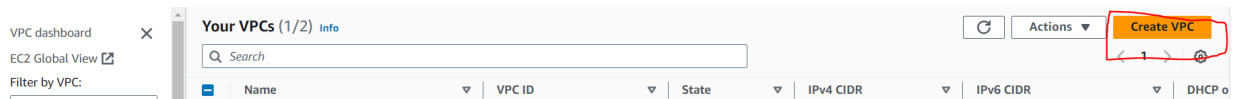


Step 1: Create a VPC and Subnets as well as routing and security groups

- Go to “Your VPCs” from the VPC service on the AWS management console and click on the orange “Create VPC” button.



- Only create a vpc here and give it a name. You are free to make your own name or follow along with the one put here
- Give it a 192.168.0.0/16 CIDR block and leave everything else as default. Click create.

Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create [Info](#)

Create only the VPC resource or create VPC, subnets, etc.

☒ VPC only

☐ VPC, subnets, etc.

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

Demo VPC

IPv4 CIDR block [Info](#)

☒ IPv4 CIDR manual input

☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

192.168.0.0/16

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block

☐ IPAM-allocated IPv6 CIDR block

☐ Amazon-provided IPv6 CIDR block

☐ IPv6 CIDR owned by me

Tenancy [Info](#)

Default

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Q Name

X

Value - *optional*

Q Demo VPC

X

Remove

Add new tag

You can add 49 more tags.

Cancel

Create VPC

- To create your subnets go to Subnets on the left hand side of the VPC service and click on it
- Add your VPC ID to where it asks

Create subnet [Info](#)

VPC

VPC ID
Create subnets in this VPC.

vpc-03bd2b389d2a4d45e (Demo VPC) ▼

Associated VPC CIDRs

IPv4 CIDRs

192.168.0.0/16

- Assign it a name letting you know what it is your first public subnet
- Put it in any availability zone and give it a CIDR of 192.168.1.0/24

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

Public Subnet

The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US West (Oregon) / us-west-2a ▼

IPv4 CIDR block [Info](#)

Q 192.168.1.0/24 X

Tags - optional

Key

Q Name X

Value - optional

Q Public Subnet X

Remove

Add new tag

You can add 49 more tags.

Remove

Add new subnet

Cancel

Create subnet

- Add a second subnet and name it Private Subnet 1 or something to let you know it is your first private subnet
- Put it in the same availability zone as the first subnet you made and give it a CIDR of 192.168.2.0/24

Subnet 2 of 2

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

Private Subnet 1

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US West (Oregon) / us-west-2a

IPv4 CIDR block [Info](#)

192.168.2.0/24

▼ Tags - optional

Key

Value - optional

Name

Private Subnet 1

Remove

Add new tag

You can add 49 more tags.

Remove

Add new subnet

- Add a third subnet and assign a name letting you know it is the second private subnet you will be making
- Put it in the same availability zone as your first public subnet and give it a CIDR of 192.168.3.0/24

Subnet 3 of 3

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 CIDR block [Info](#)

▼ Tags - *optional*

Key

Value - *optional*

You can add 49 more tags.

- Add a fourth and final subnet and give it a name letting you know it is the third private subnet
- Put it in a different availability zone from the rest of your subnets and give it a CIDR of 192.168.4.0/24

Subnet 4 of 4

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 CIDR block [Info](#)

▼ Tags - *optional*

Key

Value - *optional*

Remove

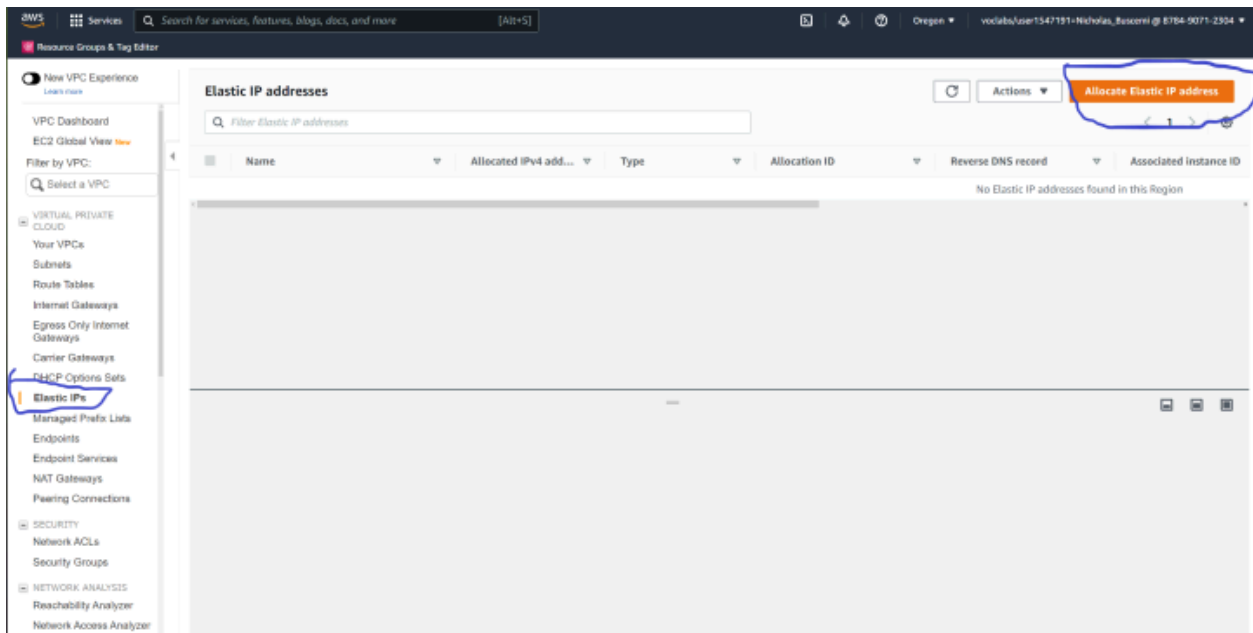
Add new tag

You can add 49 more tags.

Remove

Add new subnet

- Set up for route tables
- Allocate an Elastic IP address by going to Elastic IPs on the left hand side and click “Allocate Elastic IP address”



- Everything should be good as default but make sure that you are in the same region you have been creating everything in and then press “Allocate”. You can also add a name tag if you wish but it isn’t necessary



- Now create an internet gateway and attach it to the VPC by going to Internet Gateways on the left hand side and clicking “Create Internet Gateway”

The screenshot shows the AWS Management Console interface. On the left sidebar, under 'VIRTUAL PRIVATE CLOUD', the 'Internet Gateways' link is selected. The main panel displays 'Internet gateways (1/1)'. At the top right of this panel, the 'Create Internet gateway' button is circled in blue. Below the header, there is a table with one entry:

Name	Internet gateway ID	State	VPC ID	Owner
-	igw-07d627fd599b16b01	Attached	vpc-02c1bd9878c0e1c78	878490712304

Below the table, the details for the selected gateway 'igw-07d627fd599b16b01' are shown, including its ID, state (Attached), VPC ID, and owner.

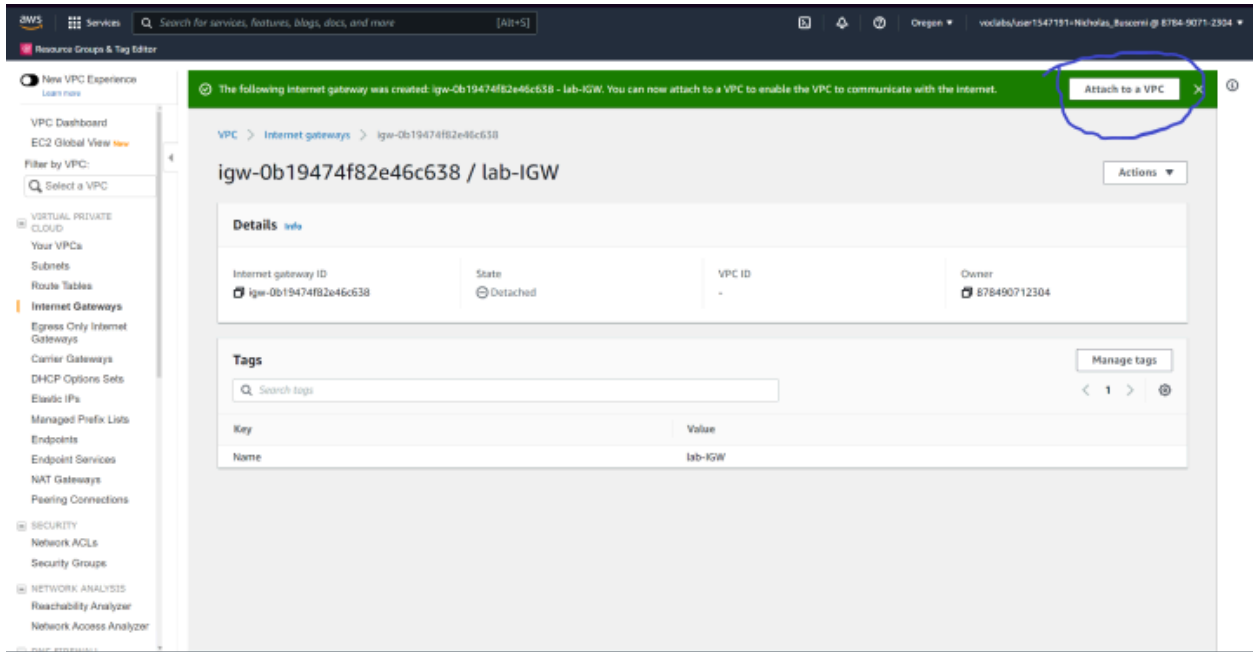
- Name it something similar to what is below and then click “Create Internet Gateway”

The screenshot shows the 'Create internet gateway' wizard in the AWS Management Console. The breadcrumb navigation at the top reads 'VPC > Internet gateways > Create internet gateway'. The main heading is 'Create internet gateway'. Below this, there is a section for 'Internet gateway settings' with a 'Name tag' field containing the value 'lab-IGW'. Below that, there is a 'Tags - optional' section with a table of tags:

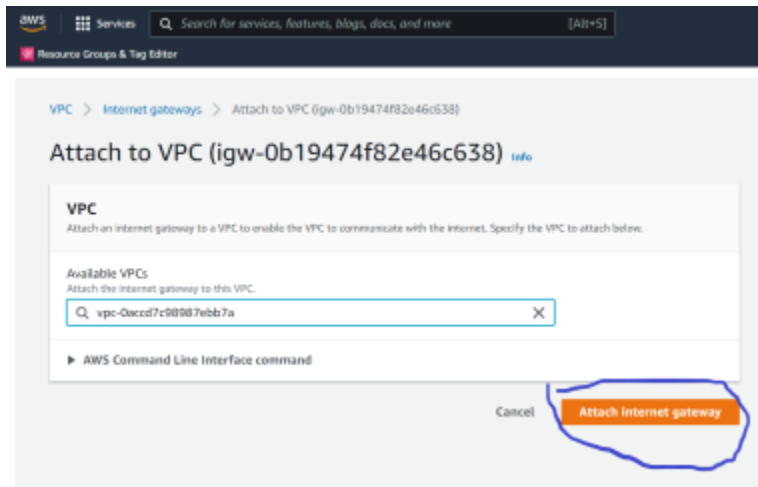
Key	Value - optional
Name	lab-IGW

At the bottom of the wizard, there are 'Cancel' and 'Create internet gateway' buttons. The 'Create internet gateway' button is circled in blue.

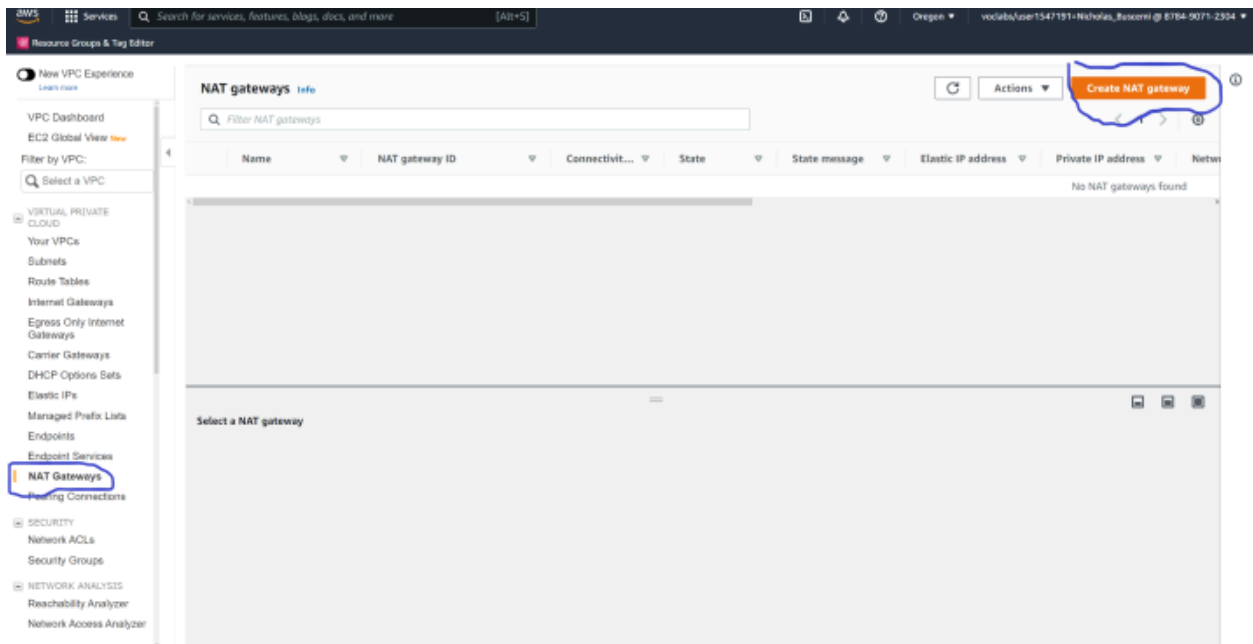
- Once it is created attach it to your VPC by clicking “Attach to a VPC” on the top of the screen



- Click the drop down and select your vpc that you made



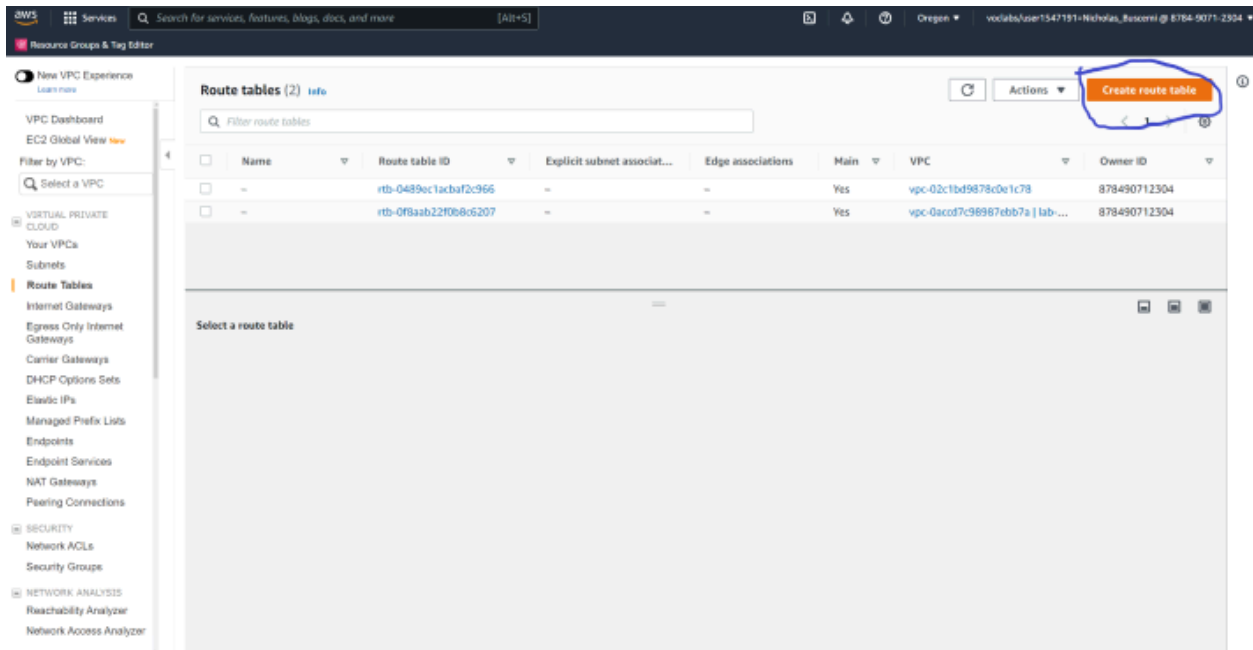
- Create a NAT Gateway by clicking on Nat Gateways on the left hand side and then clicking “Create NAT Gateway”



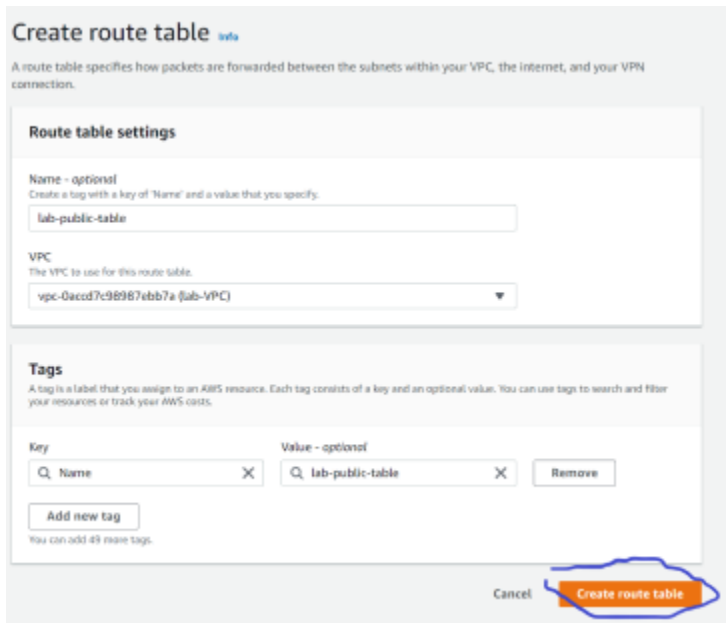
- Give it a name similar to the one below and assign it to a **public subnet**
- Click the drop down for Elastic IPs and click the one you created previously
- Click “Create NAT gateway”



- Create Route Tables by first heading to “Route Tables” on the left hand side
- Click “Create route table”



- Give it a name letting you know this is the public route table for your lab
- Assign your VPC to it and click “Create route table”



- Make a second route table naming it something to let you know that this is the private route table for your lab and assign your VPC to it

Create route table [info](#)

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.
lab-private-table

VPC
The VPC to use for this route table.
vpc-0accd7c98987ebb7a (lab-VPC)

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key: Name Value: lab-private-table Remove

Add new tag
You can add 49 more tags.

Cancel Create route table

- Now associate your subnets with their respective route table
- Click on the public route table and click on “Subnet association” next to “Details”

Route tables (1/4) [info](#)

Filter route tables

Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
-	rtb-0489cc1acba2c966	-	-	Yes	vpc-02c1bd9878c0e1c78	878490712304
lab-public-table	rtb-096cb259306549323	-	-	No	vpc-0accd7c98987ebb7a lab-...	878490712304
lab-private-table	rtb-0f53cf17d08253bb	-	-	No	vpc-0accd7c98987ebb7a lab-...	878490712304
-	rtb-0f8aab22f0b8c5207	-	-	Yes	vpc-0accd7c98987ebb7a lab-...	878490712304

rtb-096cb259306549323 / lab-public-table

Details Routes Subnet associations Edge associations Route propagation Tags

You can now check network connectivity with Reachability Analyzer [Run Reachability Analyzer](#)

Details

Route table ID rtb-096cb259306549323	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-0accd7c98987ebb7a lab-VPC	Owner ID 878490712304		

- Click on “Edit subnet associations”

Route tables (1/4)

Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
lab-public-table	rtb-0489ec1acbf2c966	-	-	Yes	vpc-02c1bd9878c0e1c78	878490712304
lab-private-table	rtb-096cb259306549323	-	-	No	vpc-0accd7c98987ebb7a lab...	878490712304
lab-private-table	rtb-0f53cf137d08253bb	-	-	No	vpc-0accd7c98987ebb7a lab...	878490712304
-	rtb-0f8aab22f0b0c5207	-	-	Yes	vpc-0accd7c98987ebb7a lab...	878490712304

Explicit subnet associations (0)

Find subnet association

Subnet ID IPv4 CIDR IPv6 CIDR

No subnet associations
You do not have any subnet associations.

Subnets without explicit associations (4)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Find subnet association

Subnet ID IPv4 CIDR IPv6 CIDR

- Click on your public subnet and then click “Save associations”

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/4)

Filter subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
Private Subnet 3	subnet-092c5783f28705ad7	192.168.4.0/24	-	Main (rtb-010a67db84e50ef4)
<input checked="" type="checkbox"/> Public Subnet	subnet-06bc254b8826ccb04	192.168.1.0/24	-	Main (rtb-010a67db84e50ef4)
Private Subnet 1	subnet-0b2f703b31b1dbf78	192.168.2.0/24	-	Main (rtb-010a67db84e50ef4)
Private Subnet 2	subnet-00fbb6995bc7ecbc6	192.168.3.0/24	-	Main (rtb-010a67db84e50ef4)

Selected subnets

subnet-06bc254b8826ccb04 / Public Subnet X

Cancel Save associations

- Now add a route to our public route table to get access to the internet gateway
- Click on “Routes” next to “Details” and click “Edit routes”

New VPC Experience
[Learn more](#)

VPC Dashboard
EC2 Global View New

Filter by VPC:

VIRTUAL PRIVATE CLOUD

Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
Carrier Gateways
DHCP Option Sets
Elastic IPs
Managed Prefix Lists
Endpoints
Endpoint Services
NAT Gateways
Peering Connections

SECURITY

Network ACLs
Security Groups

NETWORK ANALYSIS

Reachability Analyzer
Network Access Analyzer

DNS FIREWALL

Rule Groups
Domain Lists

NETWORK FIREWALL

Firewalls
Firewall Policies
Network Firewall Rule Groups

VIRTUAL PRIVATE NETWORK (VPN)

Actions

Create route table

Route tables (1/4) Info

☐

-

rtb-010a67db84e50ef44

-

-

Yes

☒

lab-public-table

rtb-07fadf542dba89a17

subnet-06bc254b8826c...

-

No

☐

lab-private-table

rtb-079223b43d56c7bf8

-

-

No

☐

-

rtb-0dffa298cf2ccb9c3

-

-

Yes

rtb-07fadf542dba89a17 / lab-public-table

Details

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (1)

Both

<

1

>

Destination

Target

Status

Propagated

192.168.0.0/16

local

Active

No

Edit routes

- Add a new route having a destination of anywhere and a target of your internet gateway and click “Save changes”

VPC > Route tables > rtb-07fadf542dba89a17 > Edit routes

Edit routes

Edit routes

Destination	Target	Status
192.168.0.0/16	local	Active
Propagated		
No		

Edit routes

Destination	Target	Status
0.0.0.0/0	igw-0a2e406efd9302f16	-
Propagated		
No		

Remove

Add route

Cancel

Preview

Save changes

- Do the same thing for your private route table by clicking on it and going to its subnet associations and editing them

The screenshot shows the AWS Management Console interface. On the left is the navigation menu with categories like VPC, SECURITY, and NETWORK ANALYSIS. The main content area is titled 'Route tables (1/4) info'. A table lists four route tables: a main table, 'lab-public-table', 'lab-private-table' (which is selected), and another main table. Below the table, the 'Subnet associations' tab for 'rtb-0f53cff17d08253bb / lab-private-table' is active. It shows 'Explicit subnet associations (0)' and a button to 'Edit subnet associations', which is circled in blue. Below that, it shows 'Subnets without explicit associations (2)'.

- Click on all three of your private subnets and save the associations

Edit subnet associations

Change which subnets are associated with this route table.

The 'Edit subnet associations' dialog box is shown. It has a search bar and a table of 'Available subnets (3/4)'. The table has columns for Name, Subnet ID, IPv4 CIDR, IPv6 CIDR, and Route table ID. Three subnets are selected: 'Private Subnet 3', 'Private Subnet 1', and 'Private Subnet 2'. Below the table, the 'Selected subnets' section displays three tags: 'subnet-00fbb6995bc7ecbc6 / Private Subnet 2', 'subnet-0b2f703b31b1dbf78 / Private Subnet 1', and 'subnet-092c5783f28705ad7 / Private Subnet 3'. At the bottom right are 'Cancel' and 'Save associations' buttons.

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/> Private Subnet 3	subnet-092c5783f28705ad7	192.168.4.0/24	-	Main (rtb-010a67db84e50ef44)
<input type="checkbox"/> Public Subnet	subnet-06bc254b8826ccb04	192.168.1.0/24	-	rtb-07fadf542dba89a17 / lab-public table
<input checked="" type="checkbox"/> Private Subnet 1	subnet-0b2f703b31b1dbf78	192.168.2.0/24	-	Main (rtb-010a67db84e50ef44)
<input checked="" type="checkbox"/> Private Subnet 2	subnet-00fbb6995bc7ecbc6	192.168.3.0/24	-	Main (rtb-010a67db84e50ef44)

Selected subnets

subnet-00fbb6995bc7ecbc6 / Private Subnet 2 subnet-0b2f703b31b1dbf78 / Private Subnet 1 subnet-092c5783f28705ad7 / Private Subnet 3

- Go to edit the routes of the private table

New VPC Experience
[Learn more](#)

VPC Dashboard

EC2 Global View New

Filter by VPC:

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

Carrier Gateways

DHCP Option Sets

Elastic IPs

Managed Prefix Lists

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

SECURITY

Network ACLs

Security Groups

NETWORK ANALYSIS

Reachability Analyzer

Network Access Analyzer

DNS FIREWALL

Rule Groups

Domain Lists

NETWORK FIREWALL

Firewalls

Firewall Policies

Network Firewall Rule Groups

VIRTUAL PRIVATE NETWORK (VPN)

You have successfully updated subnet associations for rtb-079223b43d56c7bf8 / lab-private-table.

Route tables (1/4) [Info](#)

[Create route table](#)

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associat...	Edge associations	Main
<input type="checkbox"/>	-	rtb-010a67db84e50ef44	-	-	Yes
<input type="checkbox"/>	lab-public-table	rtb-07fadf542dba89a17	subnet-06bc254b8826c...	-	No
<input checked="" type="checkbox"/>	lab-private-table	rtb-079223b43d56c7bf8	3 subnets	-	No
<input type="checkbox"/>	-	rtb-0dffa298cf2ccb9c3	-	-	Yes

rtb-079223b43d56c7bf8 / lab-private-table

Details

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (1)

Both

[Edit routes](#)

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No

- Add a route to the private table that has a destination of anywhere and a target of your Nat gateway that you made earlier

Edit routes

Edit routes

Destination

192.168.0.0/16

Target

local

Status

Active

Propagated

No

Edit routes

Destination

0.0.0.0/0

Target

nat-0dc88ba1b12f5d4bf

Status

-

Propagated

No

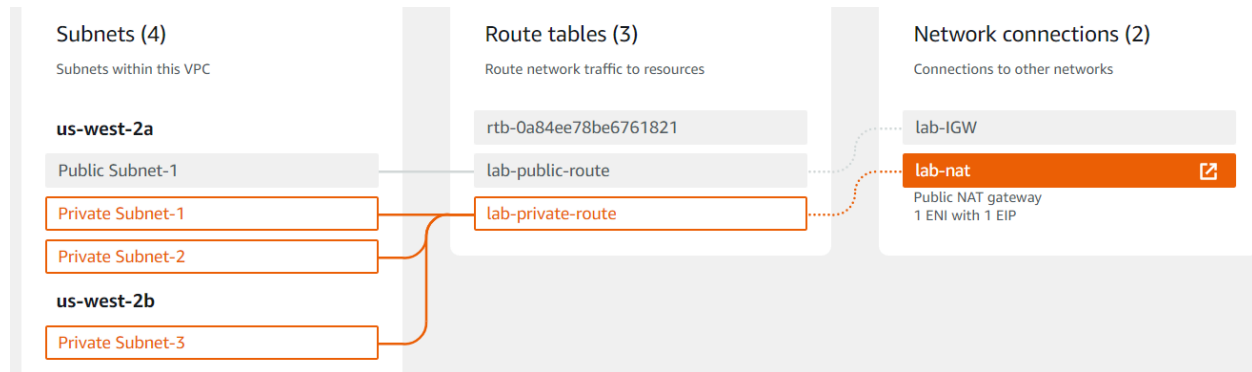
Remove

Add route

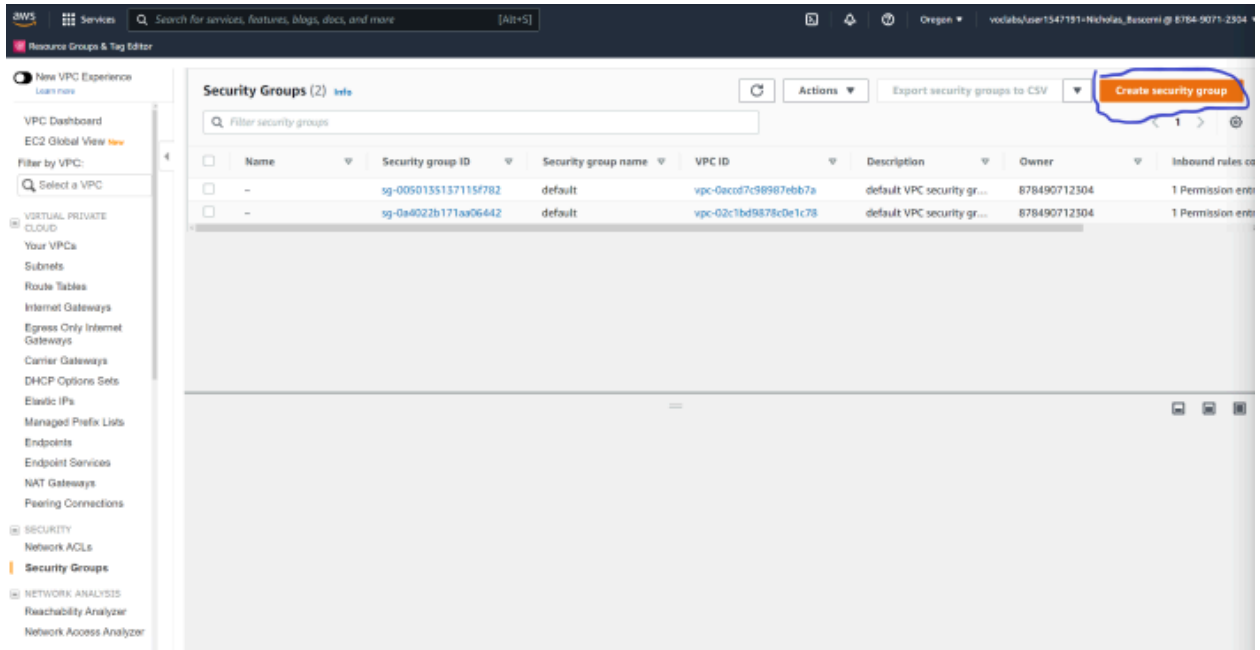
Cancel

Preview

Save changes



- Now to create our security groups (One for our bastion host, web server, app server, and our database) we will head to Security Groups on the left and click “Create security group”



- Give it a name and description letting you know it is for a bastion host
- Assign your VPC to it
- Give it three inbound rules, one for SSH using your IP and one for HTTP using 0.0.0.0/0 as well as https using 0.0.0.0/0.

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)



Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
HTTP ▾	TCP	80	Anywh... ▾ <input type="text" value="0.0.0.0/0"/>	<input type="text"/>	<div>Delete</div>
HTTPS ▾	TCP	443	Anywh... ▾ <input type="text" value="0.0.0.0/0"/>	<input type="text"/>	<div>Delete</div>
SSH ▾	TCP	22	Anywh... ▾ <input type="text" value="0.0.0.0/0"/>	<input type="text"/>	<div>Delete</div>
<div>Add rule</div>					

- Create another security group
- Give it a name and description letting you know it is for a Web server
- Assign your VPC to it
- Give it the same inbound rules as the Bastion Host security group

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
HTTP ▼	TCP	80	Anywh... <input type="text" value="0.0.0.0/0"/>	<input type="text"/>	<input type="button" value="Delete"/>
HTTPS ▼	TCP	443	Anywh... <input type="text" value="0.0.0.0/0"/>	<input type="text"/>	<input type="button" value="Delete"/>
SSH ▼	TCP	22	Anywh... <input type="text" value="0.0.0.0/0"/>	<input type="text"/>	<input type="button" value="Delete"/>
<input type="button" value="Add rule"/>					

- Create another security group
- Give it a name and description letting you know it is for an **app server**
- Assign your VPC to it
- Give it an inbound rule for **All ICMP -IPv4** with a **source of your web server SG** and another inbound rule for **SSH** with a **source of your bastion host SG**

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)



Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
All ICMP - IPv4 ▼	ICMP	All	Custom ▼ <input type="text" value="Q"/>	<input type="text"/>	<div>Delete</div>
			<div>sg-094827ea3d4c27f60 ✕</div>		
SSH ▼	TCP	22	Custom ▼ <input type="text" value="Q"/>	<input type="text"/>	<div>Delete</div>
			<div>sg-041812008930fcc7b ✕</div>		
<div>Add rule</div>					

- Create one final security group
- Give it a name and description letting you know it is for a database server
- Assign your VPC to it
- Give it two inbound rules **both for MYSQL/Aurora** and give one of them a **source of your app server SG** and the other one a **source of your bastion host SG**

VPC > Security Groups > Create security group

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
MySQL/Aurora ▼	TCP	3306	Custom ▼ <input type="text" value="Q"/>	<input type="text"/>	Delete
			sg-0782f81911c052438 ✕		
MySQL/Aurora ▼	TCP	3306	Custom ▼ <input type="text" value="Q"/>	<input type="text"/>	Delete
			sg-094827ea3d4c27f60 ✕		

[Add rule](#)

- Go back to your **bastion host inbound rules** and add one more for MySQL/Aurora and a source of your **database SG**

VPC > Security Groups > sg-0614859e85cf4602a - Bastion Host > Edit inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [Info](#)

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
-	MySQL/Aurora ▼	TCP	3306	Custom ▼ <input type="text" value="Q sg-0fe8bdc26cacfb869 ✕"/>	<input type="text"/>	Delete
				sg-0fe8bdc26cacfb869 ✕		

[Add rule](#)

Cancel [Preview changes](#) [Save rules](#)

- Go back to your web server inbound rules and add one more for All ICMP - IPv4 and a source of your app server SG.

- Go back to your app server inbound rules and add one more for MYSQL/Aurora and a source of your database SG and then an HTTP and HTTPS rule both with a source of 0.0.0.0/0

VPC > Security Groups > sg-05fdf47f3de34b823 > Edit inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
sgr-0c6a4ff7bd7e2c0d	All ICMP - IPv4	ICMP	All	Custom	<input type="text"/> <input type="button" value="Delete"/>
sgr-0596ab4407ab61318	SSH	TCP	22	Custom	<input type="text"/> <input type="button" value="Delete"/>
-	MYSQL/Aurora	TCP	3306	Custom	<input type="text"/> <input type="button" value="Delete"/>

Q

CIDR blocks

Security Groups

DatabaseServerGroup | [sg-0fe8bdc26cacfb869](#)

Prefix lists

Q sg-0fe8bdc26cacfb865 X

sg-0fe8bdc26cacfb869 X

Step 2: Create Servers

- Create Bastion Host

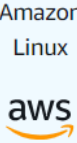
Name and tags [Info](#)


Name


[Add additional tags](#)


- Select Amazon Linux 2 AMI


Quick Start
















[Browse more AMIs](#)
Including AMIs from
AWS, Marketplace and
the Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type Free tier eligible
ami-0895022f3dac85884 (64-bit (x86)) / ami-09ebdd80c5c138f65 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2 Kernel 5.10 AMI 2.0.20240223.0 x86_64 HVM gp2

Architecture

64-bit (x86) ▼

AMI ID

ami-0895022f3dac85884

Verified provider

- Select t2.micro

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0116 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand RHEL base pricing: 0.0716 USD per Hour

☐ All generations

[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)


- Select the key pair

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

vockey ▼

 [Create new key pair](#)

- Put in your VPC and Public Subnet, enable auto assign public IP and Select an existing group and select your Bastion Host SG.

VPC - *required* | [Info](#)

vpc-064d8b2be3d4d8d9d (Demo-vpc)
192.168.0.0/16



Subnet | [Info](#)

subnet-0f1d65ae74aee11cd Public Subnet-1
VPC: vpc-064d8b2be3d4d8d9d Owner: 905418371971
Availability Zone: us-west-2a IP addresses available: 250 CIDR: 192.168.1.0/24



[Create new subnet](#)

Auto-assign public IP | [Info](#)

Enable



Firewall (security groups) | [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group

☒ Select existing security group

Common security groups [Info](#)

Select security groups



Bastion Host sg-0614859e85cf4602a ✕
VPC: vpc-064d8b2be3d4d8d9d



[Compare security group rules](#)

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

- Storage leaves default.

Availability Zone: us-west-2a IP addresses available: 250 CIDR: 192.168.1.0/24

Auto-assign public IP [Info](#)

Enable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group ☒ Select existing security group

Common security groups [Info](#)

Select security groups

Bastion Host sg-0614859e85cf4602a X
VPC: vpc-064d8b2be3d4d8d9d

[Compare security group rules](#)

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

► Configure storage [Info](#) [Advanced](#)

► Advanced details [Info](#)

Number of instances [Info](#)

1

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI...[read more](#)
ami-0895022f3dac85884

Virtual server type (instance type)

t2.micro

Firewall (security group)

Bastion Host

Storage (volumes)

1 volume(s) - 8 GiB

[Free tier](#): In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which

Cancel **Launch instance** [Review commands](#)

- Follow the same steps to create the Web Server
- Follow along like previously and change your network, subnet, and enable auto assign public ip

▼ **Network settings** [Info](#) [Edit](#)

Network [Info](#)

vpc-064d8b2be3d4d8d9d | Demo-vpc

Subnet [Info](#)

subnet-0f1d65ae74aee11cd | Public Subnet-1

Auto-assign public IP [Info](#)

Enable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group ☒ Select existing security group

Common security groups [Info](#)

Select security groups

Web-Server sg-0ec7084d99503b509 X
VPC: vpc-064d8b2be3d4d8d9d

[Compare security group rules](#)

Security groups that you add or remove here will be added to or removed from all your network interfaces.

- Storage leave default

- Then go to user data and type this into it to set up the web server

```
#!/bin/bash
sudo yum update -y
sudo amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
sudo yum install -y httpd
sudo systemctl start httpd
sudo systemctl enable httpd
```

User data - optional [Info](#)

Upload a file with your user data or enter it in the field.

 Choose file

```
#!/bin/bash
sudo yum update -y
sudo amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
Sudo yum install -y httpd
sudo systemctl start httpd
sudo systemctl enable httpd
```

☐ User data has already been base64 encoded

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI...[read more](#)
ami-0895022f3dac85884

Virtual server type (instance type)


t2.micro

Firewall (security group)

Web-Server

Storage (volumes)

1 volume(s) - 8 GiB

 **Free tier:** In your first year
includes 750 hours of t2.micro (or
t3.micro in the Regions in which

Cancel

Launch instance

[Review commands](#)

- Creating an App server
- Put in your VPC and then choose **Private Subnet 1** for the subnet and leave auto assign public ip disabled

VPC - required [Info](#)

vpc-064d8b2be3d4d8d9d (Demo-vpc)
192.168.0.0/16



Subnet [Info](#)

subnet-036ac2520e5731b3f **Private Subnet-1**
VPC: vpc-064d8b2be3d4d8d9d Owner: 905418371971
Availability Zone: us-west-2a IP addresses available: 251 CIDR: 192.168.2.0/24



[Create new subnet](#)

Auto-assign public IP [Info](#)

Disable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group

☒ Select existing security group

Common security groups [Info](#)

Select security groups



[Compare security group rules](#)

App Server sg-05fdf47f3de34b823 X
VPC: vpc-064d8b2be3d4d8d9d

Security groups that you add or remove here will be added to or removed from all your network interfaces.

- Then go into Advanced Detail section add the below script in user data column

```
#!/bin/bash
sudo yum update -y
sudo yum install -y mariadb-server
sudo service mariadb start
```

Note:

To check version of mariadb use **mysql -v**

Step 3: Create a Database

- From the management console search RDS.
- In left pane, find **DB subnet group**. Create a DB Subnet group.

Amazon RDS Subnet groups

Subnet groups (0)

Filter by subnet group

Name	Description	Status	VPC
No db subnet groups You don't have any db subnet groups.			

Create DB subnet group

- Give it a name and description letting you know what it is and then assign your VPC to it
- Put in the availability zones you used for your subnets
- Select subnets 3 and 4
- Click create

Amazon RDS

Dashboard
Databases
Query Editor
Performance insights
Snapshots
Automated backups
Reserved instances
Proxies

Subnet groups
Parameter groups
Option groups
Custom engine versions

Events
Event subscriptions

Recommendations
Certificate update

RDS > Subnet groups > Create DB subnet group

Create DB subnet group

To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.

Subnet group details

Name

You won't be able to modify the name after your subnet group has been created.

Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

Description

VPC

Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.

Add subnets

Availability Zones

Choose the Availability Zones that include the subnets you want to add.

us-west-2a
us-west-2b

Subnets

Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.

subnet-092c5783f28705ad7 (192.168.4.0/24)
subnet-00fbb6995bc7ecbc6 (192.168.3.0/24)

Subnets selected (2)

Availability zone	Subnet ID	CIDR block
us-west-2a	subnet-00fbb6995bc7ecbc6	192.168.3.0/24
us-west-2b	subnet-092c5783f28705ad7	192.168.4.0/24

- Go to Databases on the left hand side and click on “Create Database”

Services

Search for services, features, blogs, docs, and more

[Alt+=]

Oregon

ec2:lab/user1547191-Nicholas_Bocenzi @ 8/24/2021 2:04

Resource Groups & Tag Editor

Amazon RDS

Dashboard

Databases

Query Editor

Performance insights

Snapshots

Automated backups

Reserved instances

Proxies

Subnet groups

Parameter groups

Option groups

Custom engine versions

Events

Event subscriptions

Recommendations

Certificate update

Successfully created lab-DB-subnet-group. [View subnet group](#)

RDS > Databases

Databases

Group resources

Modify

Actions

Restore from S3

Create database

Filter by databases

< 1 >

DB identifier

Role

Engine

Region & AZ

Size

Status

CPU

Current activity

Maintenance

No instances found

- Click on Standard create and MariaDB for the engine type

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.

Engine options

Engine type [Info](#)

☐ Amazon Aurora



☐ MySQL



☒ **MariaDB**



☐ PostgreSQL



☐ Oracle

ORACLE®

☐ Microsoft SQL Server

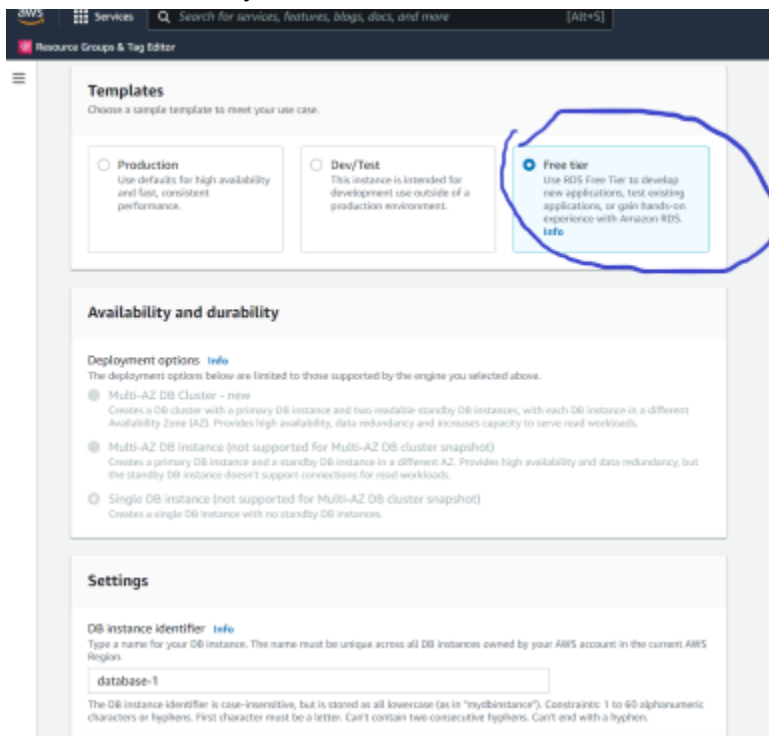


Version

MariaDB 10.6.7



- Make sure you click on Free tier here



The screenshot shows the AWS Management Console interface for creating a new Amazon RDS instance. The 'Templates' section is active, showing three options: 'Production', 'Dev/Test', and 'Free tier'. The 'Free tier' option is selected and highlighted with a blue circle. Below this, the 'Availability and durability' section shows 'Deployment options' with three radio buttons: 'Multi-AZ DB Cluster - new', 'Multi-AZ DB instance (not supported for Multi-AZ DB cluster snapshot)', and 'Single DB instance (not supported for Multi-AZ DB cluster snapshot)'. The 'Settings' section is partially visible, showing the 'DB instance identifier' field with the value 'database-1'.

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](#)

Availability and durability

Deployment options [Info](#)
The deployment options below are limited to those supported by the engine you selected above.

- ☒ **Multi-AZ DB Cluster - new**
Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.
- ☐ **Multi-AZ DB instance (not supported for Multi-AZ DB cluster snapshot)**
Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.
- ☐ **Single DB instance (not supported for Multi-AZ DB cluster snapshot)**
Creates a single DB instance with no standby DB instances.

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. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

- Give it an identifier you can easily identify it with
- Give it a master username or leave it as default admin. For the purpose of these instructions I will be using **root**
- Give it a password that you write down somewhere else to make sure you have the correct one. For the purpose of these instructions I will be using **Re:Start!9**

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. 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](#)

- Everything between this and the last step is left default
- Assign your vpc
- Make sure your subnet group is listed under the subnet group section
- Public access is no
- Choose existing VPC security groups
- Remove the default security group and add your database security group
- Select your first availability zone as well

Connectivity



Virtual private cloud (VPC) [Info](#)

VPC that defines the virtual networking environment for this DB instance.

Demo VPC (vpc-03bd2b389d2a4d45e) ▼

Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change its VPC.

Subnet group [Info](#)

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

dbsubnetgroup ▼

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 ▼

MyDatabaseServerSG ✕

Availability Zone [Info](#)

us-west-2a ▼

- Scroll down to Additional configuration on the bottom and give it an initial database name and save it in the same spot as your password since it will be used later
- Disable automated backups and encryption since they are not needed (These are normally best practice to leave enabled but the database will spin up faster with those checked off as they are not needed).
- Scroll down all the way to the bottom and create your database

▼ **Additional configuration**

Database options, encryption disabled, backup disabled, backtrack disabled, Enhanced Monitoring disabled, maintenance, CloudWatch Logs, delete protection disabled.

Database options

Initial database name [Info](#)

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

DB parameter group [Info](#)

 ▼

Option group [Info](#)

 ▼

Backup

☐ **Enable automated backups**
Creates a point-in-time snapshot of your database

Encryption

☐ **Enable encryption**
Choose to encrypt the given instance. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service console. [Info](#)

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

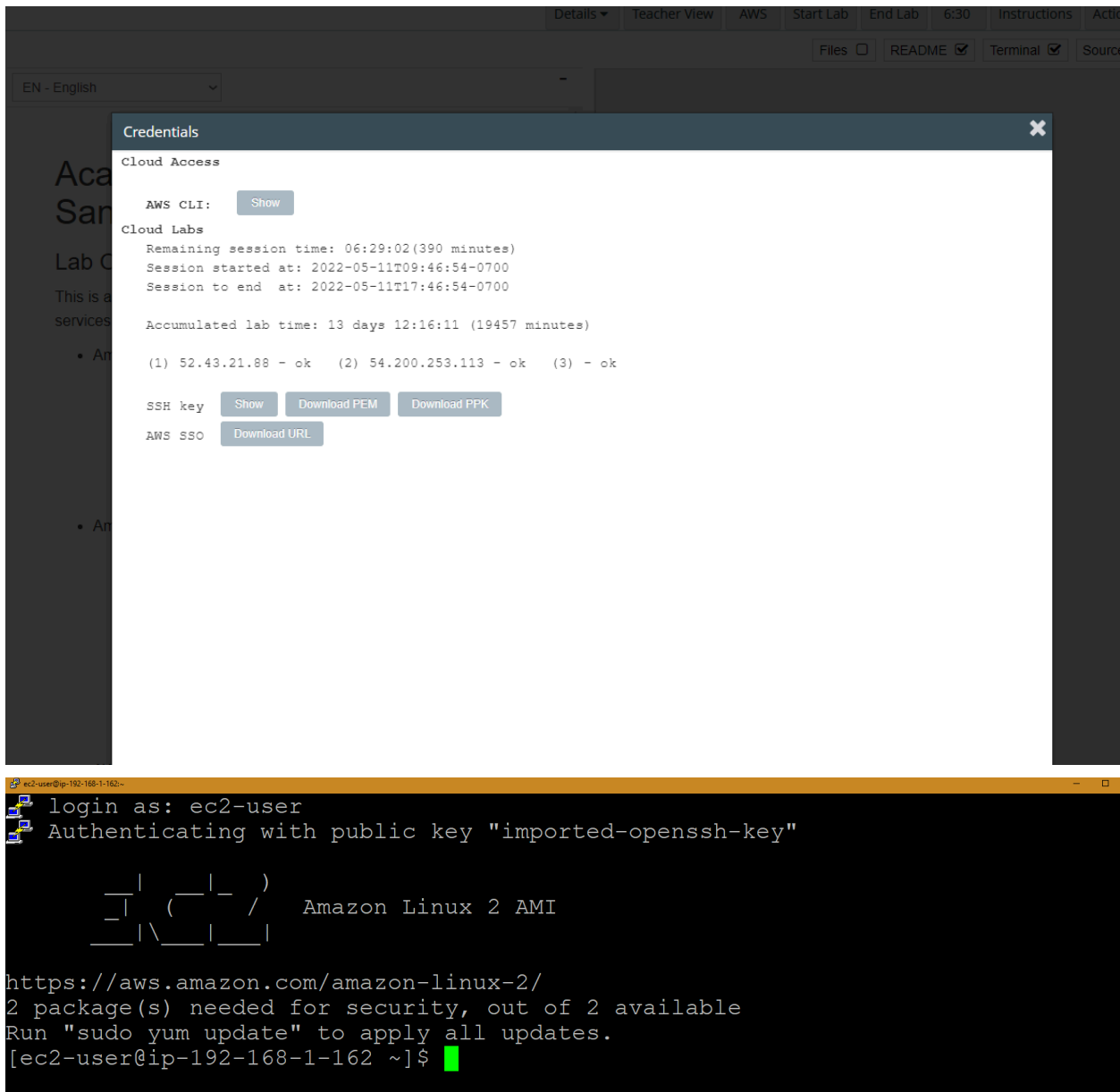
Select the log types to publish to Amazon CloudWatch Logs

☐ **Audit log**

☐ **Error log**

Step 4: Test connections

- SSH into your Bastion Host after downloading both the pem and ppk files from the lab environment



The screenshot displays a web application interface with a 'Credentials' modal open. The modal contains information about 'Cloud Access' and 'Cloud Labs'. It includes buttons for 'Show', 'Download PEM', 'Download PPK', and 'Download URL'. Below the modal, a terminal window shows the login process for an EC2 instance.

Credentials Modal:

- Cloud Access:** AWS CLI: Show
- Cloud Labs:**
 - Remaining session time: 06:29:02 (390 minutes)
 - Session started at: 2022-05-11T09:46:54-0700
 - Session to end at: 2022-05-11T17:46:54-0700
 - Accumulated lab time: 13 days 12:16:11 (19457 minutes)
 - (1) 52.43.21.88 - ok (2) 54.200.253.113 - ok (3) - ok
- SSH key:** Show Download PEM Download PPK
- AWS SSO:** Download URL

Terminal Window:

```
ec2-user@ip-192-168-1-162~$ login as: ec2-user
Authenticating with public key "imported-openssh-key"

  _ | ( _ | _ )
  _ | ( _ | _ /   Amazon Linux 2 AMI
  _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
2 package(s) needed for security, out of 2 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-192-168-1-162 ~]$
```

- ```
PS C:\Users\nickb> Pscpy -scp -P 22 -i '.\Downloads\labsuser.ppk' -l user ec2-us-200.253.113:/home/ec2-user
pscp: ec2-user: No such file or directory

labsuser.pem | 1 kB | 1.6 kB/s | ETA: 00:00:00 | 100%
PS C:\Users\nickb>
```

- ```
[ec2-user@ip-192-168-1-162 ~]$ ls
labsuser.pem
[ec2-user@ip-192-168-1-162 ~]$
```

- ```
[ec2-user@ip-192-168-1-162 ~]$ chmod 400 labsuser.pem
[ec2-user@ip-192-168-1-162 ~]$ ssh -i labsuser.pem ec2-user@192.168
.2.172
The authenticity of host '192.168.2.172 (192.168.2.172)' can't be e
stablished.
ECDSA key fingerprint is SHA256:RURnbNWL6+XNSA3+S9k0FtM1Fy0aAHcv4z7
qLtKlm7A.
ECDSA key fingerprint is MD5:ce:f3:58:79:65:eb:ae:de:6a:3c:51:5c:89
:4b:69:88.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.2.172' (ECDSA) to the list of k
nown hosts.

 | _|_)
 | (_|_ / Amazon Linux 2 AMI
 | _|_ |_|_

https://aws.amazon.com/amazon-linux-2/
2 package(s) needed for security, out of 2 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-192-168-2-172 ~]$ ls
[ec2-user@ip-192-168-2-172 ~]$
```

- Use ping and the private ip address of your web server to ping the web server and see it connect

```
[ec2-user@ip-192-168-2-172 ~]$ ping 192.168.1.252
PING 192.168.1.252 (192.168.1.252) 56(84) bytes of data.
64 bytes from 192.168.1.252: icmp_seq=1 ttl=255 time=0.486 ms
64 bytes from 192.168.1.252: icmp_seq=2 ttl=255 time=0.441 ms
64 bytes from 192.168.1.252: icmp_seq=3 ttl=255 time=0.450 ms
64 bytes from 192.168.1.252: icmp_seq=4 ttl=255 time=0.483 ms
^C
--- 192.168.1.252 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3052ms
rtt min/avg/max/mdev = 0.441/0.465/0.486/0.019 ms
[ec2-user@ip-192-168-2-172 ~]$
```

- Test out connecting to the database by typing out `mysql -user=root -password='Re:Start!9' -host=database-server-endpoint`
- Replace database-server-endpoint with the database server endpoint
- Type `show databases;` to see your database from the app server

## Connection details to your database database



This is the only time you can view this password. Copy and save the password for your reference. If you lose the password, you must modify your database to change it. You can use a SQL client application or utility to connect to your database.

[Learn about connecting to your database](#)

Master username

root

Master password

Re:Start!9 **Copy**

Endpoint

database.c1isoy422nnt.us-west-2.rds.amazonaws.com **Copy**

Close

```
[ec2-user@ip-192-168-2-31 ~]$ mysql --user=root --password='Re:Start!9' --host=database.clisoy422nnt.us-west-2.rds.amazonaws.com
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 83
Server version: 10.11.6-MariaDB managed by https://aws.amazon.com/rds/

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| innodb |
| mydb |
| mysql |
| performance_schema |
| sys |
+-----+
6 rows in set (0.01 sec)

MariaDB [(none)]> █
```

- This concludes the lab