

# Introduction to Cloud Computing and AWS to GitHub

## Introduction to the Cloud and AWS

Welcome to this lesson on Introduction to the Cloud and AWS. You'll learn about the cloud infrastructure ecosystem and understand how to use essential tools for computing, storage, and analytics through one of the biggest providers of cloud computing, Amazon Web Services (AWS).

## Lesson Overview

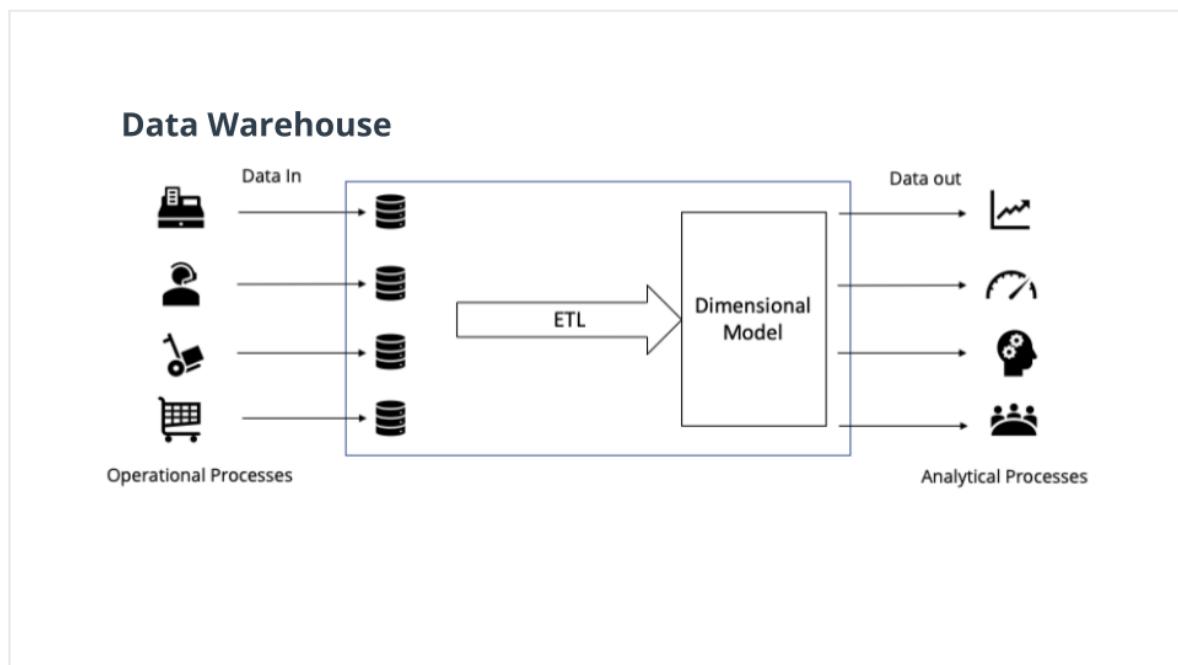
This lesson covers all the information you'll need in the next lesson to implement a Data Warehouse on AWS. It contains important reference material about:

- Creating IAM Roles
- Creating IAM Users
- Creating Security Groups
- Launching Redshift Clusters
- Deleting Redshift Clusters
- Creating S3 buckets

## Building Data Warehouses with AWS Redshift

You'll use AWS Redshift to build and query the dimensional model required to support analytical processes that are required in a Data Warehouse

Data Warehouse architecture



## What is Cloud Computing?

**Cloud computing:** the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

The arrival of cloud computing completely changed the way we deploy our

technology, providing powerful access to instant and scalable computing power to enterprises, startups, and developers alike. Whether you need servers to host a web application, reliable storage for your data, or machines to train machine learning models, it's easy to see the advantage of relying on the cloud rather than utilizing your personal computer or local servers.

For one, you no longer have to invest in lots of hardware upfront. No need to worry about whether you are paying for more than you'll need or what to do if you need to scale a lot more later on. Cloud computing makes this as easy and clicking a few buttons to scale your resources up or down.

It's significantly faster provisioning the resources you need through the cloud versus the time it would take to gather and build up the hardware you'd need to provide the same support. This allows you and your team, or company, to develop and experiment at a much faster rate.

Lastly, you can provide efficient access to your applications around the world by spreading your deployments to multiple regions.

## Amazon Web Services

Amazon Web Services is one of the largest providers in the cloud computing industry, with over 140 services in compute, storage, databases, networking, developer tools, security, and more. In this lesson, we'll learn about a few essential tools and services in AWS and practice using them. **These services can be accessed in three different ways: the AWS Management Console, the Command Line Interface (CLI), or Software Development Kits (SDKs)**, which can be used in combination.

We'll start with the AWS Management Console, which is the web user interface. The AWS CLI is a useful way to control and automate your services with code, and SDKs allow you to easily integrate services with your applications through APIs built around specific languages and platforms.

## Launch the AWS Web Console from your Udacity Classroom

You are given a *federated user account*, a temporary AWS user account with limited permissions, that you can use in this program.

Before you begin, be sure to **log out** of any AWS instances you may already have running. Then click on the "**LAUNCH CLOUD GATEWAY**" link in the left navigation pane to access a customized instance with the right permissions specific to this program. It will open up a pop-up, and clicking on the "**Open AWS Console**" button in the pop-up will open the AWS console in a new browser tab. This may take a few moments to load the first time. See a brief video below for a walkthrough.

Ensure that you do not have a pop-up blocker installed; it may prevent the new tab from launching. Please be sure to allow pop-ups from Udacity.

## Important Points to Remember

### 1. Session limit

Note that there is a certain **session time limit**. If reached, you will automatically be timed out. As long as you have not used your entire allocated budget, your work will be saved. You can re-launch using the same "Launch Cloud Gateway" button in the left navigation menu to return to your session.

### 2. Default AWS region

The default AWS region for you will be US East (N. Virginia) (*us-east-1*). However, you can switch and practice in *us-west-2* region as well. Note: You might not have necessary permissions to complete this course if you select regions other than *us-east-1* and *us-west-2*.

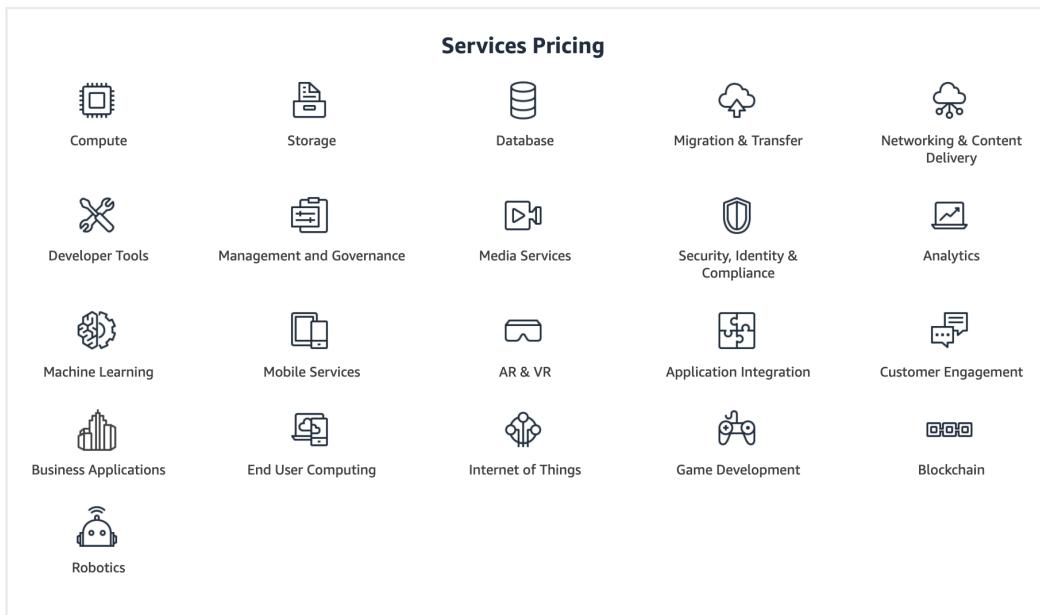
### 3. The budget allocated for you

All AWS services are a pay-as-you-go service. Udacity has set a budget for each student to complete their course work. Please understand that these credits are limited and available for you to use judiciously. **The budget for this entire course is \$25**. Although, we find about \$10 sufficient for most to complete this course.

### 4. Shut down your resources | No extra credits

We recommend you **shut down/delete every AWS resource** (e.g., EC2, Sagemaker, Database, EMR, CloudFormation) immediately after the usage or if you are stepping away for a few hours. Otherwise, you will run out of your allocated budget. **Udacity will not provide additional credits**. In case you exhaust your credits:

- **You will lose your progress on the AWS console.**
- **You will have to use your personal AWS account to finish the remaining ND.** Even if you are in the middle of the project/exercise and need to step away, you must shut down your resources. You can re-instantiate them later. To better understand pricing, see the **AWS Pricing** for all available services. > For reference, any service available to you @\$0.1/hour or higher should be monitored closely and shut down immediately after use or if you are stepping away. >

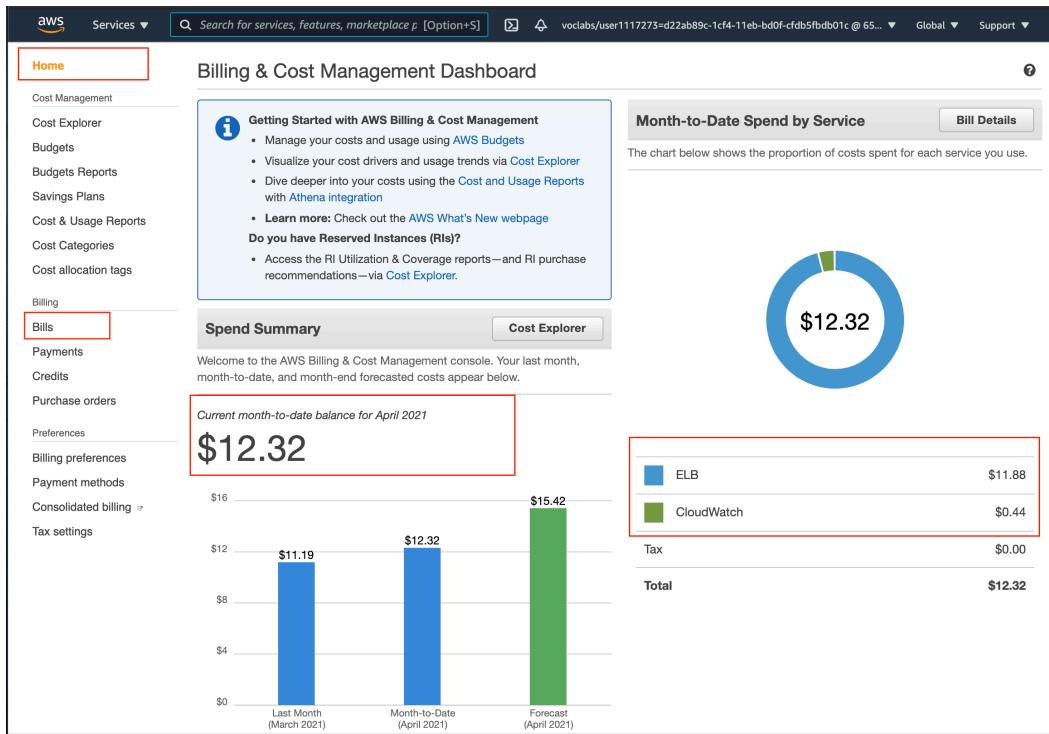


Check the pricing at <https://aws.amazon.com/pricing/>

## 5. Tracking your usage

You need to make sure that you have an adequate budget available to complete your project/task. **If you hit your budget, your session will time out and your work will be lost and unrecoverable.** Options for you to stay vigilant are:

- Track your usage on the AWS web console. Go to **AWS Billing Dashboard**, and view the monthly spending. It will list you the services constituting the spend.
- Submit a **ticket** to Student Support Services to know your current balance.



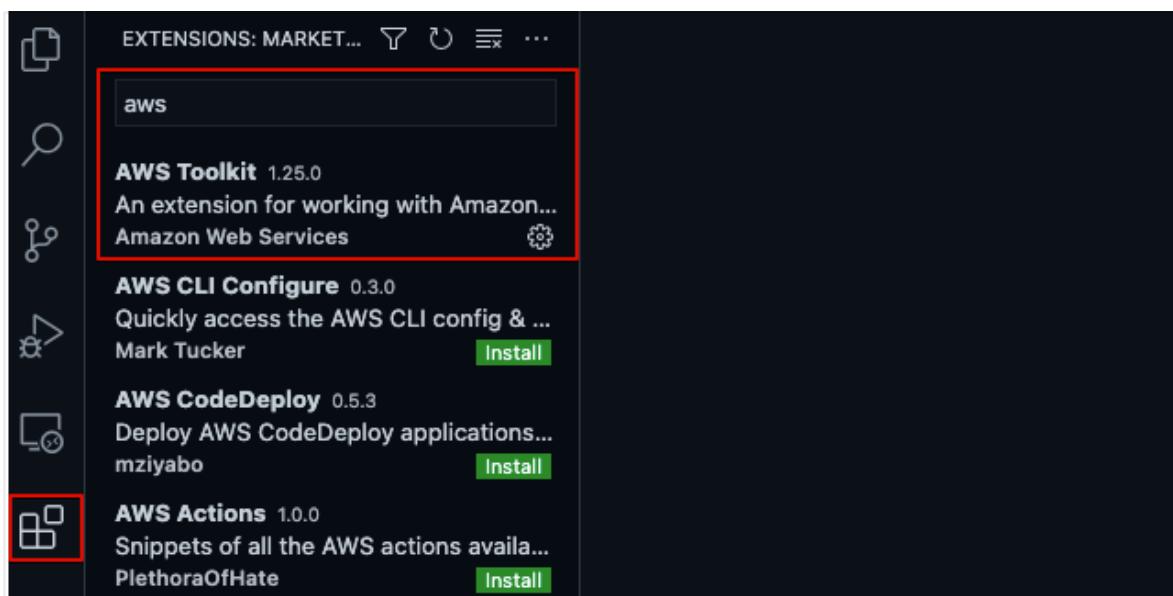
### Note -

As you are given a temporary AWS user account with **limited** permissions, you might not be able to avail **all** AWS services. We have allowed the necessary ones only. If you see a few warning messages related to insufficient permissions, you can ignore them and proceed with your practice.

## CONNECTING VS CODE WITH AWS

### Install AWS Toolkit Extension in VS Code

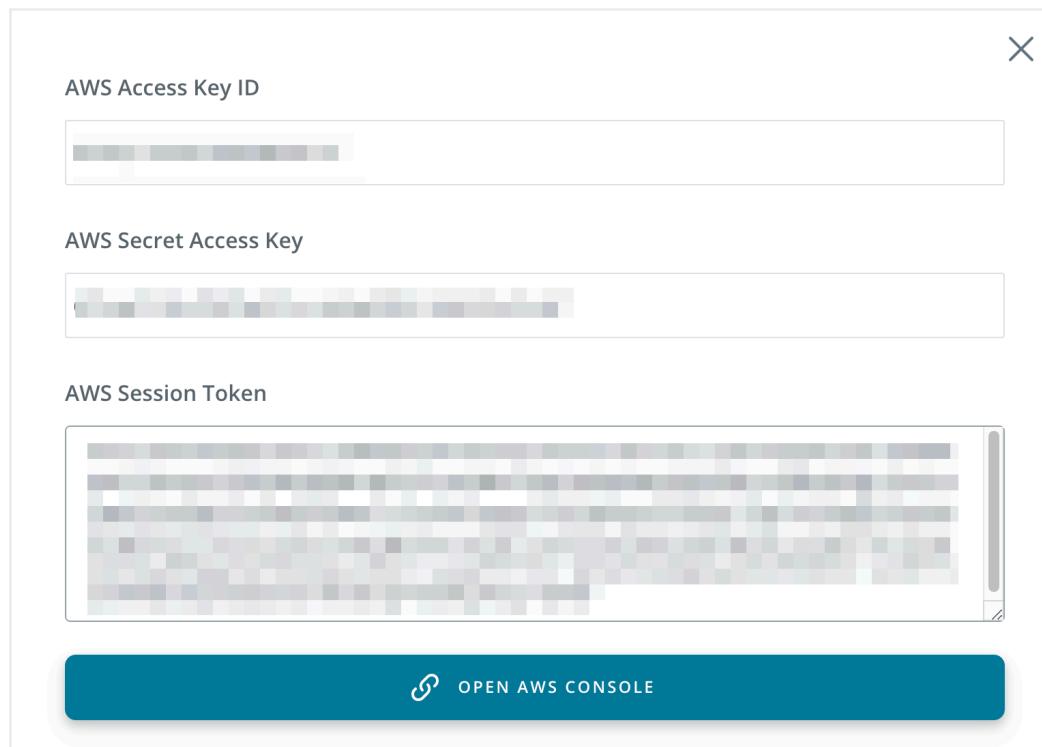
- Open **Extensions** tab
- Search **AWS**
- Install **AWS Toolkit**



**Step 1:** Create a new file called "credentials" with the following details:

```
[default]
aws_access_key_id=COPY_FROM_CLASSROOM
aws_secret_access_key=COPY_FROM_CLASSROOM
aws_session_token=COPY_FROM_CLASSROOM
```

Replace COPY\_FROM\_CLASSROOM with the values you see when you click on the "Launch AWS Gateway" button in the classroom as shown below.



**Step 2:** Create a new file called "config" with the following details:

[default]

region=us-west-2

output=json

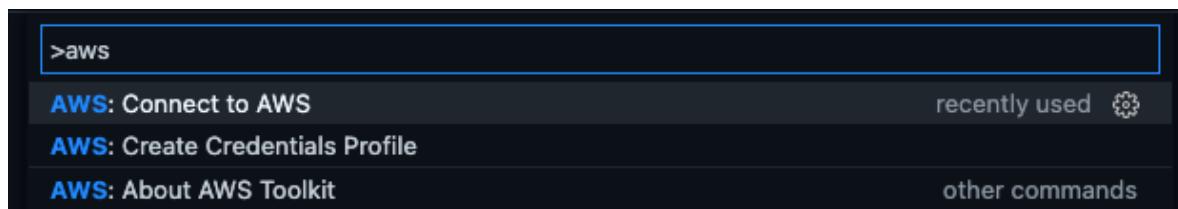
**Step 3:** Save the "credentials" and "config" file at the following location

Operating system	Location of files
Linux and macOS	~/.aws/config
	~/.aws/credentials
Windows	%USERPROFILE%\.aws\config
	%USERPROFILE%\.aws\credentials

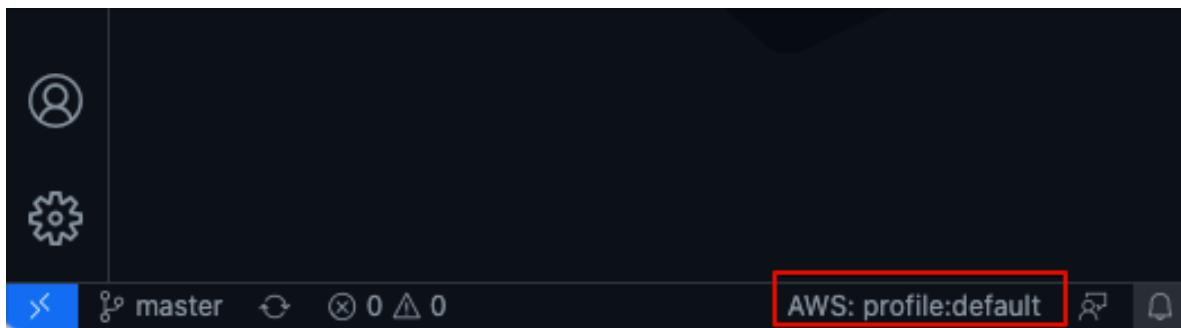
**Note** - If the .aws directory is not present, please create it first, and then save the files at the location specified in the table above.

## Connect to AWS

- Once the credentials are saved, open the VS Code's command palette by pressing Ctrl+Shift+P for Windows/Linux OR Cmd+Shift+P for Mac, and select AWS: Connect to AWS
- On a successful connection AWS: profile:default at the bottom left of VS Code window.



AWS: Connect to AWS

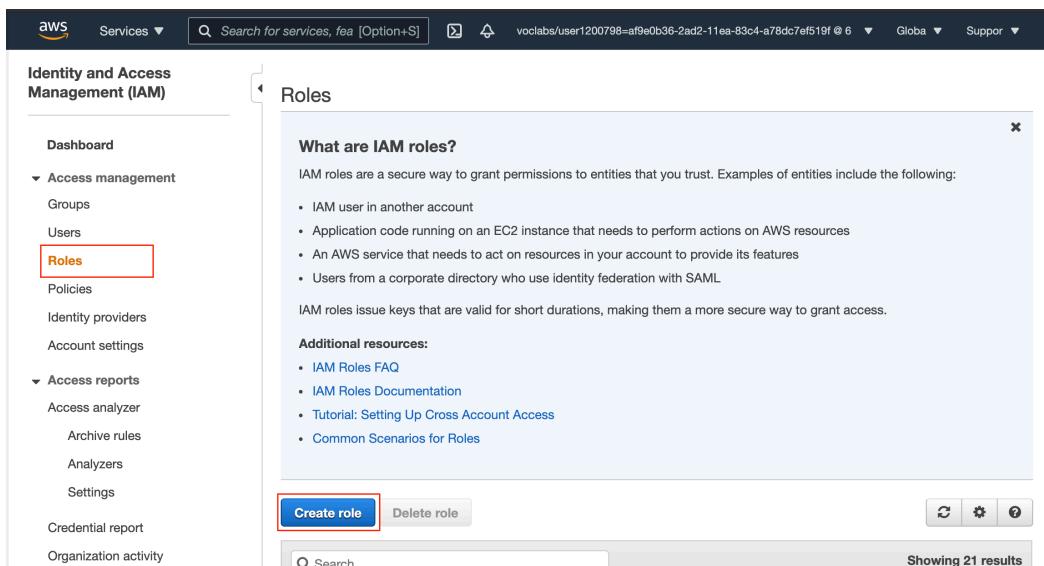


Successful AWS Connection Indicator

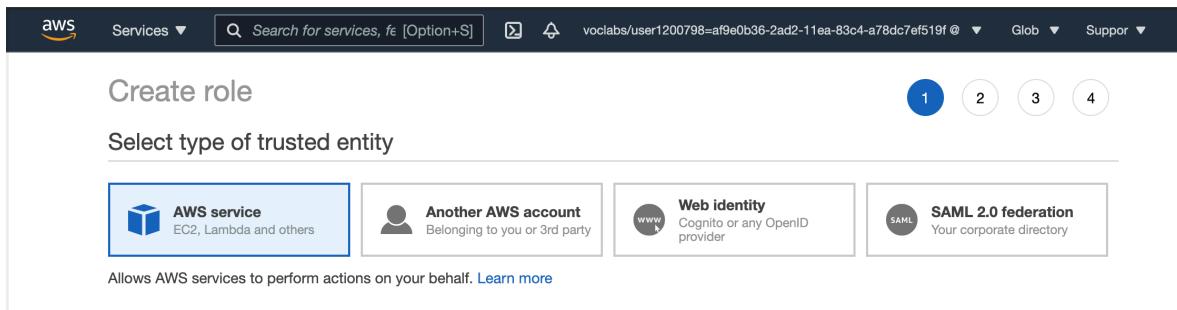
## Create an IAM Role

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](#).

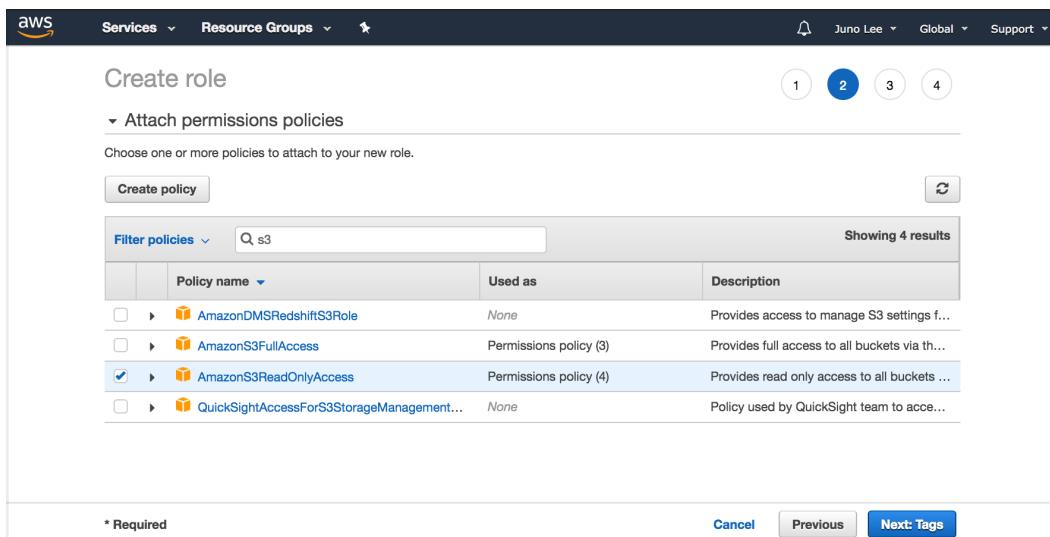
1. Once you have signed into the AWS management console, navigate to the **IAM service dashboard**. (Identity and Access Management). The IAM identity and Access Management (IAM) service to create user accounts and manage permissions for those accounts to control cluster operations
2. In the left navigation pane, choose **Roles**.
3. Choose **Create role**.



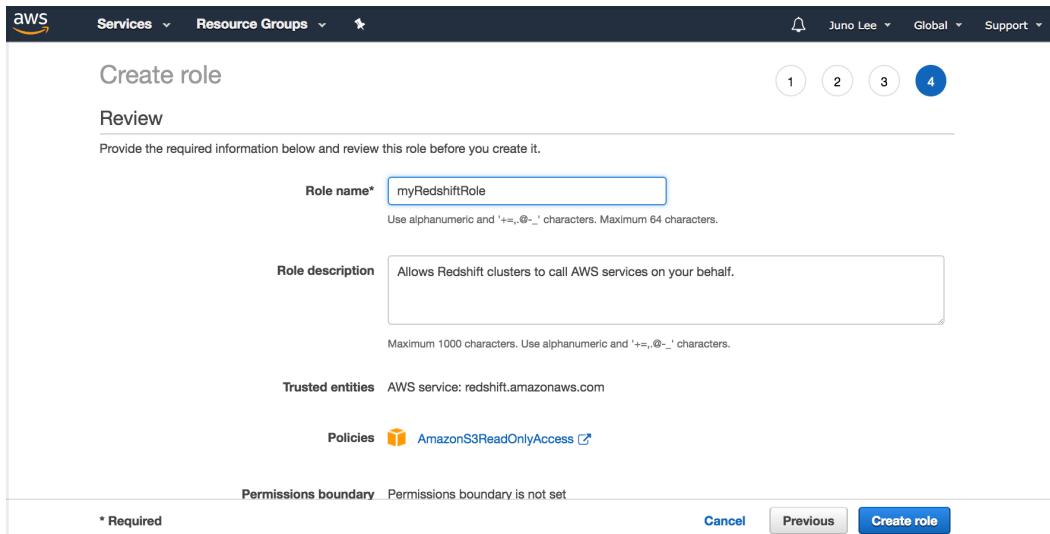
4. In the **AWS Service** group as the trusted entity, and choose **Redshift** service.
5. Under **Select your use case**, choose **Redshift - Customizable**, and then **Next: Permissions**.



6. On the **Attach permissions policies** page, search for and select the **AmazonS3ReadOnlyAccess** policy, and then click on the **Next: Tags** button.
7. Tags are optional. Click on the **Next: Review** button.



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



9. You will see a success message when the new role will be created.

✓ The role **myRedshiftRole** has been created.

Create role Delete role

🔍 ⚙️ ❓

Showing 1 result		
Role name ▾	Trusted entities	Last activity ▾
<input checked="" type="checkbox"/> myRedshiftRole	AWS service: redshift	None

## Create Security Group

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

*A security group will act as firewall rules for your Redshift cluster to control inbound and outbound traffic.*

### 1. Navigate to the **EC2 service**

The screenshot shows the AWS Management Console homepage. The top navigation bar includes the AWS logo, a 'Services' dropdown, a search bar ('Search for services, f [Option+S]'), and user account information ('voclabs/user1200798=af9e0b36-2ad2-11ea-83c4-a78dc7ef519f', 'N. Virgin', 'Support'). Below the navigation is a sidebar with 'Favorites' and 'Recently visited' sections. The 'Favorites' section lists 'Compute' (with 'EC2' highlighted), 'Customer Enablement', 'Machine Learning', 'Front-end Web & Mobile', 'AWS Amplify', 'Mobile Hub', 'AWS AppSync', 'Device Farm', 'Amazon Location S...', 'AR & VR', 'Amazon Sumerian', and 'Application Integration'. The 'Recently visited' section lists 'EC2' (highlighted with a red box), 'IAM', 'Console Home', 'CloudFormation', 'VPC', 'Elastic Container Service', 'Elastic Kubernetes Ser...', and 'Elastic Beanstalk'. A central 'All services' grid lists various AWS services like Lightsail, Lambda, Batch, Elastic Beanstalk, Serverless Application, AWS Outposts, EC2 Image Builder, Customer Support, Managed Services, Activate for Startups, Blockchain, Satellite, Ground Station, Amazon SageMaker, Amazon Augmente..., Amazon CodeGuru, Amazon DevOps Guru, Amazon Comprehend, Amazon Forecast, Amazon Fraud Dete..., Amazon Kendra, Amazon Lex, Amazon Personalize, Amazon Polly, and Amazon Rekognition.

### 2. Under **Network and Security** in the left navigation pane, select **Security Groups**. Click the **Create Security Group** button to launch a wizard

The screenshot shows the AWS Management Console with the AWS logo at the top. The navigation bar includes 'Services', a search bar with placeholder 'Search for services, [Option+S]', and user information 'voclabs/user1200798=af9e0b36-2ad2-11ea-83c4-a78dc7ef519'. The main menu on the left has sections like 'Dedicated Hosts', 'Scheduled Instances', 'Capacity Reservations', 'Images', 'AMIs', 'Elastic Block Store' (with 'Volumes', 'Snapshots', 'Lifecycle Manager'), 'Network & Security' (with 'Security Groups' highlighted), 'Elastic IPs', 'Placement Groups', 'Key Pairs', and 'Network Interfaces'. The 'Security Groups' section shows a table with 6 rows. The first row is 'sg-0377c416a9ec9aeb5' with name 'launch-wizard-2', VPC ID 'vpc-cb298db6'. The second row is 'sg-046d7262b78c7d9c' with name 'default', VPC ID 'vpc-049aec40a1d6c6'. The third row is 'sg-04ed0c83738b83c79' with name 'launch-wizard-3', VPC ID 'vpc-cb298db6'. The fourth row is 'sg-09617c813b8311606' with name 'launch-wizard-4', VPC ID 'vpc-cb298db6'. The fifth row is 'sg-0b05374e50bed3f29' with name 'launch-wizard-1', VPC ID 'vpc-cb298db6'. The sixth row is 'sg-653b316c' with name 'default', VPC ID 'vpc-cb298db6'. A red box highlights the 'Create security group' button at the top right of the table.

3. In the *Create security group* wizard, enter the basic details.

Section	Field	Value
Basic details	Security group name	redshift_security_group
	Description	Authorise redshift cluster access
	VPC	Choose the default VPC It is a VPC in a default region, and has a public subnet in each Availability Zone. If a default VPC doesn't show up, <b>create a default VPC</b>

Create a default VPC, if not available already

Your VPCs [Info](#)

Filter VPCs

Name ▾ | VPC ID ▾

[Actions](#) ▾ [Create VPC](#)

- [Create default VPC](#)
- [Create flow log](#)
- [Edit CIDRs](#)
- [Edit DHCP options set](#)
- [Edit DNS hostnames](#)
- [Edit DNS resolution](#)

## Info about a default VPC

**Default VPC**

A default VPC enables you to launch Amazon EC2 resources without having to create and configure your own VPC and subnets. We'll create a default VPC with a default subnet in each Availability Zone, an internet gateway, and a route table with a route to the internet gateway.

[Cancel](#) [Create default VPC](#)

## Basic details

**Basic details**

Security group name [Info](#)  
redshift\_security\_group  
Name cannot be edited after creation.

Description [Info](#)  
Authorise redshift cluster access

VPC [Info](#)  
vpc-cb298db6 (default-vpc) ▾

4. In the *Inbound rules* section, click on **Add Rule** and enter the following values:

Section	Field	Value
Inbound rules	Type	Custom TCP Rule
	Protocol	TCP
	Port range	5439 The default port for Amazon Redshift is 5439, but your port might be different.

	Source type	Custom
	Source	0.0.0.0/0 <i>(Anywhere in the world)</i>

**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.

Inbound rules [Info](#)

Inbound rule 1 [Delete](#)

Type <a href="#">Info</a> Custom TCP	Protocol <a href="#">Info</a> TCP	Port range <a href="#">Info</a> 5439
Source type <a href="#">Info</a> Custom	Source <a href="#">Info</a> Q	Description - optional <a href="#">Info</a> Allow traffic from anywhere in the world
0.0.0.0/0 X		

[Add rule](#)

### Inbound rules

5. Outbound rules allow traffic to anywhere by default.

Outbound rules [Info](#)

Outbound rule 1 [Delete](#)

Type <a href="#">Info</a> All traffic	Protocol <a href="#">Info</a> All	Port range <a href="#">Info</a> All
Destination type <a href="#">Info</a> Custom	Destination <a href="#">Info</a> Q	Description - optional <a href="#">Info</a> Allow traffic to anywhere
0.0.0.0/0 X		

[Add rule](#)

### Outbound rules

6. Click on the Create security group button at the bottom. You will see a success message.

⌚ Security group (sg-0d62433f1477d8eca | redshift\_security\_group) was created successfully X

▶ Details

EC2 > Security Groups > sg-0d62433f1477d8eca - redshift\_security\_group Actions ▾

**sg-0d62433f1477d8eca - redshift\_security\_group**

Details				
Security group name redshift_security_group	Security group ID sg-0d62433f1477d8eca	Description Authorise redshift cluster access	VPC ID vpc-cb298db6	
Owner 644752792305	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry		

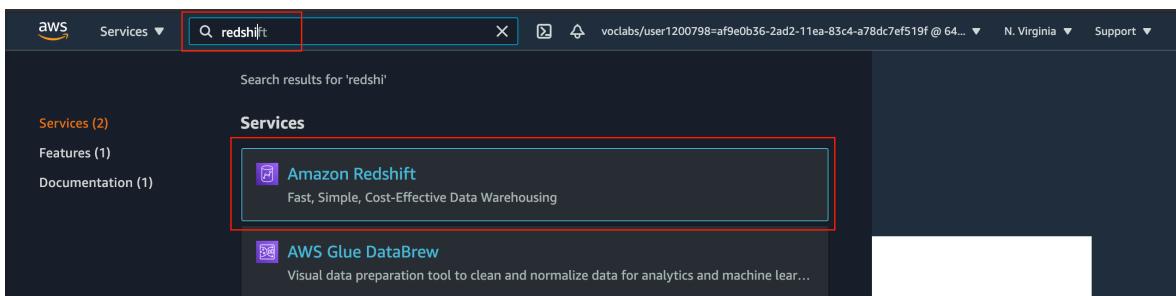
**Inbound rules** Edit inbound rules

Type	Protocol	Port range	Source	Description - optional
Redshift	TCP	5439	0.0.0.0/0	Allow traffic from anywhere in the world

## Launch a Redshift Cluster

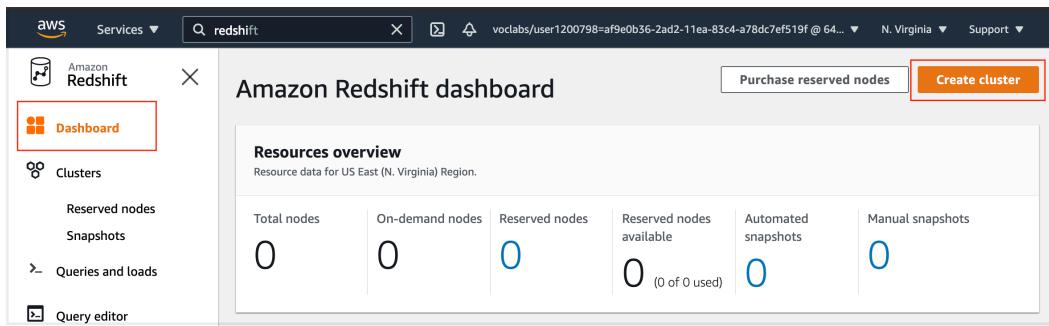
**WARNING:** The cluster that you are about to launch will be live, and you will be charged the standard Amazon Redshift usage fees for the cluster until you delete it. You will not need to use the Redshift cluster in this lesson. If you create a Redshift cluster now, **Make sure to delete it each time 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.

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



Navigate to a new service

2. On the Amazon Redshift Dashboard, choose **Create cluster**. It will launch the *Create cluster* wizard.



Amazon redshift dashboard

### 3. Cluster configuration

Provide a unique identifier, such as redshift-cluster-1, and choose the **Free trial** option. It will automatically, choose the following configuration:

- 1 node of dc2.large hardware type. It is a high performance with fixed local SSD storage
- 2 vCPUs
- 160 GB storage capacity
-

## Cluster configuration

### Cluster identifier

This is the unique key that identifies a cluster.

redshift-cluster-1

The identifier must be from 1-63 characters. Valid characters are a-z (lowercase only) and - (hyphen).

### What are you planning to use this cluster for?

**Production**

Configure for fast and consistent performance at the best price.

**Free trial**

Configure for learning about Amazon Redshift. This configuration is free for a limited time if your organization has never created an Amazon Redshift cluster.

 If your organization has never created an Amazon Redshift cluster, you're eligible for a free limited time trial of our dc2.Large node. The following are estimated charges if you are not eligible for a free trial.

[Learn more](#)

### Calculated configuration summary

dc2.large | 1 node

High performance with fixed local SSD storage

#### Compute

2 vCPU (gen 2) / node x 1 = 2 vCPU

Estimated on-demand compute price	Estimated reserved (1 year)	Estimated reserved (3 year)
-----------------------------------	-----------------------------	-----------------------------

\$2,190.00/year

\$0.25/node/hour

Estimated on-demand compute price	Estimated reserved (1 year)	Estimated reserved (3 year)
-----------------------------------	-----------------------------	-----------------------------

\$1,407.00/year

\$0.075/node/hour

**36% discount**

Estimated on-demand compute price	Estimated reserved (1 year)	Estimated reserved (3 year)
-----------------------------------	-----------------------------	-----------------------------

\$879.667/year

\$0.05/node/hour

**60% discount**

#### Storage capacity

160 GB x 1 nodes = 160 GB

## Cluster's basic configuration

### Calculated configuration summary

dc2.large | 1 node

High performance with fixed local SSD storage

#### Compute

2 vCPU (gen 2) / node x 1 = 2 vCPU

Estimated on-demand compute price

\$2,190.00/year

\$0.25/node/hour

Estimated reserved (1 year)

\$1,407.00/year

\$0.075/node/hour

**36% discount**

Estimated reserved (3 year)

\$879.667/year

\$0.05/node/hour

**60% discount**

Storage capacity

160 GB x 1 nodes = 160 GB

#### 4. Database configurations

A few fields will be already filled up by default. Ensure to have the following values:

Field	Value
Database name	dev
Database port	5439
Master user name	awsuser
Master user password	Enter a password of your choice

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

#### Database configurations

**Database name (optional)**  
Specify a database name to create an additional database.  
  
The name must be 1-64 alphanumeric characters (lowercase only), and it can't be a **reserved word**.

**Database port (optional)**  
Port number where the database accepts inbound connections. You can't change the port after the cluster has been created.  
  
The port must be numeric (1150-65535).

---

**Master user name**  
Enter a login ID for the master user of your DB instance.  
  
The name must be 1-128 alphanumeric characters, and it can't be a **reserved word**.

**Master user password**  
  
 Show password

**● The master password must be 8 - 64 characters.** **● The value must contain at least one uppercase letter.**  
**● The value must contain at least one lowercase letter.** **● The value must contain at least one number.**  
**● The master password can only contain ASCII characters (ASCII codes 33-126), except ' (single quotation mark), " (double quotation mark), /, \, or @.**

*Database configuration. For me, I do not have the first to textbook*

#### 5. Cluster permissions (optional)

Choose the IAM role created earlier, *myRedshiftRole*, from the drop-down and click on the Associate IAM role button.

▼ Cluster permissions (optional)

Your cluster needs permissions to access other AWS services on your behalf. For the required permissions, add IAM roles with the principal "redshift.amazonaws.com". You can associate up to 10 IAM roles with this cluster. [Learn more](#)

Available IAM roles	C	Associate IAM role
myRedshiftRole		
Associated IAM roles		
Status		
No IAM roles associated with this resource		

Cluster permissions

## 6. Additional configurations

Toggle the button to turn off the "use defaults" feature, and expand the **Network and security** section. Choose the following values:

Field	Value
Virtual private cloud (VPC)	Default VPC If you are not able to view/select the default VPC, refer to the resolution given <a href="#">here</a> . You will have to <b>create a cluster subnet group</b> . <i>(It's easy, see the snapshots below)</i>
VPC security groups	Choose the <i>redshift_security_group</i> created earlier.
Cluster subnet group	Choose the default It is the one you have just created.
Availability Zone	No preference
Enhanced VPC routing	Disabled
Publicly accessible	Enable

Leave the rest of the values as default.

## ▼ Network and security

### Virtual private cloud (VPC)

This VPC defines the virtual networking environment for this cluster.

Default VPC - default-vpc  
vpc-cb298db6

ⓘ You can't change the VPC associated with this cluster after the cluster has been created. [Learn more](#) X

### VPC security groups

This VPC security group defines which subnets and IP ranges the cluster can use in the VPC.

Choose one or more security groups

redshift\_security\_group X  
sg-0d62433f1477d8eca

default X  
sg-653b316c

### Cluster subnet group

Choose the Amazon Redshift subnet group to launch the cluster in.

cluster-subnet-group-1

### Availability Zone

Specify the Availability Zone that you want the cluster to be created in. Otherwise, Amazon Redshift chooses an Availability Zone for you.

No preference

### Enhanced VPC routing

Enabling this option forces network traffic between your cluster and data repositories through a VPC, instead of the internet. [Learn more](#)

- Disabled
- Enabled

### 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

Network and security section

## Create cluster subnet group

**Cluster subnet group details**

**Name**  
You can't modify the name after your subnet group has been created.  
 The name must be 1-255 characters. Valid characters are A-Z, a-z, 0-9, space, hyphen (-), underscore (\_), and period ( . ).

**Description**  
This is a cluster subnet group for demo purposes. We have added the default VPC and all its subnets.

**Add subnets**

**VPC**  
Choose the VPC that contains the subnets that you want to include in your cluster subnet group.

Availability Zone	Subnet	Add subnet
<input type="button" value="Choose an Availability Zone"/>	<input type="button" value="Choose a subnet"/>	<input type="button" value="Add subnet"/>

7. Review your Cluster configuration and click on the **Create cluster** button at the bottom. It will take a few minutes to finish and show you a **Complete** status.

⌚ Cluster subnet group cluster-subnet-group-1 was created successfully X

Amazon Redshift > Configurations > Subnet groups

Cluster subnet groups (1/1)							<input type="button" value="C"/>	<input type="button" value="Delete"/>	<input type="button" value="Actions"/>	<input type="button" value="Create cluster subnet group"/>
	<input type="text" value="Search"/>						<	1	>	⟳
	Name	Status	VPC ID	Description	Tags					
<input type="checkbox"/>	cluster-subnet-group-1	<input checked="" type="checkbox"/> Complete	vpc-cb298db6	This is a cluster subne...						
	6 Subnets									

Success message/complete status

8. Click on the **Clusters** menu item from the left navigation pane, and look at the cluster that you just launched. Make sure that the **Status** is **Available** before you try to connect to the database later. You can expect this to take 5-10 minutes

The screenshot shows the Amazon Redshift console. In the left navigation pane, 'Clusters' is selected. The main content area displays a table titled 'Clusters (1)'. The first row in the table is highlighted with a red box around the 'Status' column, which shows 'Available'. Other columns include 'Cluster', 'Cluster namespace', 'Storage capacity us...', 'CPU utilization', and 'Snapsh...'. A success message at the top of the page reads: 'Cluster subnet group cluster-subnet-group-1 was created successfully'.

Cluster is ready to be connected

## Create an IAM User

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

1. Navigate to the **IAM console**. In the left navigation pane, choose **Users**, and click on the **Add User** button. It will launch a new wizard.

The screenshot shows the AWS Identity and Access Management (IAM) console. In the left navigation pane, 'Users' is selected. The main content area has a heading 'Add user' with a red box around it. Below it is a search bar and a table with two users: 'WindowsAd...' and 'Admin'. The table has columns for 'User name', 'Groups', 'Access key age', and 'Password age'. The 'WindowsAd...' user has 'None' in all columns. The 'Admin' user also has 'None' in all columns. There are also 'Delete user' and 'Edit user' buttons.

### 2. Set user details

Enter a name for your user , say `airflow_redshift_user`, and choose **Programmatic access**. Then click on the **Next: Permissions** button.

The screenshot shows the 'Add user' wizard, Step 1: Set user details. At the top right, there are five numbered tabs: 1, 2, 3, 4, 5. Tab 1 is highlighted. The section title is 'Set user details'. It says 'You can add multiple users at once with the same access type and permissions.' Below is a 'User name\*' field containing 'airflow\_redshift\_user'. There is also a '+ Add another user' link. The next section is 'Select AWS access type'. It says 'Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step.' Below are two options: 'Programmatic access' (selected) and 'AWS Management Console access'. Both descriptions mention the use of access keys and secret access keys. At the bottom, there is a note '\* Required' and a 'Cancel' button. To the right of the 'Cancel' button is a blue 'Next: Permissions' button.

Create IAM users -> Set user details

### 3. Set permissions

Choose **Attach existing policies directly** option.

- Search for redshift and select **AmazonRedshiftFullAccess**.
- Then, search for S3 and select **AmazonS3ReadOnlyAccess**.

After selecting both policies, choose **Next: Tags**. Skip this page and choose **Next: Review**.

Set permissions

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

Create policy

Filter policies redshift

	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

Create IAM user → Set permissions → Select *AmazonRedshiftFullAccess*

### 4. Review your choices and finally click on the **Create user** button.

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

Review the new IAM user details

### 5. 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.

The screenshot shows a modal window titled "Add user". At the top right are five numbered tabs: 1, 2, 3, 4, and 5, with tab 5 being the active one. The main area contains a "Success" message: "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." Below this message is a link: "Users with AWS Management Console access can sign-in at: <https://junolee.siginin.aws.amazon.com/console>". A "Download .csv" button is located above a table. The table has three columns: "User", "Access key ID", and "Secret access key". It lists a single user: "airflow\_redshift\_user". The "Access key ID" column shows the value "AKIAJBFNV3NT4NVHNDKA" and the "Secret access key" column shows "\*\*\*\*\* Show". A "Close" button is at the bottom right of the modal.

User created successfully.  
Copy the **Access key Id** and **Secret access key**.

## 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.

Steps to delete a cluster are:

1. On the **Clusters** page of your Amazon Redshift console, click on the check-box next to your cluster name. Then click on the **Actions** drop-down button on top → select **Delete**.

The screenshot shows the AWS Amazon Redshift Clusters page. On the left, there's a sidebar with various options like Dashboard, Clusters (which is selected and highlighted with a red box), Reserved nodes, Snapshots, Queries and loads, Query editor, Configurations, AWS Marketplace, Recommendations, and Alarms. The main area shows a table titled 'Clusters (1/1)' with one item: 'redshift-cluster-1' (dc2.large | 1 node | 160 GB). To the right of the table is a 'Actions' menu with several options: Manage cluster, Resize, Edit, Reboot, Relocate, Pause, Add AWS Partner integration, Delete (which is also highlighted with a red box), Defer maintenance, Modify publicly accessible setting, Backup and disaster recovery, Restore table, Create snapshot, Configure cross-region snapshot, Relocate, and Permissions.

## Delete a cluster

2. You can choose to not **Create final snapshot**, and click on the **Delete cluster** button.

The screenshot shows a confirmation dialog box titled 'Delete redshift-cluster-1?'. It contains the following text:  
Deleting the cluster causes the following results:

- Deletes all databases (and data) in the cluster.
- Deletes the automated snapshot.
- Retains all manual snapshots until you manually delete them (none exist).
- You can't rotate keys for encrypted manual snapshots if you delete this cluster.

Are you sure that you want to permanently delete **redshift-cluster-1?**  
**Final snapshot**  
You can create a final manual snapshot of your cluster before it's deleted so you can later restore it. Restoring it enables you to resume running the cluster and querying data.  
 **Create final snapshot**  
  
At the bottom are two buttons: 'Cancel' and 'Delete cluster' (which is highlighted with a red box).

Prompt before deleting the cluster

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.

=====

Let's learn how to create a bucket in **Amazon S3**, and view a few properties of an existing bucket.

## Create a Bucket

1. Navigate to the **S3 dashboard**, and click on the **Create bucket** button. It will launch a new wizard.

The screenshot shows the AWS S3 Buckets dashboard. On the left, there is a sidebar with options like 'Buckets', 'Access points', 'Batch Operations', 'Access analyzer for S3', 'Account settings for Block Public Access', and 'Storage Lens'. The main area is titled 'Buckets (0)' and contains a table with columns 'Name', 'Region', 'Access', and 'Creation date'. A message at the bottom says 'No buckets' and 'You don't have any buckets.' A prominent red 'Create bucket' button is located at the top right of the main area.

S3 service → Buckets dashboard.  
View all of the S3 buckets in your account  
(*S3 is a global service, not a region-specific*).

## 2. General configuration

Provide the bucket-name and the region where you want to locate the bucket. The bucket name must be unique worldwide, and must not contain spaces or uppercase letters.

The screenshot shows the 'Create bucket' wizard. At the top, it says 'Amazon S3 > Create bucket'. Below that is the title 'Create bucket' and a note that 'Buckets are containers for data stored in S3. [Learn more](#)'. The main section is titled 'General configuration' and contains fields for 'Bucket name' (with 'myawsbucket' entered) and 'Region' (set to 'US East (Ohio) us-east-2'). There is also a note about copying settings from an existing bucket. A red 'Create bucket' button is at the bottom.

Create a bucket - Provide general details

### 3. Public Access settings

You can choose public visibility. Let's uncheck the *Block all public access* option.

#### Bucket settings for Block Public Access

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

##### **Block all public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

###### **Block public access to buckets and objects granted through new access control lists (ACLs)**

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

###### **Block public access to buckets and objects granted through any access control lists (ACLs)**

S3 will ignore all ACLs that grant public access to buckets and objects.

###### **Block public access to buckets and objects granted through new public bucket or access point policies**

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

###### **Block public and cross-account access to buckets and objects through any public bucket or access point policies**

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.



#### Turning off block all public access might result in this bucket and the objects within becoming public

AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Create a bucket - make it public

### 4. Bucket Versioning and Encryption

- Bucket Versioning - Keep it disabled.
- Encryption - If enabled, it will encrypt the files being stored in the bucket.
- Object Lock - If enabled, it will prevent the files in the bucket from being deleted or modified.

### Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

#### Bucket Versioning

- Disable
- Enable

### Tags (0) - *optional*

Track storage cost or other criteria by tagging your bucket. [Learn more](#)

No tags associated with this bucket.

[Add tag](#)

### Default encryption

Automatically encrypt new objects stored in this bucket. [Learn more](#)

#### Server-side encryption

- Disable
- Enable

Create a bucket - provide additional details

In the snapshots above, we have created a public bucket. Let's see **how to upload files and folders to the bucket**, and configure additional settings.

### Upload File/Folders to the Bucket

From the **S3 dashboard**, click on the name of the bucket you have created in the step above.

The screenshot shows the 'Bucket overview' section of the Amazon S3 console. It displays the following details:

Region US East (Ohio) us-east-2	Amazon resource name (ARN) arn:aws:s3:::mtvbucket	Creation date November 25, 2020, 16:11 (UTC+05:30)	Access Objects can be public
------------------------------------	--	---	---------------------------------

Below the overview, there is a navigation bar with tabs: Objects (highlighted in orange), Properties, Permissions, Metrics, Management, and Access points. A red box highlights the 'Objects' tab.

A central upload area contains the text: "Drag and drop files and folders you want to upload here, or choose Upload." Below this is a search bar labeled "Find objects by prefix".

The "Objects (0)" section includes a toolbar with "Delete", "Actions", "Create folder", and a prominent "Upload" button (also highlighted with a red box). There is also a search bar for object prefixes.

The object listing table has columns: Name, Type, Last modified, Size, and Storage class. The table is currently empty, showing "No objects" and the message "You don't have any objects in this bucket." A "Upload" button is located at the bottom of this section.

Details of an existing bucket. Upload files/folders to this bucket.

In the snapshot above, it shows that the bucket is in the Region: US East (Ohio) us-east-2, and it has a unique Amazon resource name (ARN): arn:aws:s3:::mtvbucket. You can view more details of the bucket, in the tabs next to the bucket overview: **Objects, Properties, Permissions, Metrics, Management, and Access points**. Let's upload a sample file to the bucket:

1. Click on the **Upload** button to upload files and folders into the current bucket. In the snapshot below, we have uploaded a **Sample.txt** file.

The screenshot shows the 'Objects (1)' section of the Amazon S3 console. At the top, there are buttons for 'Delete', 'Actions ▾', 'Create folder', and 'Upload'. Below is a search bar with the placeholder 'Find objects by prefix'. A navigation bar with arrows and a refresh icon is at the top right. The main table has columns for Name, Type, Last modified, Size, and Storage class. One row is visible for 'Sample.txt', which is a 'txt' file last modified on November 25, 2020, at 16:51 (UTC+05:30), with a size of 2.0 KB and a storage class of Standard.

A sample file in the bucket

2. Click on the file name to view the file-specific details, as shown below.

The screenshot shows the details page for the 'Sample.txt' object. The top navigation bar shows 'Amazon S3 > mtvbucket > Sample.txt'. On the right, there is an 'Object actions ▾' button. Below the navigation, there are tabs for 'Details' (which is selected) and 'Versions'. The main area is titled 'Object overview' and contains two columns of key-value pairs. The left column includes 'Owner', 'AWS Region (US East (Ohio) us-east-2)', 'Last modified (November 25, 2020, 16:51 (UTC+05:30))', 'Size (2.0 KB)', 'Type (txt)', and 'Key (Sample.txt)'. The right column includes 'S3 URI (s3://mtvbucket/Sample.txt)', 'Amazon resource name (ARN) (arn:aws:s3:::mtvbucket/Sample.txt)', 'Entity tag (Etag) (19e4248fd5e3034c9b2d673d905725c0)', and 'Object URL (https://mtvbucket.s3.us-east-2.amazonaws.com/Sample.txt)'.

Details of an individual file (object)

## Details of an Existing Bucket

### 1. Properties

There are several properties that you can set for S3 buckets, such as:

- Bucket Versioning - Allows you to keep multiple versions of an object in the same bucket.
- Static website hosting - Mark if the bucket is used to host a website. S3 is a very cost-effective and cheap solution for serving up static web content.
- Requester pays - Make the requester pays for requests and data transfer costs.
- Server access logging - Log requests for access to your bucket.

## - Permissions

It shows who has access to the S3 bucket, and who has access to the data within the bucket. In the example snapshots above, the bucket is public, meaning anyone can access it. Here, we can write an access policy (in JSON format) to provide access to the objects stored in the bucket.

## 2. Metrics

View the metrics for usage, request, and data transfer activity within your bucket, such as, total bucket size, total number of objects, and storage class analysis.

## 3. Management

It allows you to create life cycle rules to help manage your objects. It includes rules such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time.

## 4. Access points

Here, you can create access endpoints for sharing the bucket at scale. Using an endpoint, you can perform all regular operations on the bucket.

## Creating PostgreSQL Database

According to AWS:

**Amazon RDS** is a relational database service that manages common database administration tasks, resizes automatically, and is cost-friendly.

Let's see how to create a PostgreSQL database, and view the details of an existing database.

## RDS Dashboard

Navigate to the **RDS dashboard**. It shows the database-resources summary, such as the count of database instances, the health of the database service, reserved instances, snapshots. You can also view the portion of the allocated storage. You can launch the **Create database** wizard from here.

The screenshot shows the Amazon RDS dashboard. On the left, there's a navigation pane with various options like Dashboard, Databases, Query Editor, etc. The main area is titled 'Resources' and shows usage statistics for the US East (Ohio) region. It lists DB Instances (0/40), DB Clusters (0/40), and other resources like Parameter groups, Option groups, Subnet groups, and Supported platforms (VPC). Below this is a section titled 'Create database' with a note about setting up a relational database in the cloud, a 'Restore from S3' button, and a prominent orange 'Create database' button. A note at the bottom says 'Note: your DB instances will launch in the US East (Ohio) region'.

RDS dashboard

## Create a PostgreSQL DB

If you haven't launched already, choose the **Databases** menu item on the left navigation pane, and click on the **Create Database** button.

The screenshot shows the 'Databases' dashboard under the 'Amazon RDS' service. The left sidebar has links for Dashboard, Databases (which is highlighted in orange), Performance Insights, Snapshots, etc. The main area has a search bar for 'Filter databases' and a table header with columns for DB identifier, Role, Engine, Region & AZ, Size, and Status. A note at the bottom says 'No instances found'. At the top right of the main area, there are buttons for 'Restore from S3' and a prominent orange 'Create database' button.

Amazon RDS service -> databases dashboard

### 1. Choose a database creation method

AWS provides two options to choose from:

- **Standard create** - You have set all of the configuration options, including ones for availability, security, backups, and maintenance.
- **Easy create** - You use the industry best-practice configurations. All configuration options, except the Encryption and VPC details,

can be changed after the database is created.

The steps below will show you the **Standard create** fields/options.

RDS > Create database

## Create database

**Choose a database creation method** [Info](#)

**Standard create**  
You set all of the configuration options, including ones for availability, security, backups, and maintenance.

**Easy create**  
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Choose a database creation method

## 2. Engine options

Select **PostgreSQL** option. It will pick up the latest stable release by default, though you can select a version of your choice as well.

**Engine options**

Engine type [Info](#)

<input type="radio"/> Amazon Aurora 	<input type="radio"/> MySQL 	<input type="radio"/> MariaDB 
<input checked="" type="radio"/> PostgreSQL 	<input type="radio"/> Oracle 	<input type="radio"/> Microsoft SQL Server 

Version

PostgreSQL 12.5-R1

Engine Option

## 3. Templates

Use either the **RDS Free Tier** or **Dev/Test** template. On free-tier resources, you can develop and test applications to gain hands-on experience with Amazon RDS.

The free tier will offer you 750 hrs of Amazon RDS in a Single-AZ db.t2.micro Instance, 20 GB of General Purpose Storage (SSD), and

20 GB for automated backup storage and any user-initiated DB Snapshots.

**Templates**  
Choose a sample template to meet your use case.

**Production**  
Use defaults for high availability and fast, consistent performance.

**Dev/Test**  
This instance is intended for development use outside of a production environment.

**Free tier**  
Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS.  
[Info](#)

## Templates

### 4. Settings

Provide a *DB instance identifier*, such as *postgreSQL-test*, and master credentials (username and a password). Take note of this password, as it is useful for future steps. You will be able to find this password and change it later in the console.

Alternatively, you can auto-generate the password. In this case, AWS will show you the password once you create the database successfully.

**Settings**

**DB instance identifier** [Info](#)  
Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens (1 to 15 for SQL Server). First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

**Credentials Settings**

**Master username** [Info](#)  
Type a login ID for the master user of your DB instance.

1 to 16 alphanumeric characters. First character must be a letter  
 **Auto generate a password**  
Amazon RDS can generate a password for you, or you can specify your own password

**Master password** [Info](#)

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), '(single quote)', "(double quote)" and @ (at sign).

**Confirm password** [Info](#)

## Settings

### 5. DB instance class

The options here present the options for processing power and memory requirements. Since we have selected the Free tier option above, the only available option is db.t2.micro, which has 1 vCPU, and 1 GiB RAM.

### DB instance class

**DB instance class** [Info](#)

Choose a DB instance class that meets your processing power and memory requirements. The DB instance class options below are limited to those supported by the engine you selected above.

Standard classes (includes m classes)

Memory optimized classes (includes r and x classes)

Burstable classes (includes t classes)

db.t2.micro

1 vCPUs    1 GiB RAM    Not EBS Optimized

[New instance classes are available for specific engine versions.](#) [Info](#)

Include previous generation classes

### DB instance class

## 6. Storage and Availability & durability

Choose the default values for both these sections. It will offer you 20 GiB SSD storage, expandable up to 1000 GiB, by default. For *Availability & durability* section, it will not offer us to have a Multi-AZ deployment.

### Storage

**Storage type** [Info](#)

General Purpose (SSD) ▾

**Allocated storage**

20 GiB

(Minimum: 20 GiB, Maximum: 16,384 GiB) Higher allocated storage [may improve](#) IOPS performance.

**Storage autoscaling** [Info](#)

Provides dynamic scaling support for your database's storage based on your application's needs.

**Enable storage autoscaling**  
Enabling this feature will allow the storage to increase once the specified threshold is exceeded.

**Maximum storage threshold** [Info](#)

Charges will apply when your database autoscales to the specified threshold

1000 GiB

Minimum: 21 GiB, Maximum: 16,384 GiB

### Availability & durability

**Multi-AZ deployment** [Info](#)

- Create a standby instance (recommended for production usage)  
Creates a standby in a different Availability Zone (AZ) to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups.
- Do not create a standby instance

## Storage and Availability & durability

## 7. Connectivity

Choose/ensure the following values:

Field	Value
VPC	Default VPC
Subnet group	default
Public access	YES Once you get familiar, choose NO next time. You will need additional configuration to do so.
VPC security group	Either choose default or create a new one
Availability Zone	No preference
Database port	5432 (default)

**Leave the values default for the Database authentication section.**

## Connectivity

**Virtual private cloud (VPC) [Info](#)**  
VPC that defines the virtual networking environment for this DB instance.

Default VPC (vpc-cb298db6) ▾

Only VPCs with a corresponding DB subnet group are listed.

ⓘ After a database is created, you can't change the VPC selection.

**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 access [Info](#)**

Yes  
Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the database.

No  
RDS will not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.

**VPC security group**  
Choose a VPC security group to allow access to your database. Ensure that the security group rules allow the appropriate incoming traffic.

Choose existing  
Choose existing VPC security groups

Create new  
Create new VPC security group

**Existing VPC security groups**

Choose VPC security groups ▾

default X

**Availability Zone [Info](#)**

No preference ▾

**▼ Additional configuration**

**Database port [Info](#)**  
TCP/IP port that the database will use for application connections.

5432

## Connectivity

### 8. Additional configuration

- Provide the database name. If you do not specify a database name, Amazon RDS will not create a database.
- In the *Backup* section and select *1 day*, since this is for demonstration purposes.
- Leave the default values for the rest and click on the **Create database** button on the bottom right.

## ▼ Additional configuration

Database options, backup enabled, backtrack disabled, Performance Insights enabled, Enhanced Monitoring disabled, maintenance, CloudWatch Logs, delete protection disabled

### Database options

Initial database name [Info](#)

myFirstDatabase

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

DB parameter group [Info](#)

default.postgres12



Option group [Info](#)

default:postgres-12



### Backup

Creates a point-in-time snapshot of your database

**Enable automatic backups**

Creates a point-in-time snapshot of your database

Backup retention period [Info](#)

Choose the number of days that RDS should retain automatic backups for this instance.

1 day



Backup window [Info](#)

Select the period for which you want automated backups of the database to be created by Amazon RDS.

Select window

No preference

Copy tags to snapshots

Performance Insights [Info](#)

Enable Performance Insights

Retention period [Info](#)

Default (7 days)



Master key [Info](#)

(default) aws/rds



Account

644752792305

KMS key ID

alias/aws/rds

⚠ You can't change the KMS key after enabling Performance Insights.

## Monitoring

### Enable Enhanced monitoring

Enabling Enhanced monitoring metrics are useful when you want to see how different processes or threads use the CPU

## 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

ⓘ Ensure that general, slow query, and audit logs are turned on. Error logs are enabled by default. [Learn more](#)

## Maintenance

Auto minor version upgrade [Info](#)

### Enable auto minor version upgrade

Enabling auto minor version upgrade will automatically upgrade to new minor versions as they are released. The automatic upgrades occur during the maintenance window for the database.

Maintenance window [Info](#)

Select the period you want pending modifications or maintenance applied to the database by Amazon RDS.

Select window

No preference

## Deletion protection

### Enable deletion protection

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

## Additional Information

## 9. Success

You should land on a confirmation page. It will take a few minutes to launch the database. Wait a few minutes for the status to change to **Available**.

The screenshot shows the 'Create database' page in the Amazon RDS console. On the left, there's a sidebar with various navigation links like Dashboard, Databases, Performance Insights, etc. The main area has a green header bar with the text 'Your DB instance is being created.' and a note: 'Note: Your instance may take a few minutes to launch.' Below this, there are sections for 'Connecting to your DB instance' and 'Usage charges'. At the bottom right, there are buttons for 'All DB instances' and 'View DB Instance details'.

The screenshot shows the 'Databases' page in the Amazon RDS console. A green header bar indicates 'Successfully created database database-1'. The main area displays a table of databases, with one row highlighted for 'database-1'. The table columns include DB identifier, Instance, Engine, Region & AZ, Size, and Status (which is 'Available').

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

For each database in the list above, you can see the Region and availability zone it's running in, the size, and the status that it's up and running. You can also see the percentage utilization of the underlying CPU.

## Lesson Review

In this lesson, we covered:

- An Introduction to cloud computing using AWS
- How to sign into the AWS Gateway from the Udacity classroom
- Creating an IAM role and user
- Creating a security group
- Launching a Redshift Cluster
- Creating an S3 bucket
- Creating a PostgreSQL Database

As you are working through the next lesson, remember to use this lesson as a reference for instructions on working with these AWS components.