

Bucket name Access

<input type="checkbox"/> dend	Public
<input checked="" type="checkbox"/> dend-bucket-demo	Bucket and objects not public

Properties
 Static
 Rec
 Transfer

Then, enter the name of the bucket and select **Confirm**.



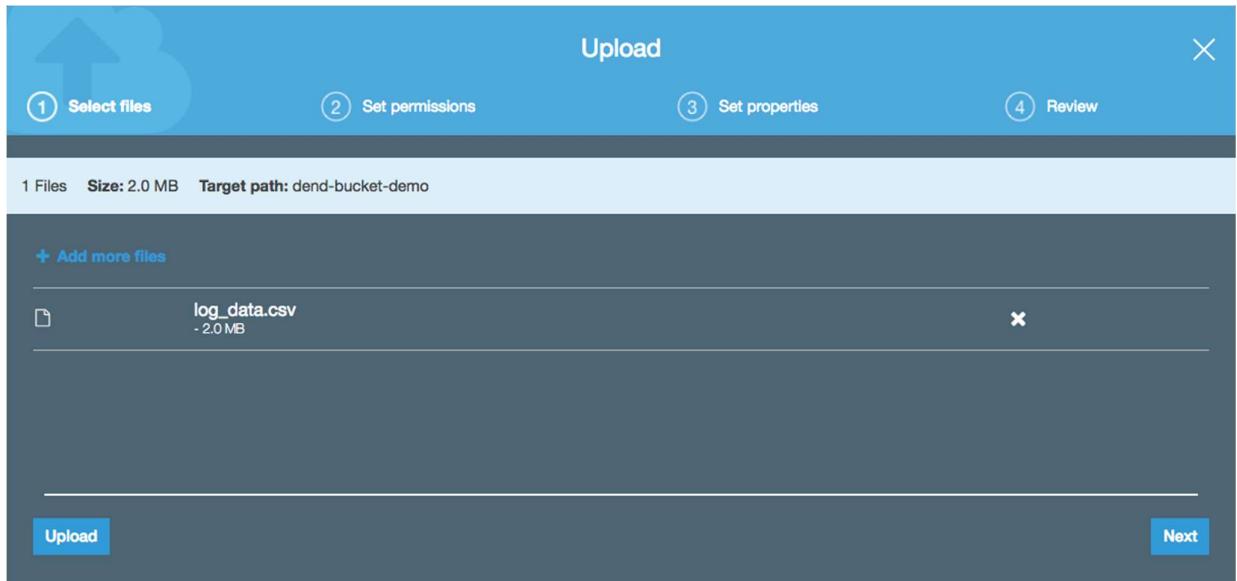
Upload to S3 Bucket

- For this exercise, download and upzip `log_data` from the Resources tab in the classroom.
1. Click on the bucket you just created and select **Upload** on the top left.

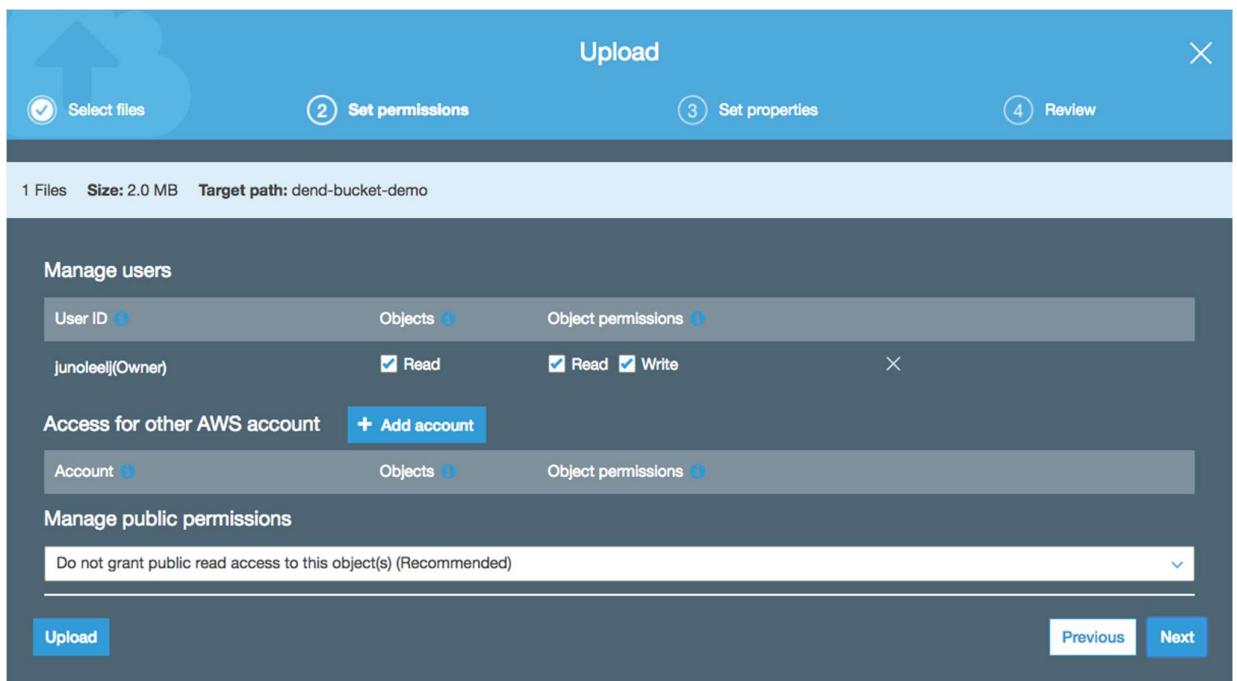
The screenshot shows the Amazon S3 console. In the top navigation bar, 'Amazon S3' is selected, and the path 'dend-bucket-demo' is shown. Below the navigation is a horizontal menu bar with four tabs: 'Overview' (selected), 'Properties', 'Permissions', and 'Management'. Underneath the menu bar are several buttons: 'Upload' (highlighted in blue), '+ Create folder', 'Download', and 'Actions'. A large central area displays the message 'This bucket is empty. Upload new objects to'.

2. Select **Add files** and choose the `log_data.csv` file you downloaded from this classroom.

The screenshot shows the 'Upload' wizard for AWS S3. The title bar says 'Upload'. Below it, there are four numbered steps: 1) Select files, 2) Set permissions, 3) Set properties, and 4) Review. The main area has a dark background with a large white 'Upload' icon. It includes a placeholder text 'Drag and drop here OR' and a 'Add files' button. At the bottom, there are 'Upload' and 'Next' buttons.



3. Leave the default settings and select **Next**.



4. Choose the **Standard** storage class and select **Next**.

Upload

Select files Set permissions Set properties Review

1 Files Size: 2.0 MB Target path: dend-bucket-demo

Storage class
Choose a storage class based on your use case and access requirements. [Learn more](#) or see [Amazon S3 pricing](#)

Storage class	Designed for	Availability Zones	Min storage duration	Min billable object size	Monitoring and automation fees	Retrieval fees
<input type="radio"/> Standard	Frequently accessed data	≥ 3	-	-	-	-
<input checked="" type="radio"/> Intelligent-Tiering	Long-lived data with changing or unknown access patterns	≥ 3	30 days	-	Per-object fees apply	-
<input type="radio"/> Standard-IA	Long-lived, infrequently accessed data	≥ 3	30 days	128KB	-	Per-GB fees apply
<input type="radio"/> One Zone-IA	Long-lived, infrequently accessed, non-critical data	≥ 1	30 days	128KB	-	Per-GB fees apply

Upload Previous Next

5. Review your settings and select **Upload**.

Upload

Select files Set permissions Set properties Review

Files Edit
1 Files Size: 2.0 MB

Permissions Edit
1 grantees

Properties Edit

Encryption No Storage class Standard
Metadata
Tag

Previous Upload

6. You should be able to see details on the file you just uploaded by selecting it in your bucket.

Type a prefix and press Enter to search. Press ESC to clear.

Upload + Create folder Download Actions ▾

<input checked="" type="checkbox"/> Name ▾	Last modified ▾
<input checked="" type="checkbox"/> log_data.csv	Feb 20, 2019 10:41:09 AM GMT-0700

log_data.csv

Download Copy path Select from

Latest version ▾

Overview

Key	log_data.csv
Size	2.0 MB
Expiration date	N/A
Expiration rule	N/A
ETag	02d47b26d067f8a223ee4e2699fe3b
Last modified	Feb 20, 2019 10:41:09 AM GMT-0700
Object URL	https://s3-us-west-2.amazonaws.com/dend-bucket-demo/log_data.csv

Properties

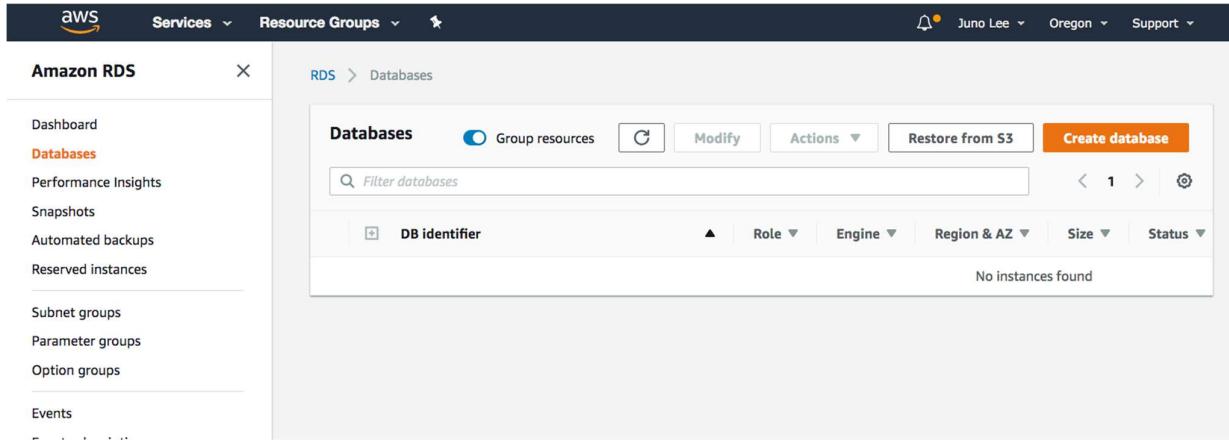
Storage class	Standard
Encryption	None
Metadata	1
Tags	0 Tags
Object lock	Disabled

Permissions

Owner: junooleeli

Create a PostgreSQL DB Instance using RDS

1. Go to the [Amazon RDS console](#) and click on **Databases** on the left navigation pane. Choose what region you'd like to create this database in on the right of the top menu bar.
2. Click on the **Create Database** button.



The screenshot shows the AWS RDS console interface. The left sidebar has 'Amazon RDS' selected under 'Databases'. The main area is titled 'Databases' and shows a table with one column: 'DB identifier'. A search bar at the top says 'Filter databases'. Below the table, it says 'No instances found'. The top navigation bar includes 'Services', 'Resource Groups', and user information 'Juno Lee', 'Oregon', and 'Support'.

3. Select **PostgreSQL** on the Select Engine page.

Select engine

Engine options

Amazon Aurora

Amazon
Aurora

MySQL



MariaDB



PostgreSQL



Oracle

ORACLE®

Microsoft SQL Server



PostgreSQL

PostgreSQL is a powerful, open-source object-relational database system with a strong reputation of reliability, stability, and correctness.

- High reliability and stability in a variety of workloads.
- Advanced features to perform in high-volume environments.
- Vibrant open-source community that releases new features multiple times per year.
- Supports multiple extensions that add even more functionality to the database.
- Supports up to 5 Read Replicas per instance, within a single Region or cross-region.
- The most Oracle-compatible open-source database.

If you want to create PostgreSQL 11 in the Preview environment, click [here](#)

Aurora global database feature is now available.

This feature is now available in our new database creation flow.

[Try it now](#)

Only enable options eligible for RDS Free Usage Tier [Info](#)

[Cancel](#)

[Next](#)

4. Since this is for demonstration purposes, select **Dev/Test** under Use case.

Choose use case

Use case

Do you plan to use this database for production purposes?

Use case

Production

Use [Multi-AZ Deployment](#) and [Provisioned IOPS Storage](#) as defaults for high availability and fast, consistent performance.

Dev/Test

This instance is intended for use outside of production or under the [RDS Free Usage Tier](#).

Billing is based on [RDS pricing](#) .

[Cancel](#)

[Previous](#)

[Next](#)

5. Next, is a long **Specify DB details** page. You can leave the default values (shown below) for most of these settings. Just make the following choices:

- For **DB instance class**, select `db.t2.small`

Specify DB details

Instance specifications

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

DB engine

PostgreSQL

License model [Info](#)

postgresql-license

DB engine version [Info](#)

PostgreSQL 10.6-R1



Free tier

The Amazon RDS Free Tier provides a single db.t2.micro instance as well as up to 20 GiB 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

GiB

(Minimum: 20 GiB, Maximum: 16384 GiB) Higher allocated storage [may improve](#) IOPS performance.

- For DB instance identifier, enter **postgresql-test** or another name of your choice
- Enter a master username and password

Estimated monthly costs

DB Instance	26.28 USD
Storage	2.30 USD
Total	28.58 USD

Billing estimate is based on on-demand usage as described in [Amazon RDS Pricing](#). Estimate does not include costs for backup storage, IOs (if applicable), or data transfer.

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

Settings

DB instance identifier [Info](#)
Specify a name that is unique for all DB instances owned by your AWS account in the current region.

DB instance identifier is case insensitive, but stored as all lower-case, as in "mydbinstance". Must contain from 1 to 63 alphanumeric characters or hyphens (1 to 15 for SQL Server). First character must be a letter. Cannot end with a hyphen or contain two consecutive hyphens.

Master username [Info](#)
Specify an alphanumeric string that defines the login ID for the master user.

Master Username must start with a letter. Must contain 1 to 63 alphanumeric characters.

Master password [Info](#)

Confirm password [Info](#)

Master Password must be at least eight characters long, as in "mypassword". Can be any printable ASCII character except "/", "", or "@".

[Cancel](#) [Previous](#) [Next](#)

- Leave the default values for the next few sections.

Configure advanced settings

Network & Security

Virtual Private Cloud (VPC) [Info](#)

VPC defines the virtual networking environment for this DB instance.

Default VPC (vpc-2cc4274b)



Only VPCs with a corresponding DB subnet group are listed.

Subnet group [Info](#)

DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.

default



Public accessibility [Info](#)

Yes

EC2 instances and devices outside of the VPC hosting the DB instance will connect to the DB instances. You must also select one or more VPC security groups that specify which EC2 instances and devices can connect to the DB instance.

No

DB instance will not have a public IP address assigned. No EC2 instance or devices outside of the VPC will be able to connect.

Availability zone [Info](#)

No preference



VPC security groups

Security groups have rules authorizing connections from all the EC2 instances and devices that need to access the DB instance.

Create new VPC security group

Choose existing VPC security groups

Database options

Database name [Info](#)

If you do not specify a database name, Amazon RDS does not create a database.

Port [Info](#)
TCP/IP port the DB instance will use for application connections.

DB parameter group [Info](#)
▼

Option group [Info](#)
▼

IAM DB authentication [Info](#)
 Enable IAM DB authentication
Manage your database user credentials through AWS IAM users and roles.
 Disable

Encryption

Encryption
 Enable encryption [Learn more](#) ⓘ
Select to encrypt the given instance. Master key ids and aliases appear in the list after they have been created using the Key Management Service(KMS) console.
 Disable encryption

- In the **Backup** section and select **1 day** since this is for demonstration purposes.

Backup

Backup retention period [Info](#)
Select the number of days that Amazon RDS should retain automatic backups of this DB instance.

▼

Backup window [Info](#)
 Select window
 No preference
 Copy tags to snapshots

Monitoring

Enhanced monitoring

Enable enhanced monitoring
Enhanced monitoring metrics are useful when you want to see how different processes or threads use the CPU.
 Disable enhanced monitoring

Monitoring Role ▼ Granularity ▼

I authorize RDS to create the IAM role rds-monitoring-role.

Performance Insights

Enable Performance Insights
 Disable Performance Insights

Retention period [Info](#)
▼

Master key [Info](#)

- Leave the default values for the rest and click on **Create database** on the bottom right.

Log exports

Select the log types to publish to Amazon CloudWatch Logs

Postgresql log
 Upgrade log

IAM role
The following service-linked role is used for publishing logs to CloudWatch Logs.

RDS Service Linked Role

Maintenance

Auto minor version upgrade [Info](#)

Enable auto minor version upgrade
Enables automatic upgrades to new minor versions as they are released. The automatic upgrades occur during the maintenance window for the DB instance.

Disable auto minor version upgrade

Maintenance window [Info](#)
Select the period in which you want pending modifications or patches applied to the DB instance by Amazon RDS.

Select window
 No preference

Deletion protection

Enable deletion protection
Protects the database from being deleted accidentally. While this option is enabled, you can't delete the database.

ⓘ Amazon RDS requires permissions to manage AWS resources on your behalf. By clicking Launch DB Instance, you grant permission for Amazon RDS to create a service-linked role in AWS IAM that contains the required permissions. [Learn more](#).

[Cancel](#) [Previous](#) [Create database](#)

You should land on a confirmation page.

Amazon RDS

RDS > Create database

Your DB instance is being created.
Note: Your instance may take a few minutes to launch.

Connecting to your DB instance

Once Amazon RDS finishes provisioning your DB instance, you can use a SQL client application or utility to connect to the instance.
[Learn about connecting to your DB instance](#)

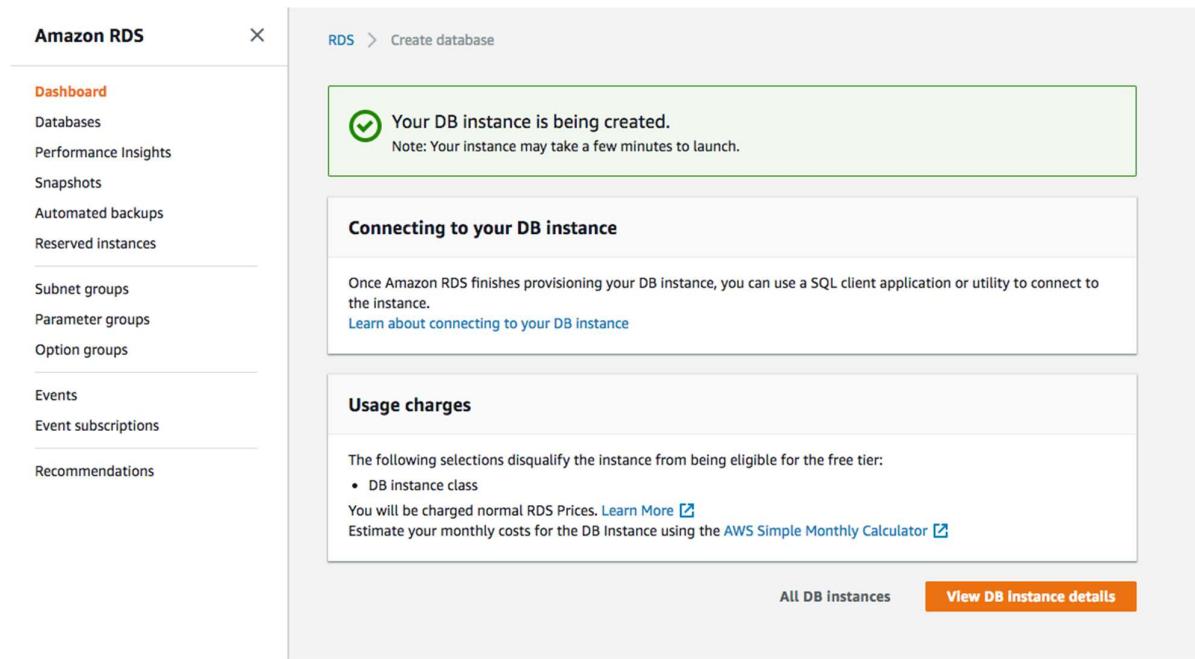
Usage charges

The following selections disqualify the instance from being eligible for the free tier:

- DB instance class

You will be charged normal RDS Prices. [Learn More](#)
Estimate your monthly costs for the DB Instance using the [AWS Simple Monthly Calculator](#)

All DB instances [View DB Instance details](#)



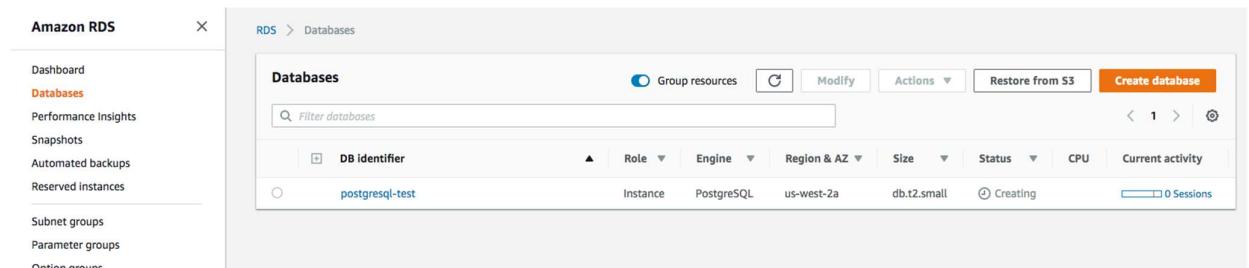
6. Click **Databases** on the left navigation pane to return to your list of databases. You should see your newly created database with the status **Creating**.

Amazon RDS

RDS > Databases

Databases

DB identifier	Role	Engine	Region & AZ	Size	Status	CPU	Current activity
postgresql-test	Instance	PostgreSQL	us-west-2a	db.t2.small	Creating	0	0 Sessions



7. Wait a few minutes for this to change to the status **Available**.

RDS > Databases

Databases

DB identifier	Role	Engine	Region & AZ	Size	Status	CPU	Current acti
postgresql-test	Instance	PostgreSQL	us-west-2a	db.t2.small	Available	5.00%	0 Se

