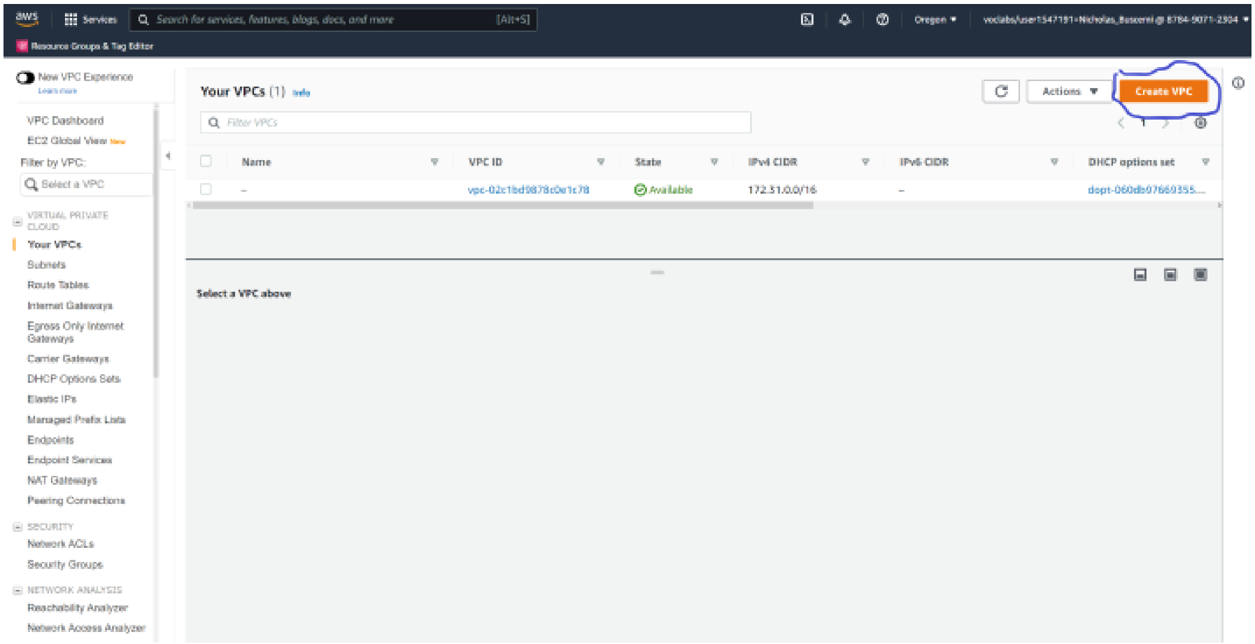
Step 1: Create a VPC and Subnets as well as routing and security groups

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

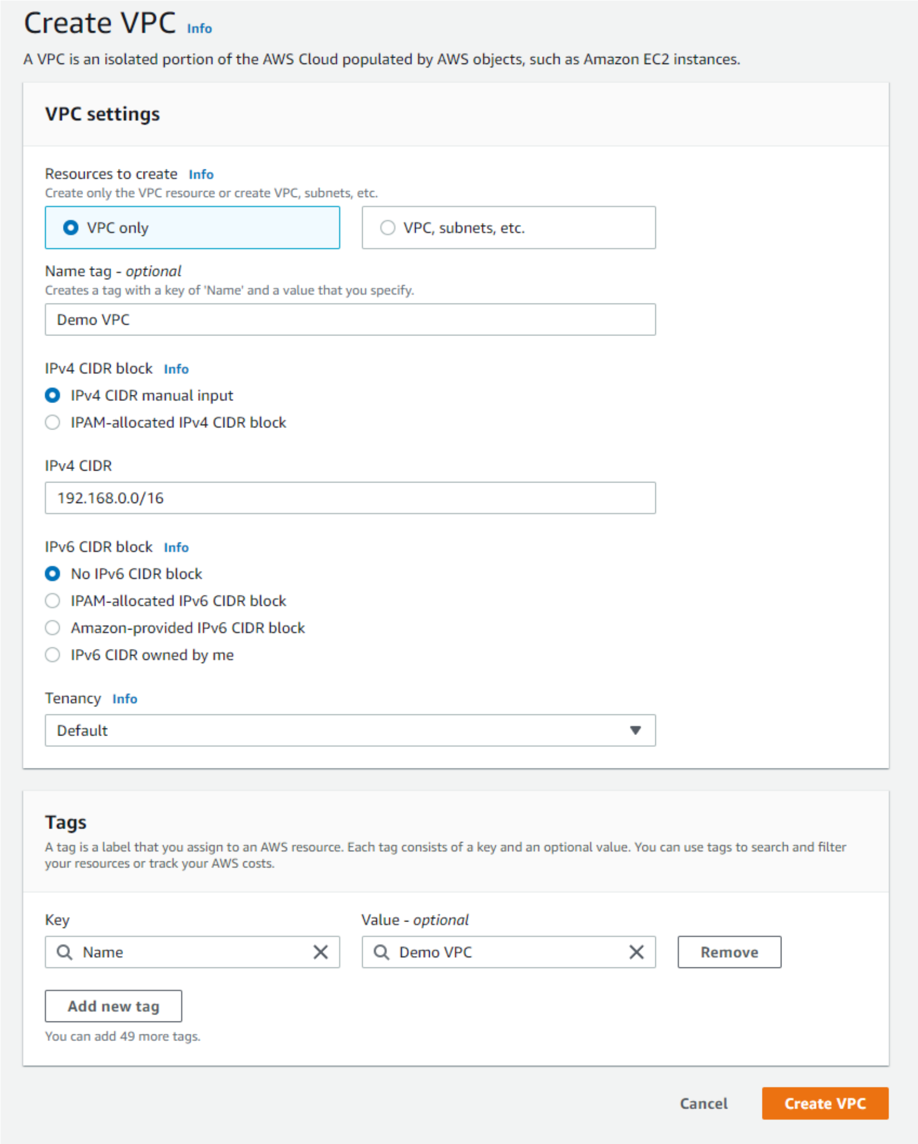


Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set
–	vpc-02c1bd9878c0e1c78	Available	172.31.0.0/16	–	dopt-060db07660355...

Select a VPC above

- 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

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

VPC settings

Resources to create
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
● IPv4 CIDR manual input
○ IPAM-allocated IPv4 CIDR block

IPv4 CIDR
192.168.0.0/16

IPv6 CIDR block
● No IPv6 CIDR block
○ IPAM-allocated IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block
○ IPv6 CIDR owned by me

Tenancy
Default

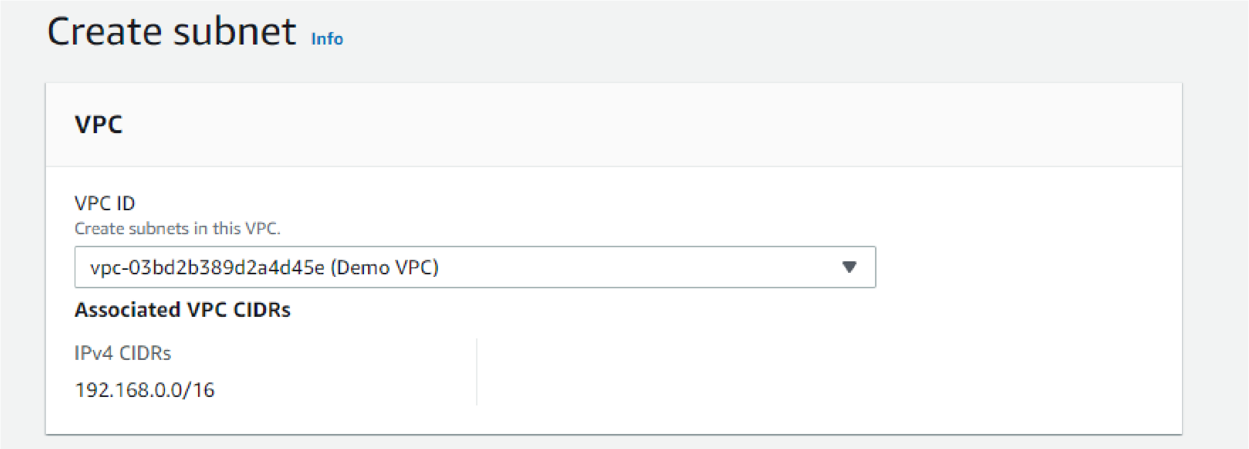
Tags

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	Value - *optional*
Name	Demo VPC

You can add 49 more tags.

- 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

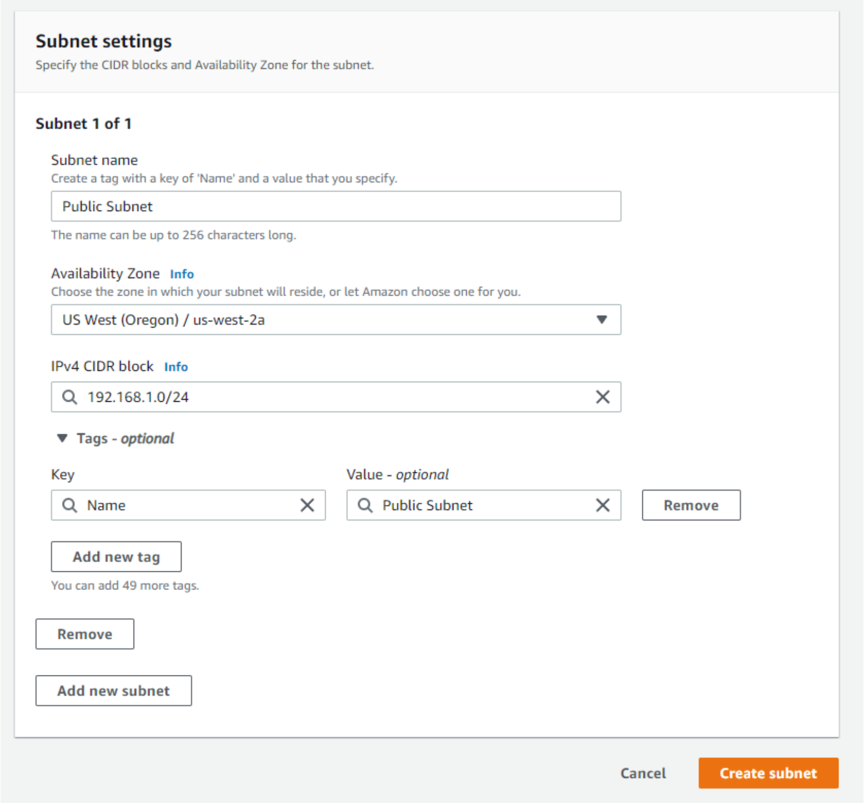
VPC

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.

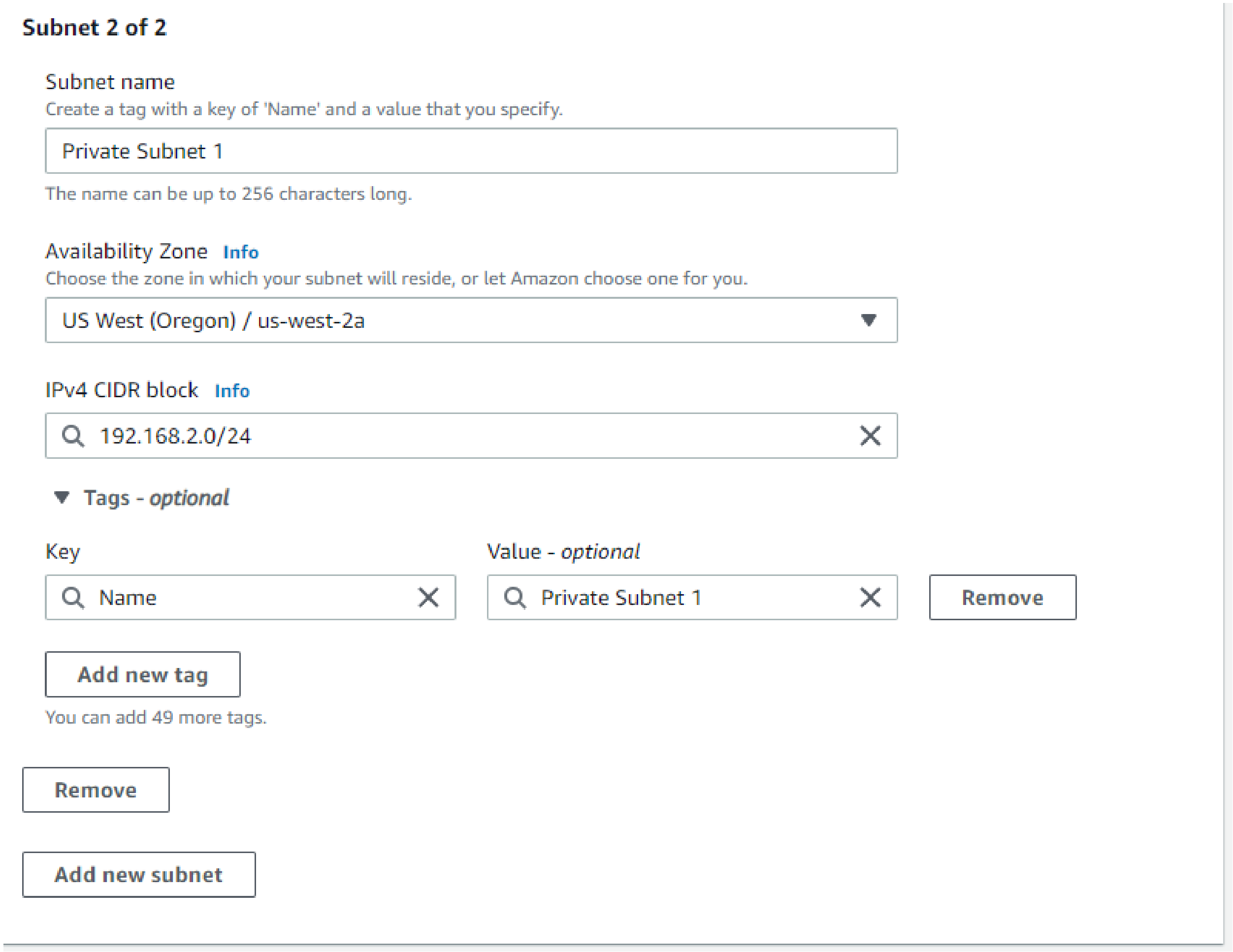
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US West (Oregon) / us-west-2a

IPv4 CIDR block Info
192.168.1.0/24

Tags - *optional*

Key	Value - *optional*
Name	Public 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

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

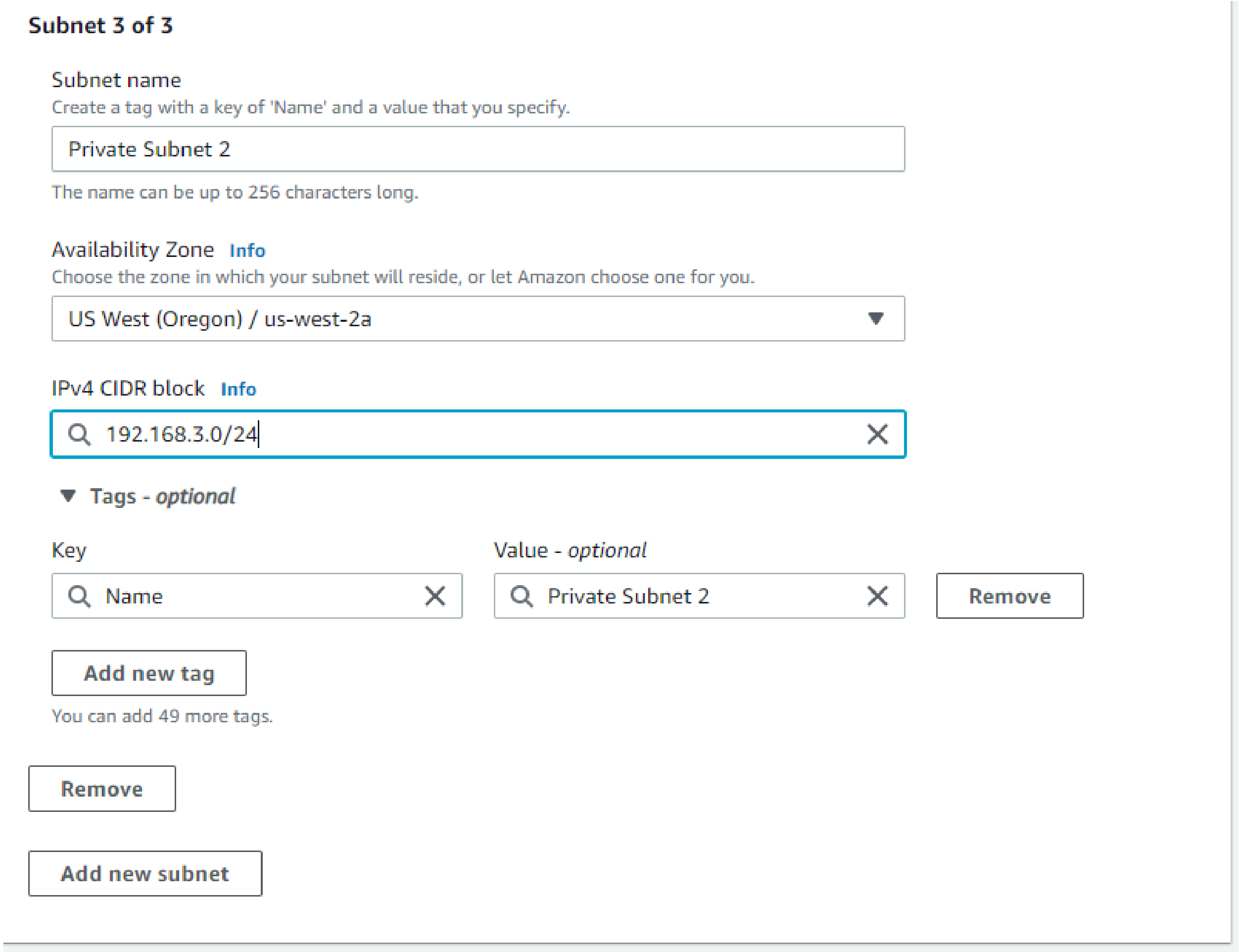
192.168.2.0/24

Tags - *optional*

Key	Value - *optional*
Name	Private Subnet 1

You can add 49 more tags.

- 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.
Private Subnet 2
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

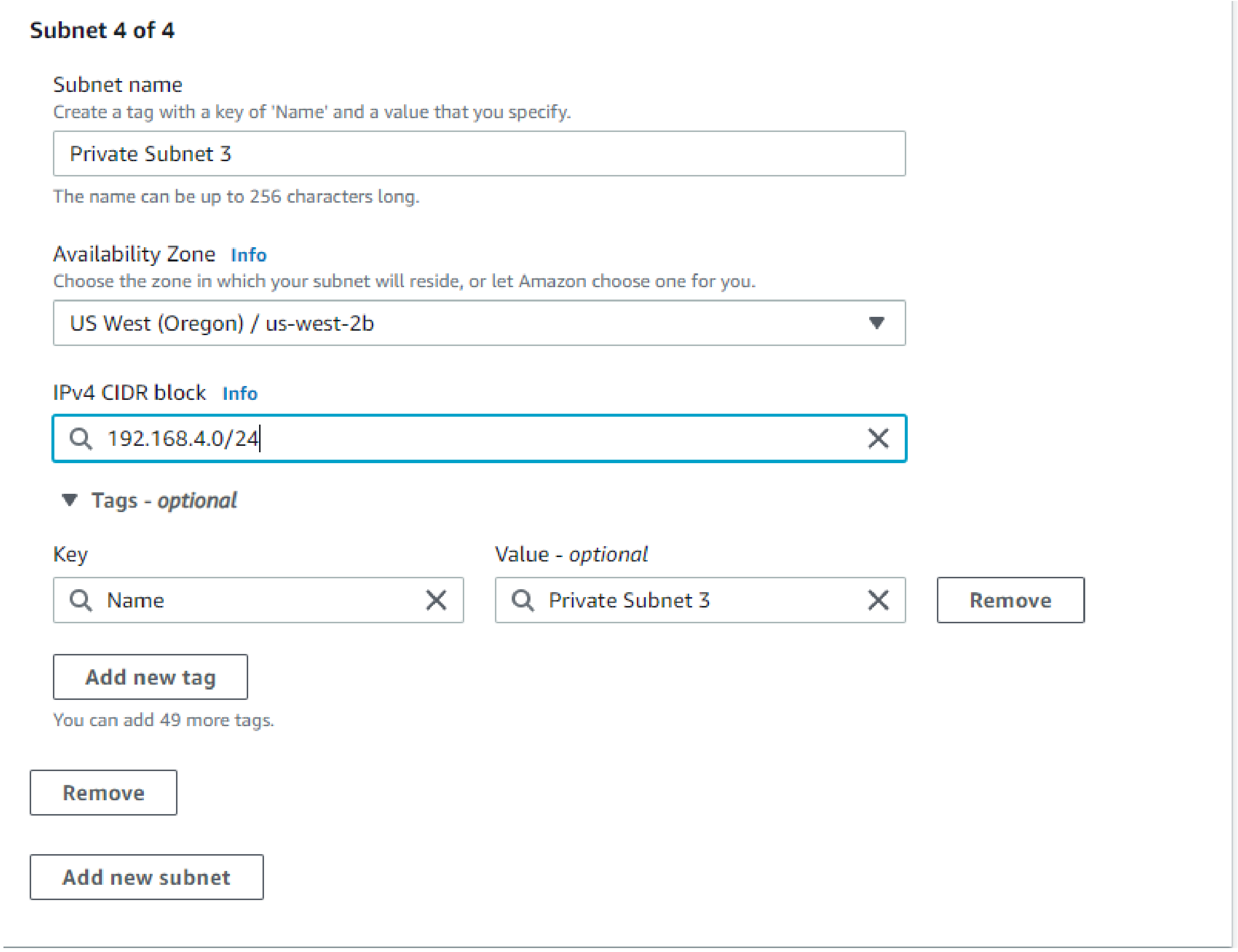
IPv4 CIDR block Info
192.168.3.0/24

Tags - *optional*

Key	Value - *optional*
Name	Private Subnet 2

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.
Private Subnet 3
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-2b

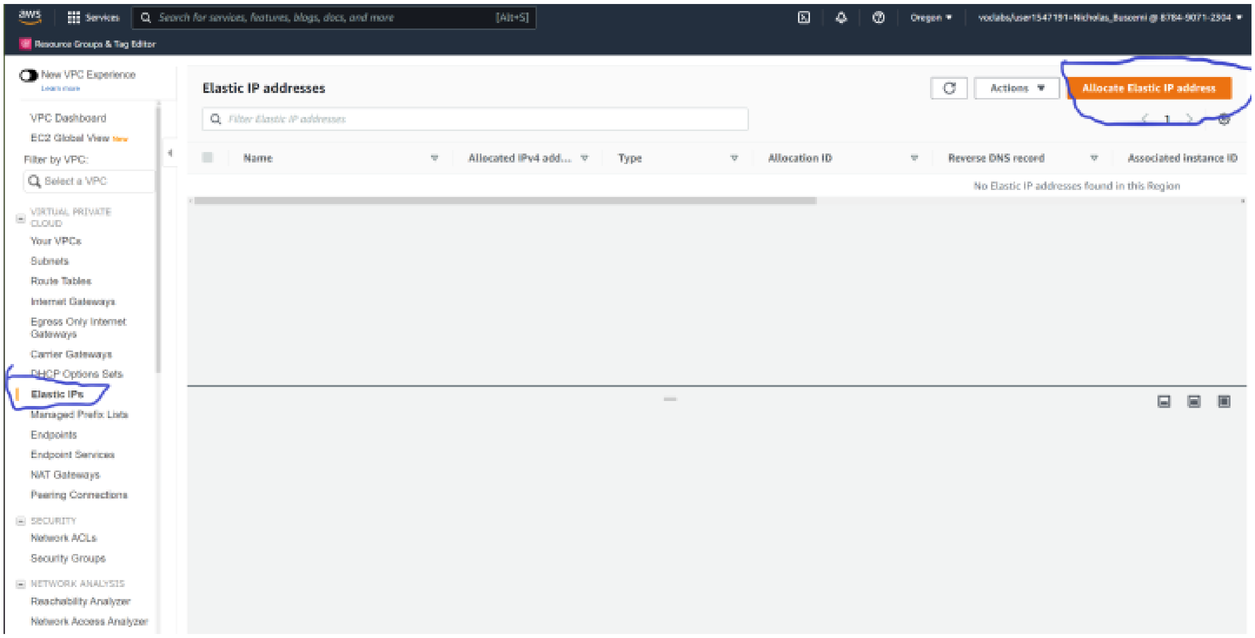
IPv4 CIDR block Info
192.168.4.0/24

▼ Tags - *optional*

Key	Value - *optional*
Name	Private Subnet 3

You can add 49 more tags.

- 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”

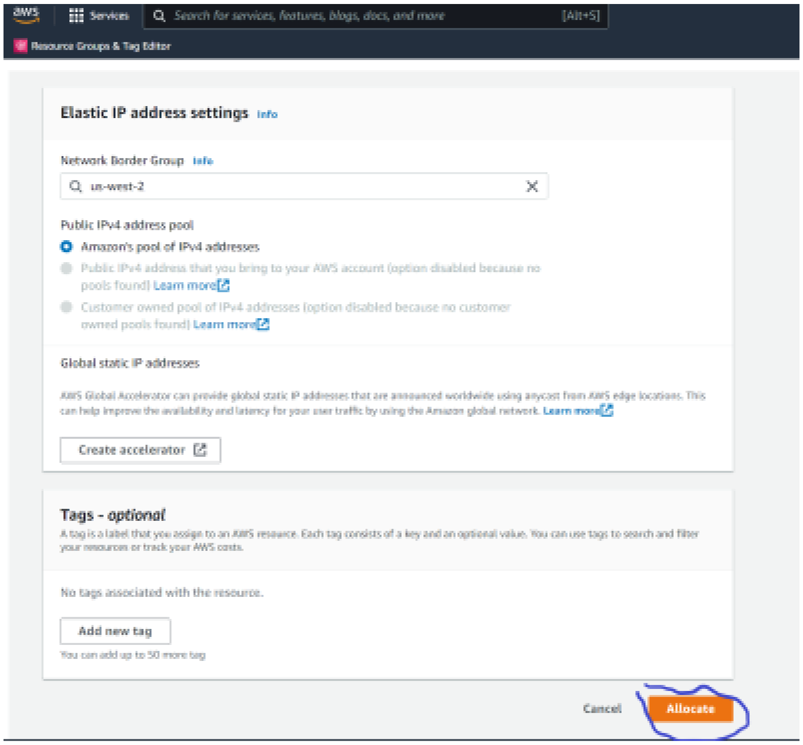


Elastic IP addresses

Name	Allocated IPv4 add...	Type	Allocation ID	Reverse DNS record	Associated instance ID

No Elastic IP addresses found in this Region

- 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


aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Resource Groups & Tag Editor
Create accelerator
Add new tag
Cancel
Allocate

Elastic IP address settings Info

Network Border Group Info

us-west-2

Public IPv4 address pool

● Amazon's pool of IPv4 addresses

○ Public IPv4 address that you bring to your AWS account (option disabled because no pools found) Learn more

○ Customer owned pool of IPv4 addresses (option disabled because no customer owned pools found) Learn more

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. Learn more

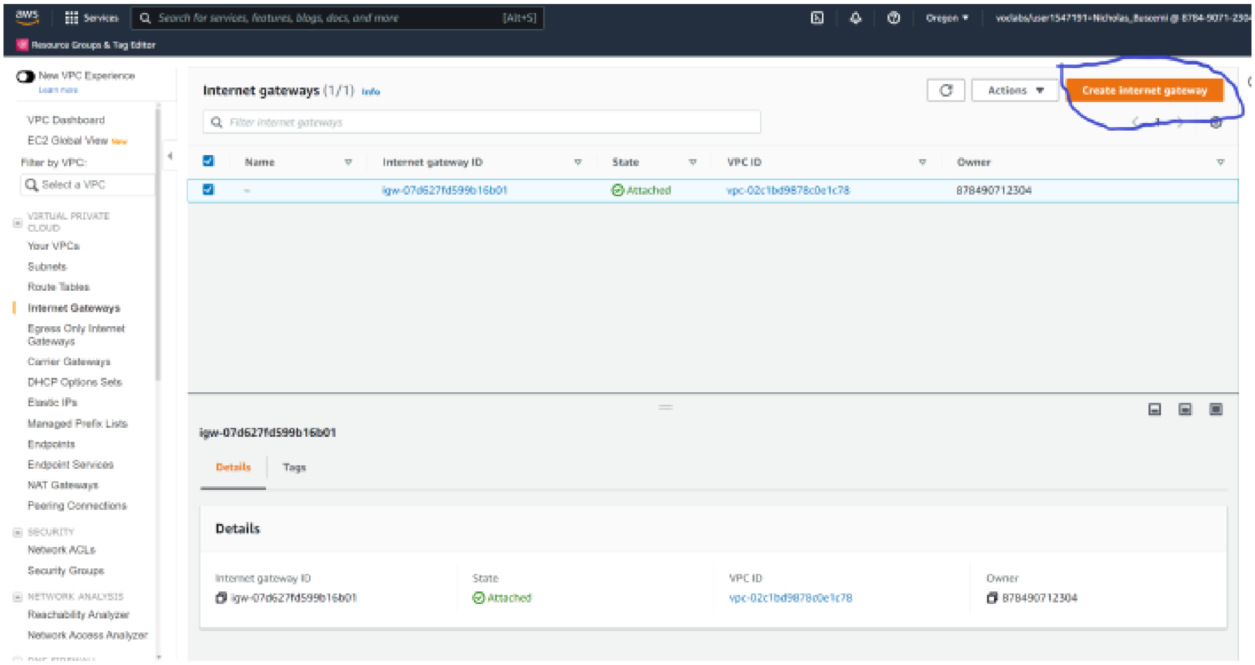
Tags - *optional*

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.

No tags associated with the resource.

You can add up to 50 more tag

- 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”



Internet gateways (1/1)

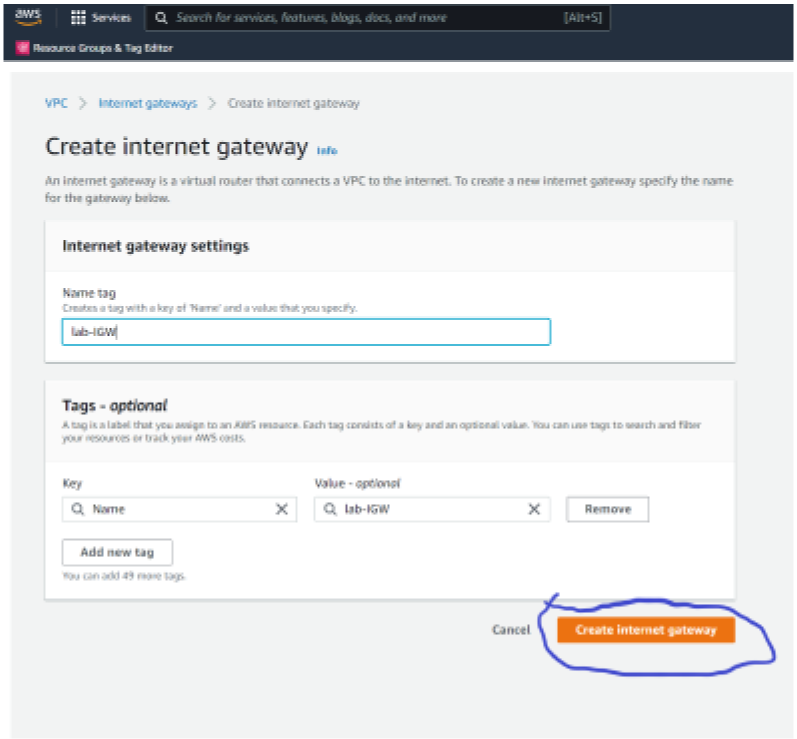
☑	Name	Internet gateway ID	State	VPC ID	Owner
☑	–	igw-07d627fd599b16b01	✓ Attached	vpc-02c1bd9878c0e1c78	878490712304

igw-07d627fd599b16b01

Details

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

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



VPC > Internet gateways > Create internet gateway

Create internet gateway

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

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

Tags - *optional*

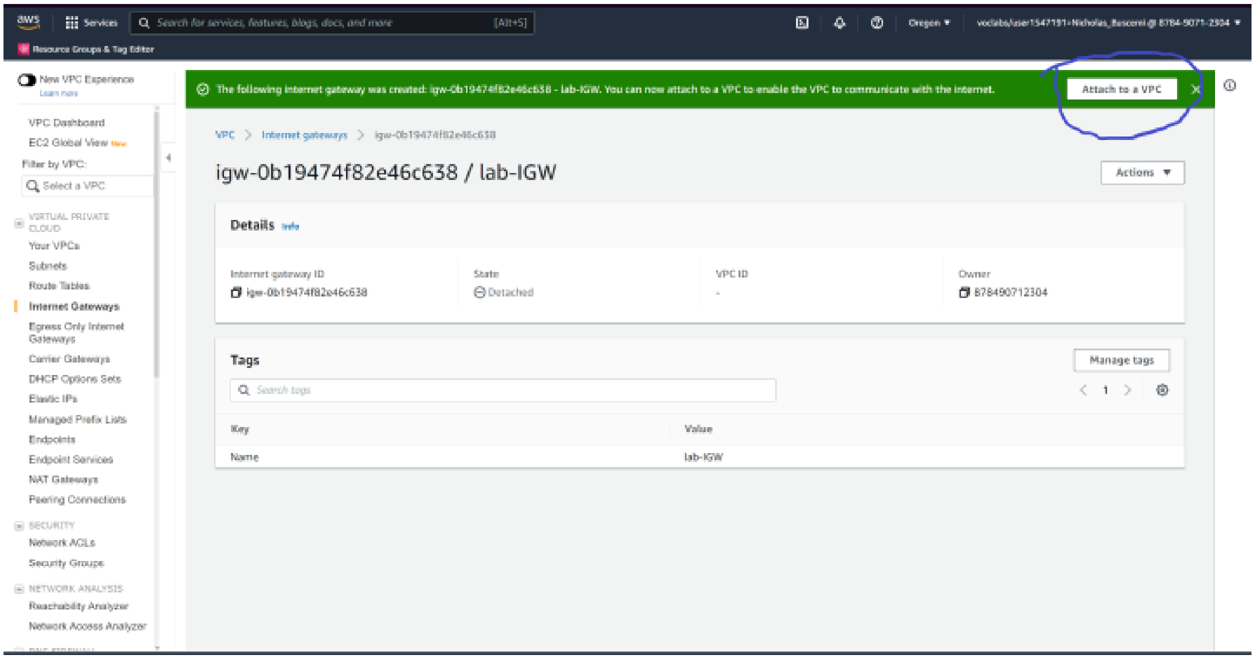
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*
Name	lab-IGW

You can add 49 more tags.

Services
Search for services, features, blogs, docs, and more [Alt+S]
Resource Groups & Tag Editor
Info
Remove
Add new tag
Cancel
Create internet gateway

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



The following internet gateway was created: igw-0b19474f82e46c638 - lab-IGW. You can now attach to a VPC to enable the VPC to communicate with the internet.

igw-0b19474f82e46c638 / lab-IGW

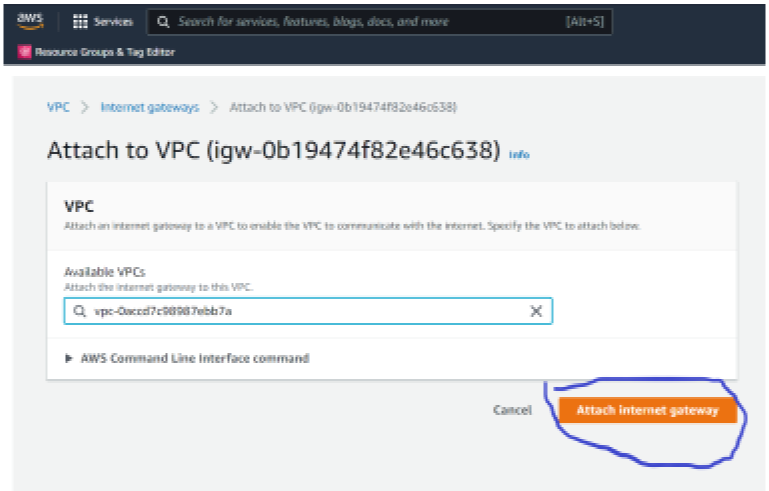
Details Info

Internet gateway ID	State	VPC ID	Owner
igw-0b19474f82e46c638	Detached	-	878490712304

Tags

Key	Value
Name	lab-IGW

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


Services
Search for services, features, blogs, docs, and more [Alt+S]
Resource Groups & Tag Editor
VPC > Internet gateways > Attach to VPC (igw-0b19474f82e46c638)
AWS Command Line Interface command
Cancel
Attach internet gateway

Attach to VPC (igw-0b19474f82e46c638) Info

VPC

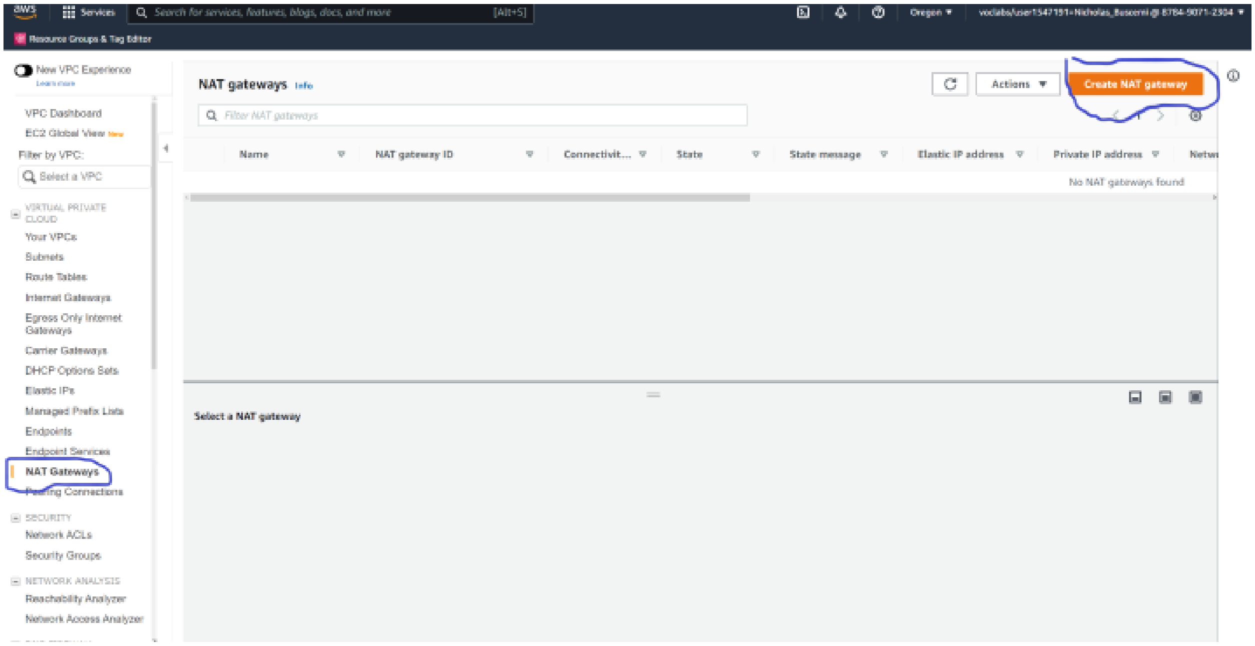
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

vpc-0accd7c98987ebb7a

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



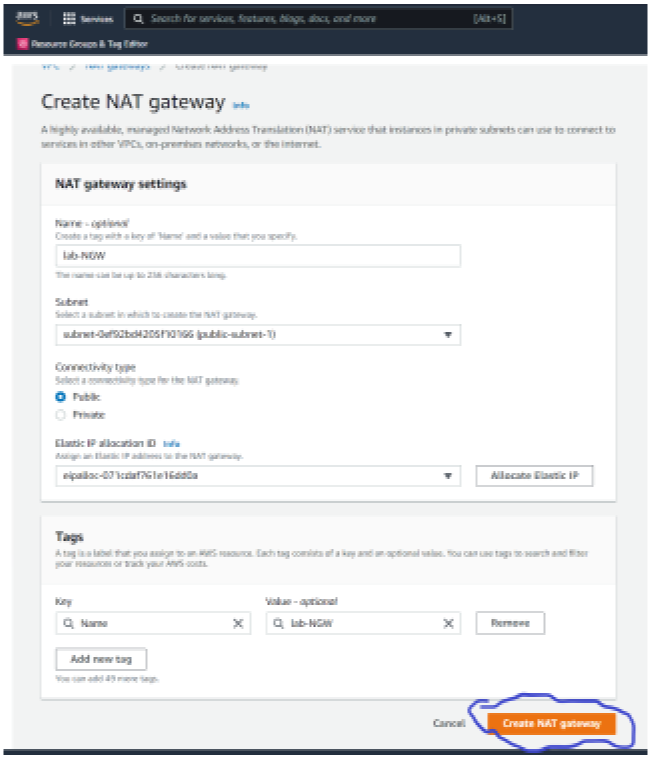
NAT gateways Info

Name	NAT gateway ID	Connectivit…	State	State message	Elastic IP address	Private IP address	Netw

No NAT gateways found

Select a 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”


aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Resource Groups & Tag Editor
VPC > NAT gateways > Create NAT gateway

Create NAT gateway Info

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

NAT gateway settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.
lab-NGW
The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.
subnet-0ef92bd4205f10166 (public-subnet-1) ▾

Connectivity type
Select a connectivity type for the NAT gateway.
● Public
○ Private

Elastic IP allocation ID Info
Assign an Elastic IP address to the NAT gateway.
eipalloc-071cdaf761e16dd0a ▾ Allocate Elastic IP

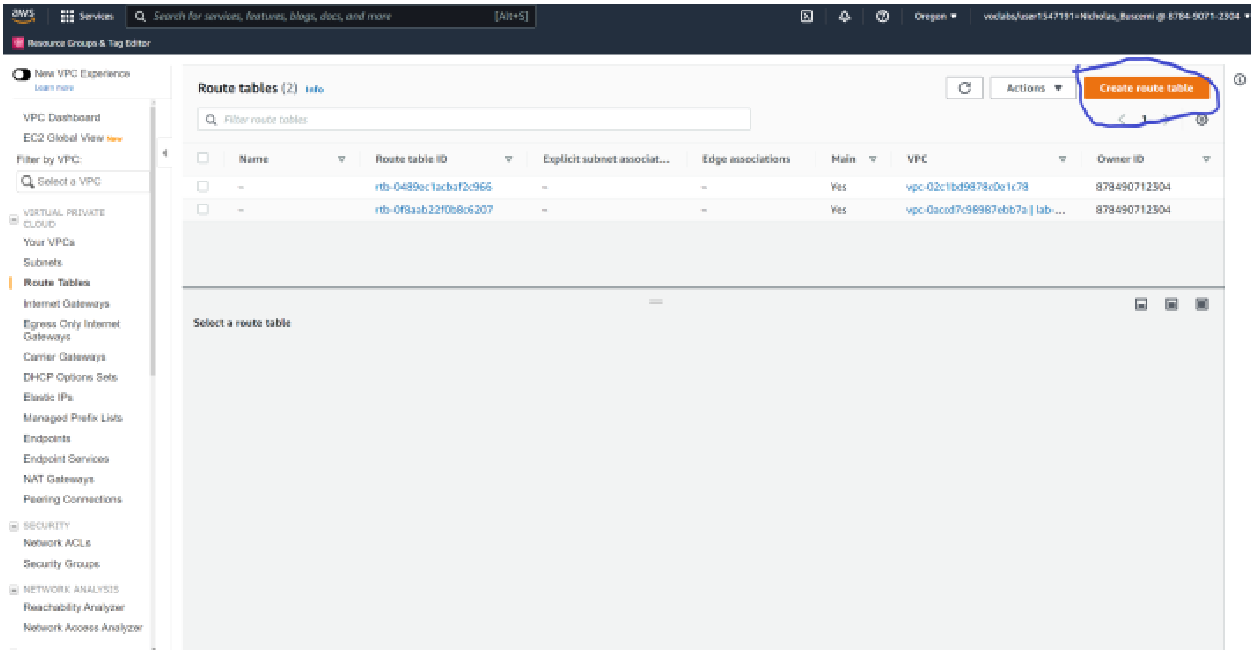
Tags

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	Value - optional	
Name	lab-NGW	Remove

Add new tag
You can add 49 more tags.

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

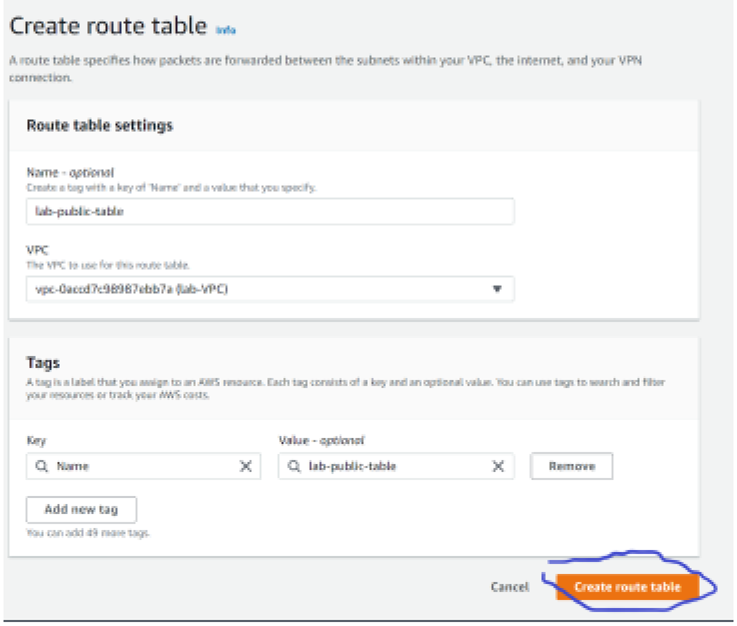


Route tables (2) Info

Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
–	rtb-0489ec1acbaf2c966	–	–	Yes	vpc-02c1bd9878c0e1c78	878490712304
–	rtb-0f8aab22f0b8c6207	–	–	Yes	vpc-0accd7c98987ebb7a | lab-...	878490712304

Select a 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”



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-public-table

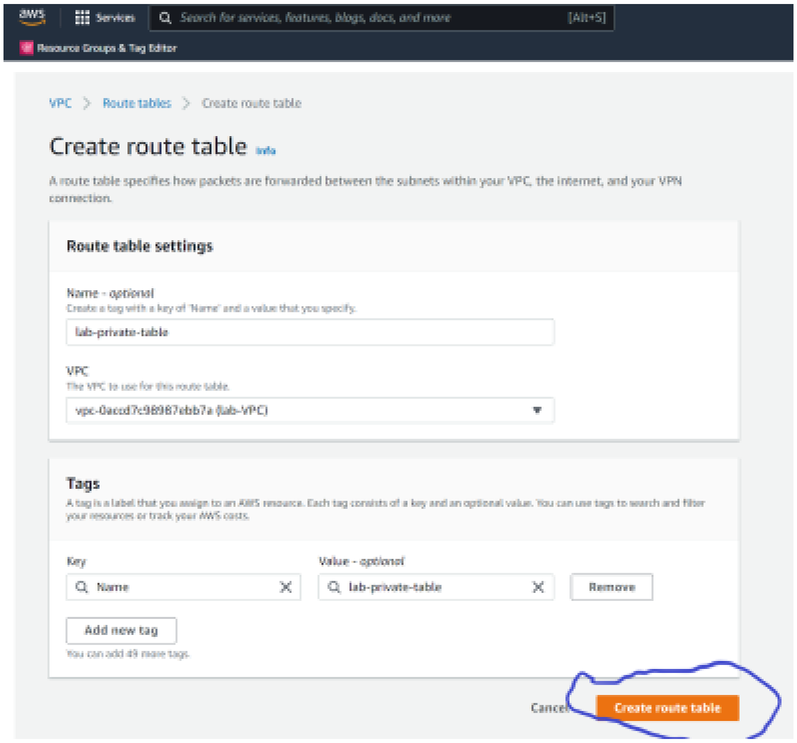
VPC
The VPC to use for this route table.
vpc-0accd7c98987ebb7a (lab-VPC)

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	Value - optional
Name	lab-public-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


aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Resource Groups & Tag Editor
VPC > Route tables > Create route table

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

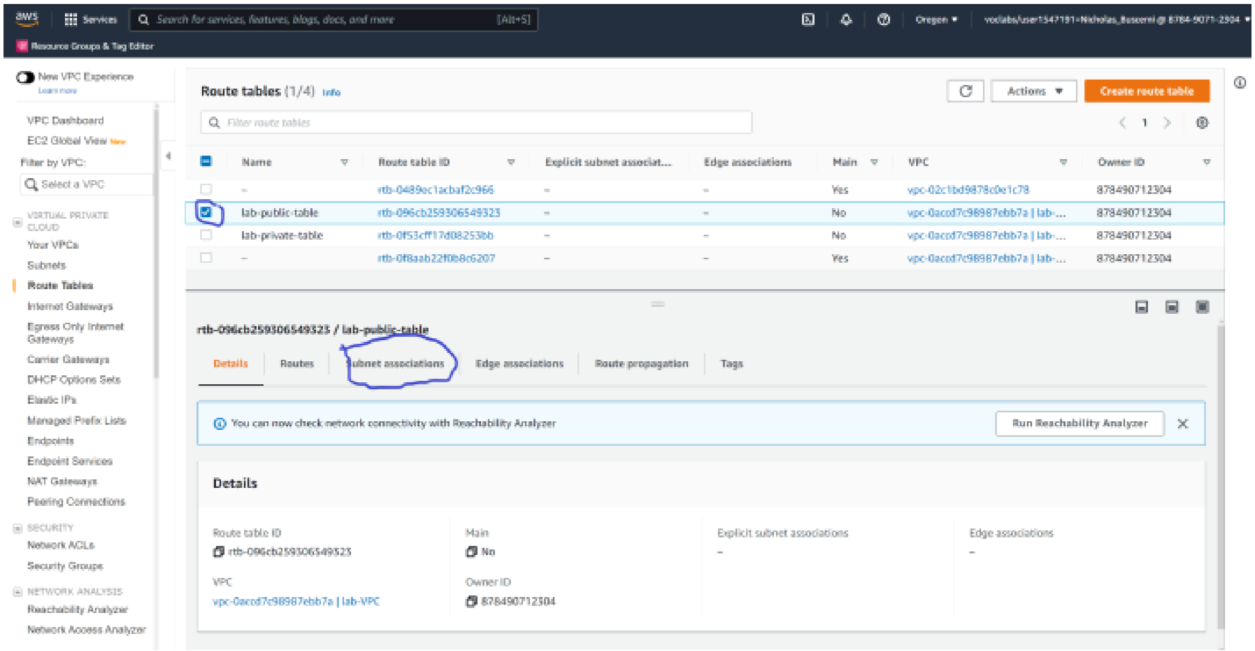
VPC
The VPC to use for this route table.
vpc-0acod7c98987ebb7a (lab-VPC)

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	Value - *optional*
Name	lab-private-table

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



	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
□	–	rtb-0489ec1acbaf2c966	–	–	Yes	vpc-02c1bd9878c0e1c78	878490712304
☑	lab-public-table	rtb-096cb259306549323	–	–	No	vpc-0acod7c98987ebb7a | lab-...	878490712304
□	lab-private-table	rtb-0f53cff17d08253bb	–	–	No	vpc-0acod7c98987ebb7a | lab-...	878490712304
□	–	rtb-0f8aab22f0b8c6207	–	–	Yes	vpc-0acod7c98987ebb7a | lab-...	878490712304

rtb-096cb259306549323 / lab-public-table

You can now check network connectivity with Reachability Analyzer

Details

Route table ID
rtb-096cb259306549323

VPC
vpc-0acod7c98987ebb7a | lab-VPC

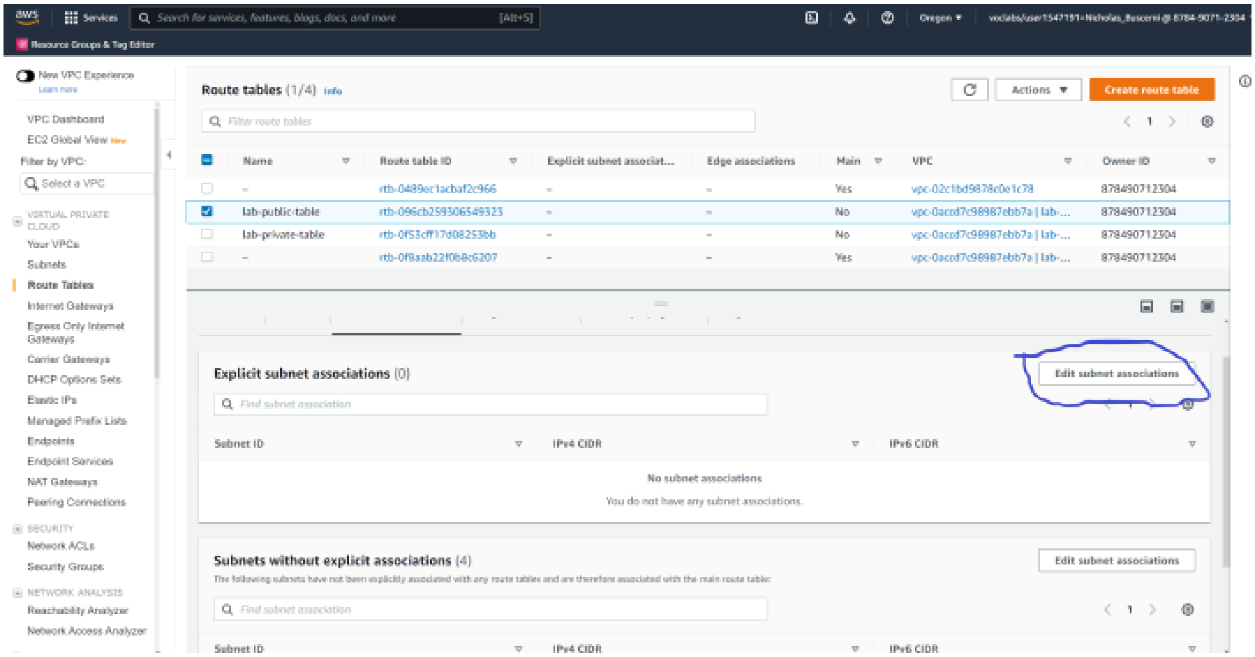
Main
No

Owner ID
878490712304

Explicit subnet associations
–

Edge associations
–

- Click on “Edit subnet associations”



Route tables (1/4) Info

	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
□	–	rtb-0489ec1acbaf2c966	–	–	Yes	vpc-02c1bd9878c0e1c78	878490712304
☑	lab-public-table	rtb-096cb259306549323	–	–	No	vpc-0acd7c98987ebb7a | lab-...	878490712304
□	lab-private-table	rtb-0f53cff17d08253bb	–	–	No	vpc-0acd7c98987ebb7a | lab-...	878490712304
□	–	rtb-0f8aab22f0b8c6207	–	–	Yes	vpc-0acd7c98987ebb7a | lab-...	878490712304

Explicit subnet associations (0)

Subnet ID	IPv4 CIDR	IPv6 CIDR

No subnet associations

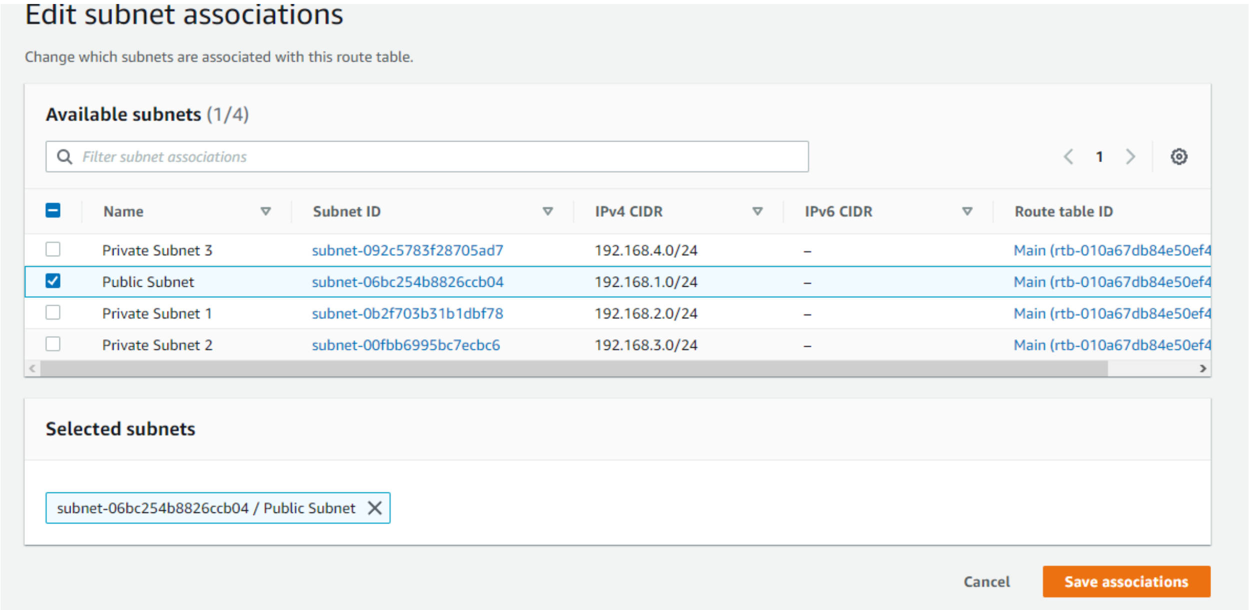
You do not have any subnet associations.

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:

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)

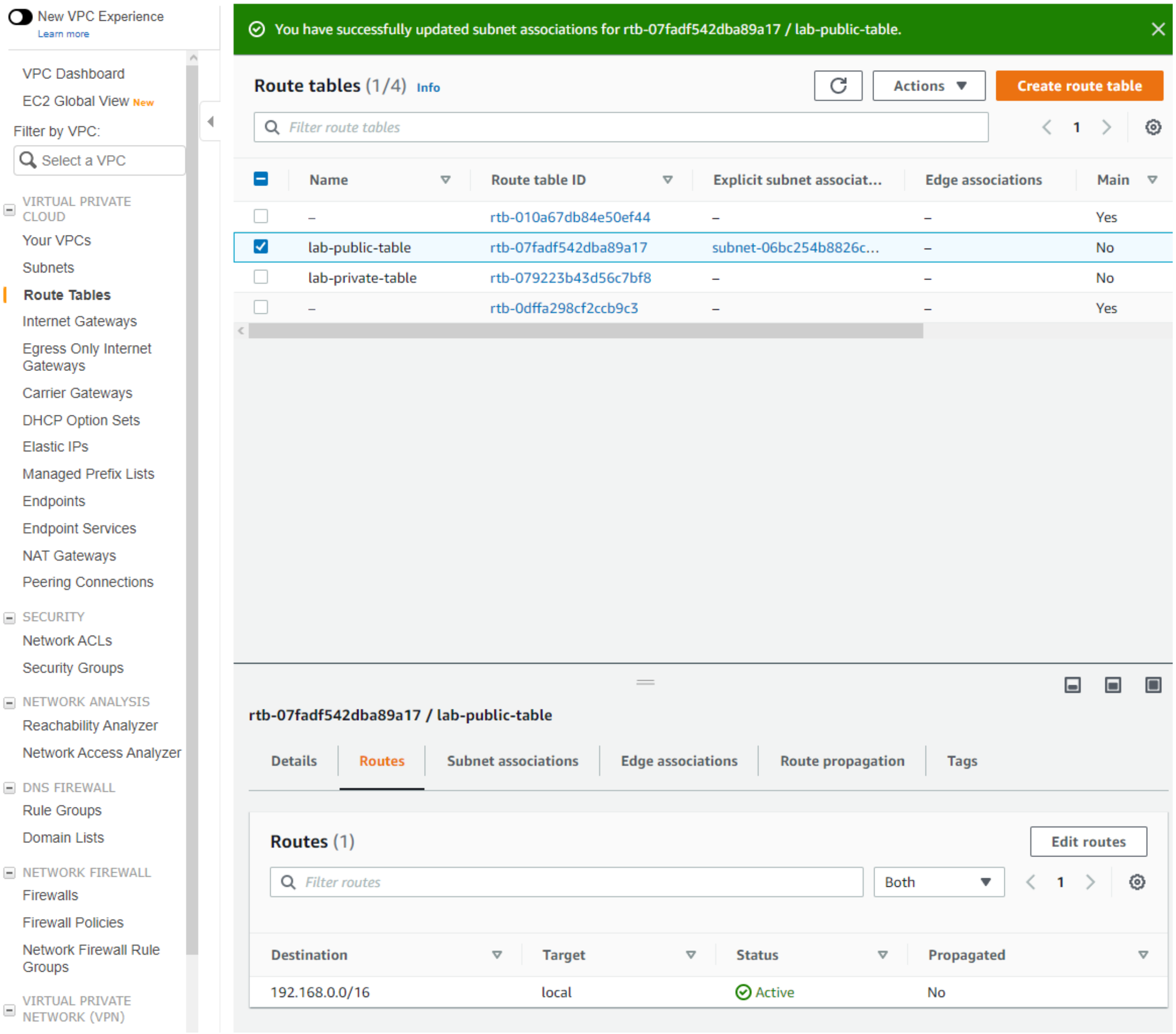
	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
□	Private Subnet 3	subnet-092c5783f28705ad7	192.168.4.0/24	–	Main (rtb-010a67db84e50ef4
☑	Public Subnet	subnet-06bc254b8826ccb04	192.168.1.0/24	–	Main (rtb-010a67db84e50ef4
□	Private Subnet 1	subnet-0b2f703b31b1dbf78	192.168.2.0/24	–	Main (rtb-010a67db84e50ef4
□	Private Subnet 2	subnet-00fbb6995bc7ecbc6	192.168.3.0/24	–	Main (rtb-010a67db84e50ef4

Selected subnets

subnet-06bc254b8826ccb04 / Public Subnet ✕

- 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”



You have successfully updated subnet associations for rtb-07fadf542dba89a17 / lab-public-table.

Route tables (1/4) Info

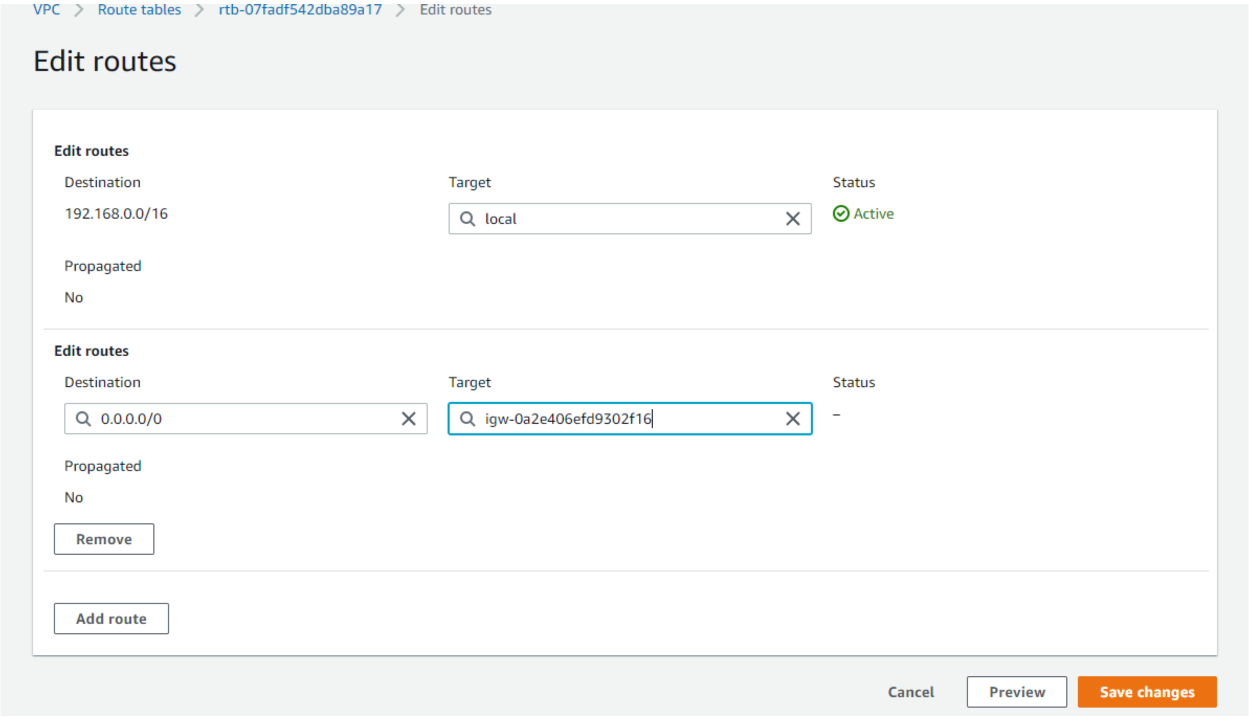
	Name	Route table ID	Explicit subnet associat...	Edge associations	Main
□	–	rtb-010a67db84e50ef44	–	–	Yes
☑	lab-public-table	rtb-07fadf542dba89a17	subnet-06bc254b8826c...	–	No
□	lab-private-table	rtb-079223b43d56c7bf8	–	–	No
□	–	rtb-0dffa298cf2ccb9c3	–	–	Yes

rtb-07fadf542dba89a17 / lab-public-table

Routes (1)

Destination	Target	Status	Propagated
192.168.0.0/16	local	✓ Active	No

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



Edit routes

Edit routes

Destination	Target	Status
192.168.0.0/16	local	Active

Propagated

No

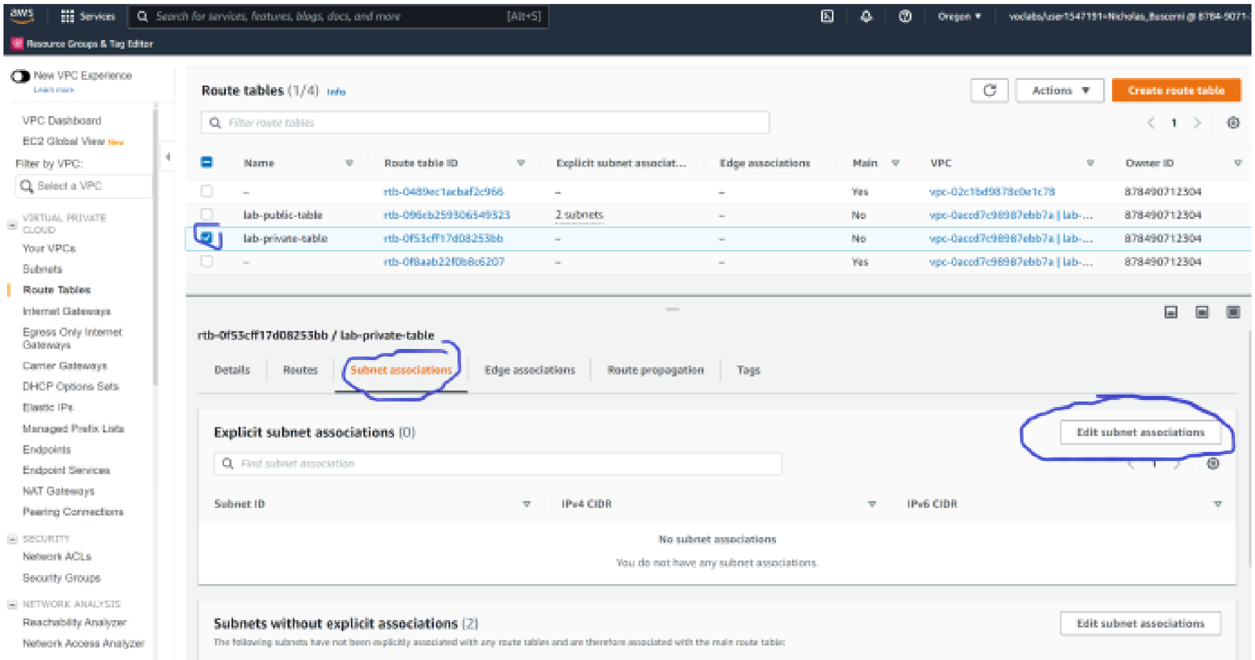
Edit routes

Destination	Target	Status
0.0.0.0/0	igw-0a2e406efd9302f16	-

Propagated

No

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



Route tables (1/4) Info

Filter route tables

	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
□	–	rtb-0489ec1acbaf2c966	–	–	Yes	vpc-02c1bd9878e0e1c78	878490712304
□	lab-public-table	rtb-096cb259306549323	2 subnets	–	No	vpc-0acd7c98987ebb7a | lab-...	878490712304
☑	lab-private-table	rtb-0f53cff17d08253bb	–	–	No	vpc-0acd7c98987ebb7a | lab-...	878490712304
□	–	rtb-0f8aab22f0b8c6207	–	–	Yes	vpc-0acd7c98987ebb7a | lab-...	878490712304

rtb-0f53cff17d08253bb / lab-private-table

Explicit subnet associations (0)

Find subnet association

Subnet ID	IPv4 CIDR	IPv6 CIDR

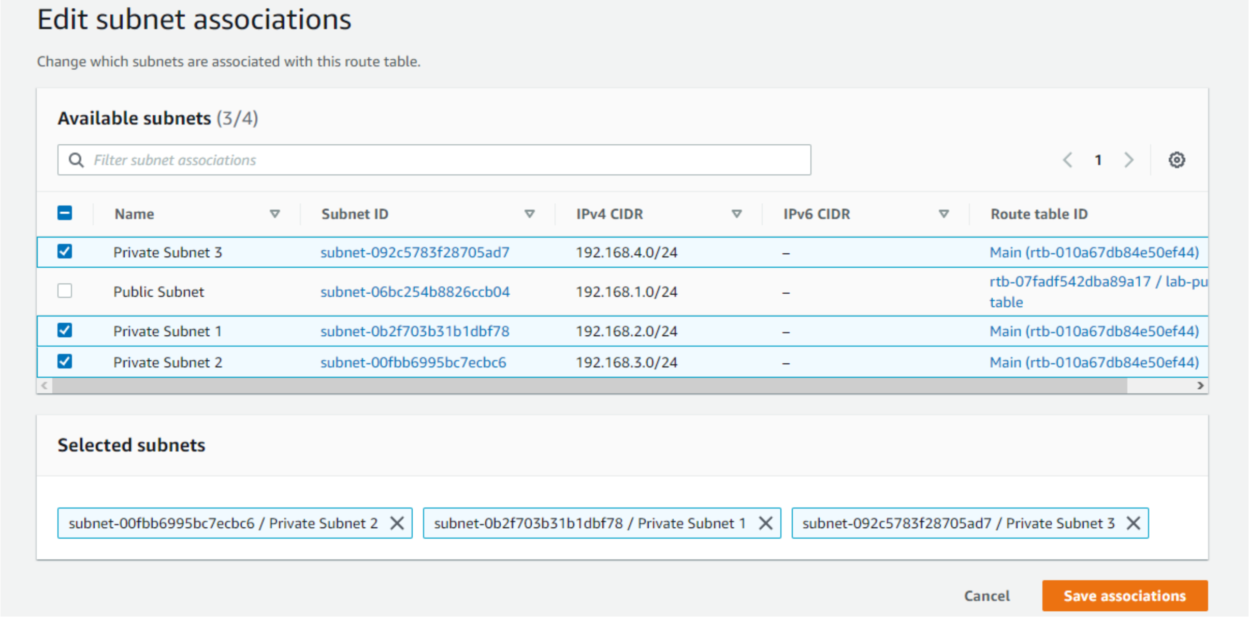
No subnet associations

You do not have any subnet associations.

Subnets without explicit associations (2)

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

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



Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (3/4)

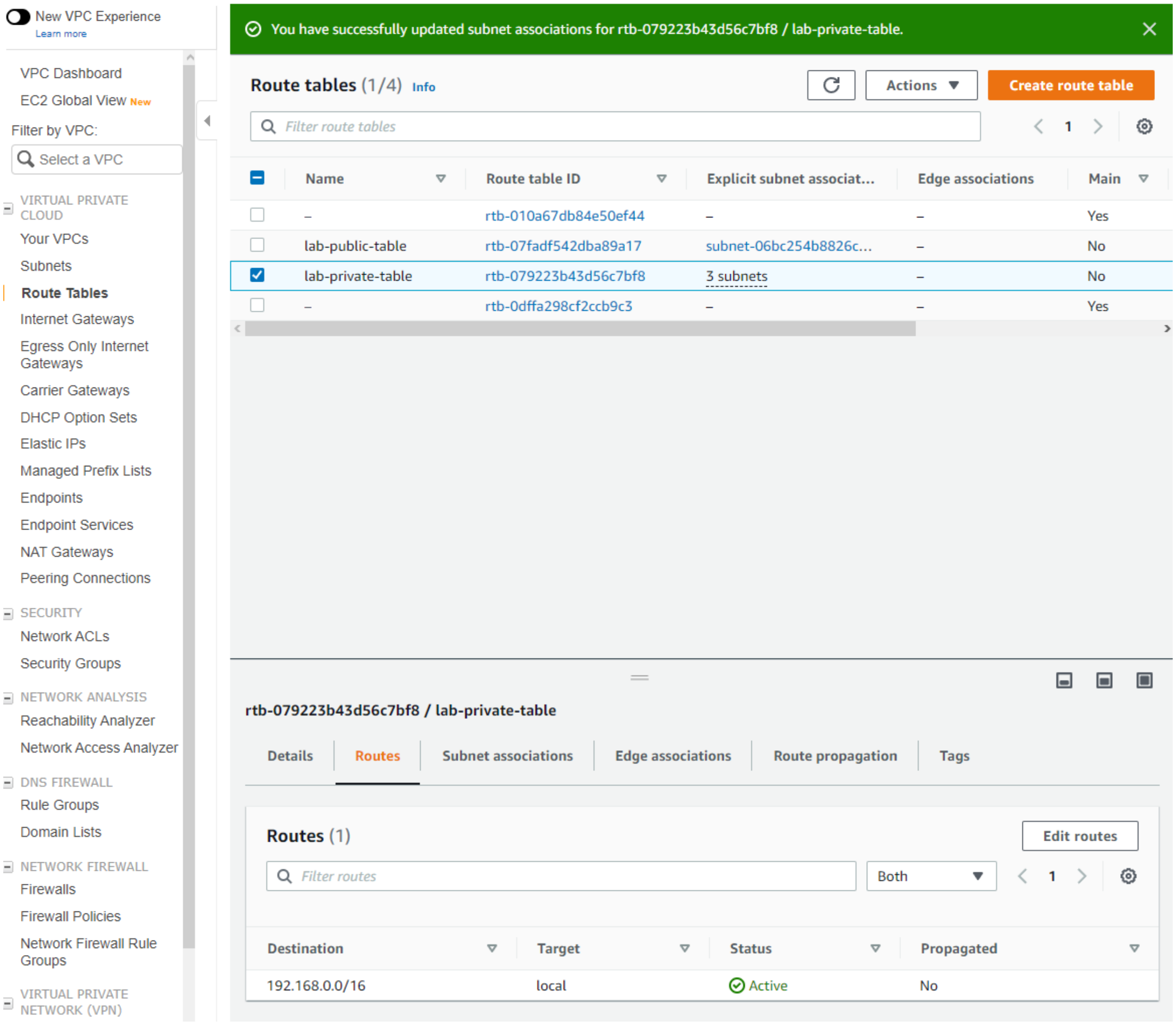
Filter subnet associations

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☑	Private Subnet 3	subnet-092c5783f28705ad7	192.168.4.0/24	–	Main (rtb-010a67db84e50ef44)
□	Public Subnet	subnet-06bc254b8826ccb04	192.168.1.0/24	–	rtb-07fadf542dba89a17 / lab-pu table
☑	Private Subnet 1	subnet-0b2f703b31b1dbf78	192.168.2.0/24	–	Main (rtb-010a67db84e50ef44)
☑	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



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

Route tables (1/4) Info

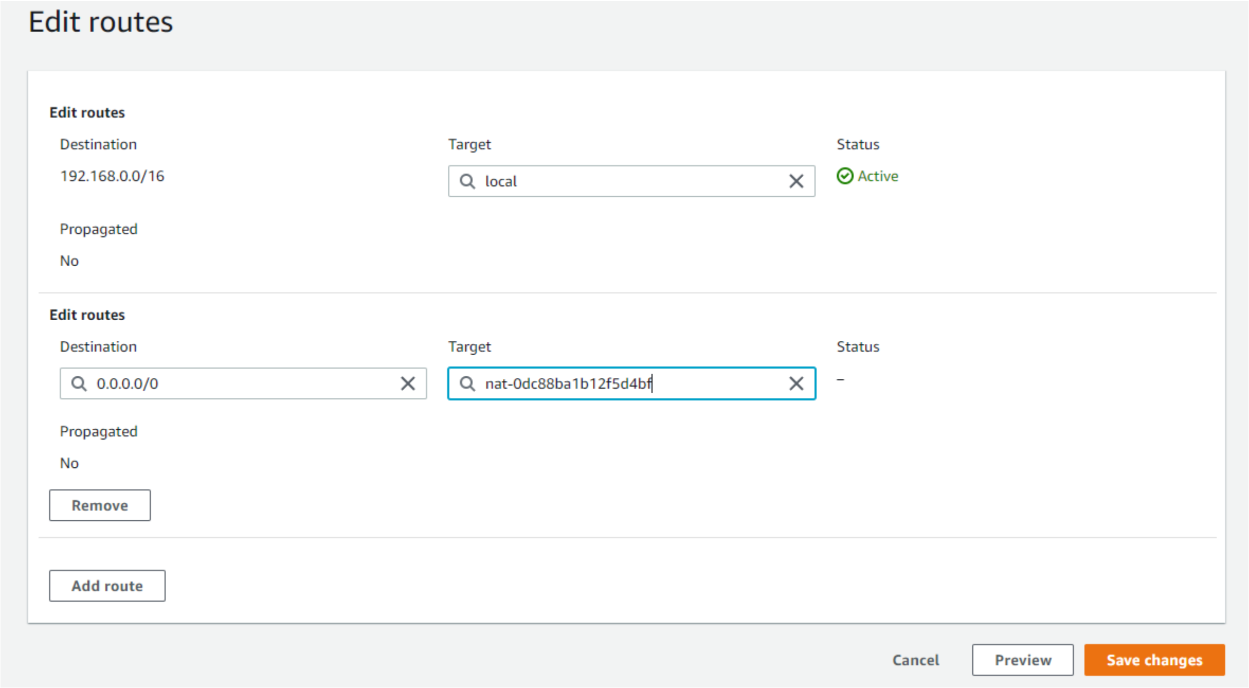
	Name	Route table ID	Explicit subnet associat...	Edge associations	Main
□	–	rtb-010a67db84e50ef44	–	–	Yes
□	lab-public-table	rtb-07fadf542dba89a17	subnet-06bc254b8826c...	–	No
☑	lab-private-table	rtb-079223b43d56c7bf8	3 subnets	–	No
□	–	rtb-0dffa298cf2ccb9c3	–	–	Yes

rtb-079223b43d56c7bf8 / lab-private-table

Routes (1)

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

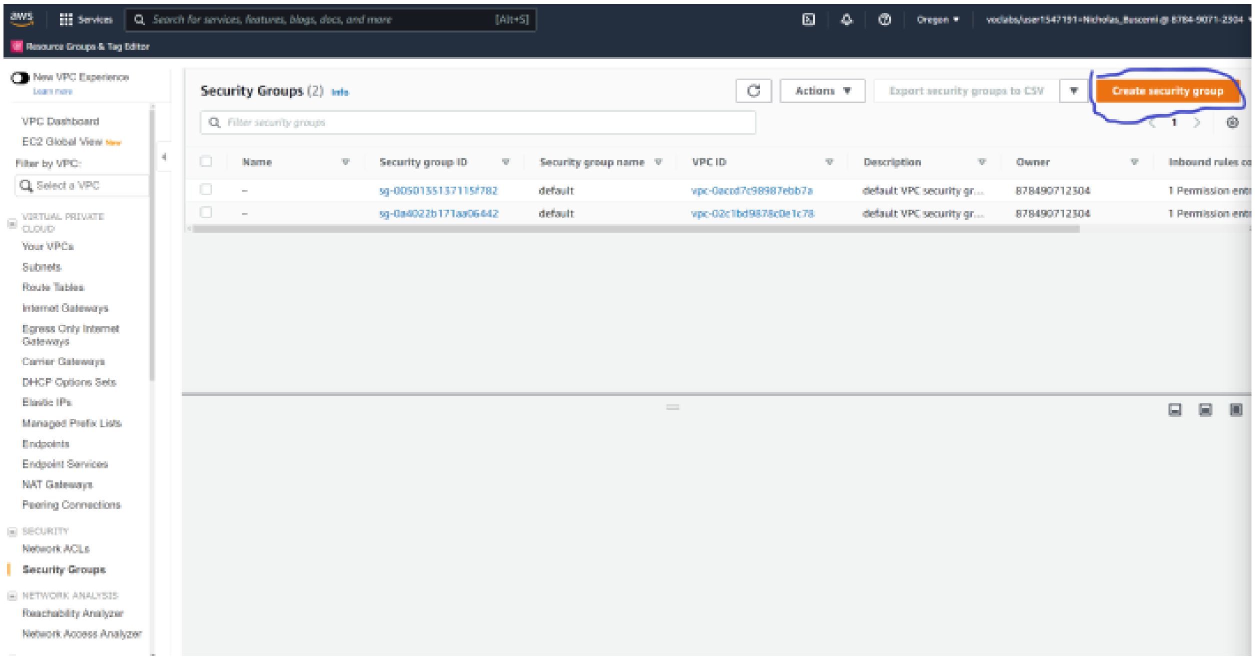
Destination: 0.0.0.0/0

Target: nat-0dc88ba1b12f5d4bf

Status: –

Propagated: No

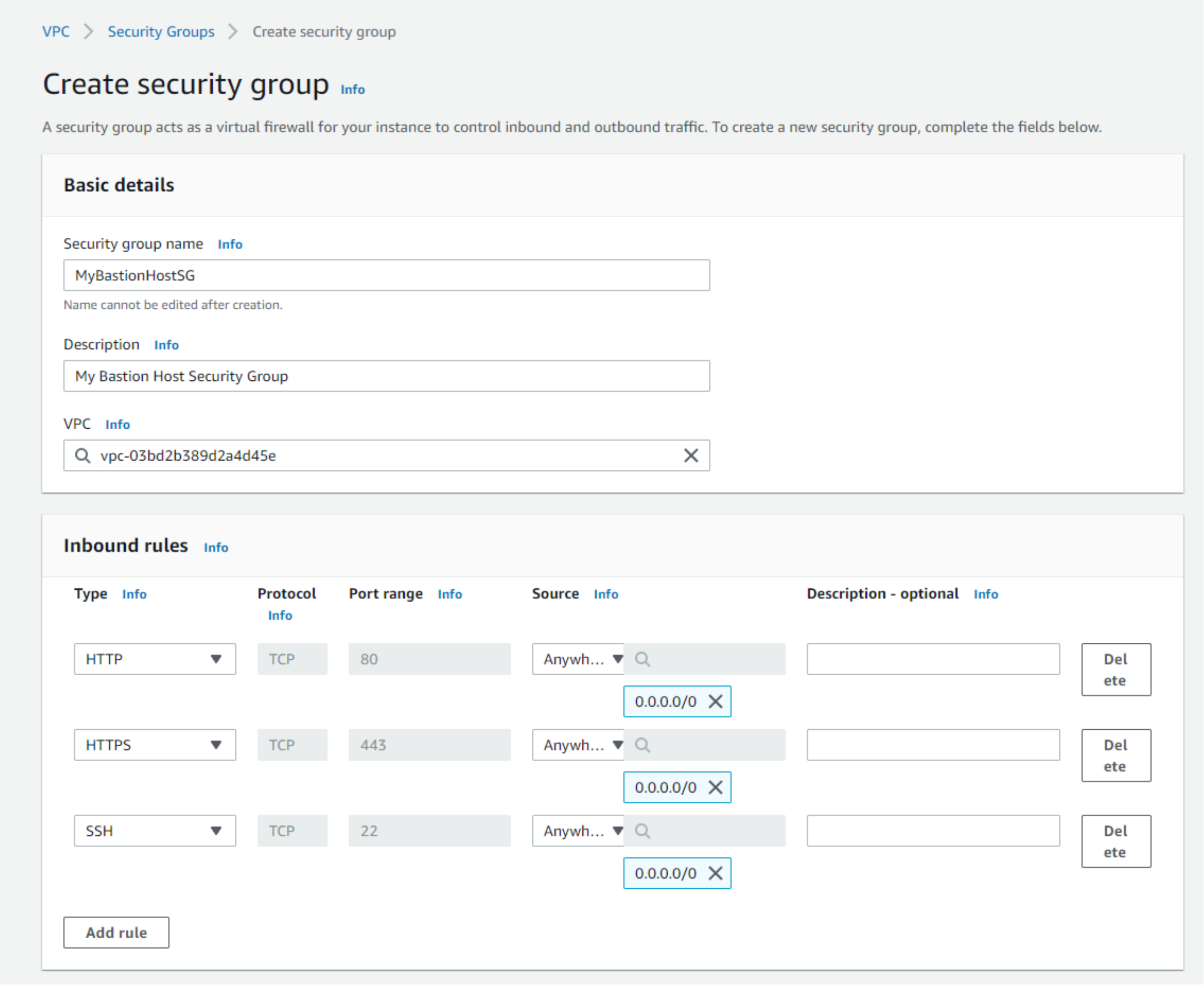
- Now to create our security groups (One for our bastion host, web server, app server, and our database) we will head to Security Groups on the left and click “Create security group”



	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules co
□	–	sg-0050135137115f782	default	vpc-0acd7c98987ebb7a	default VPC security gr...	878490712304	1 Permission entr
□	–	sg-0a4022b171aa06442	default	vpc-02c1bd9878c0e1c78	default VPC security gr...	878490712304	1 Permission entr

- 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



VPC > Security Groups > Create security group

Create security group

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: MyBastionHostSG

Name cannot be edited after creation.

Description: My Bastion Host Security Group

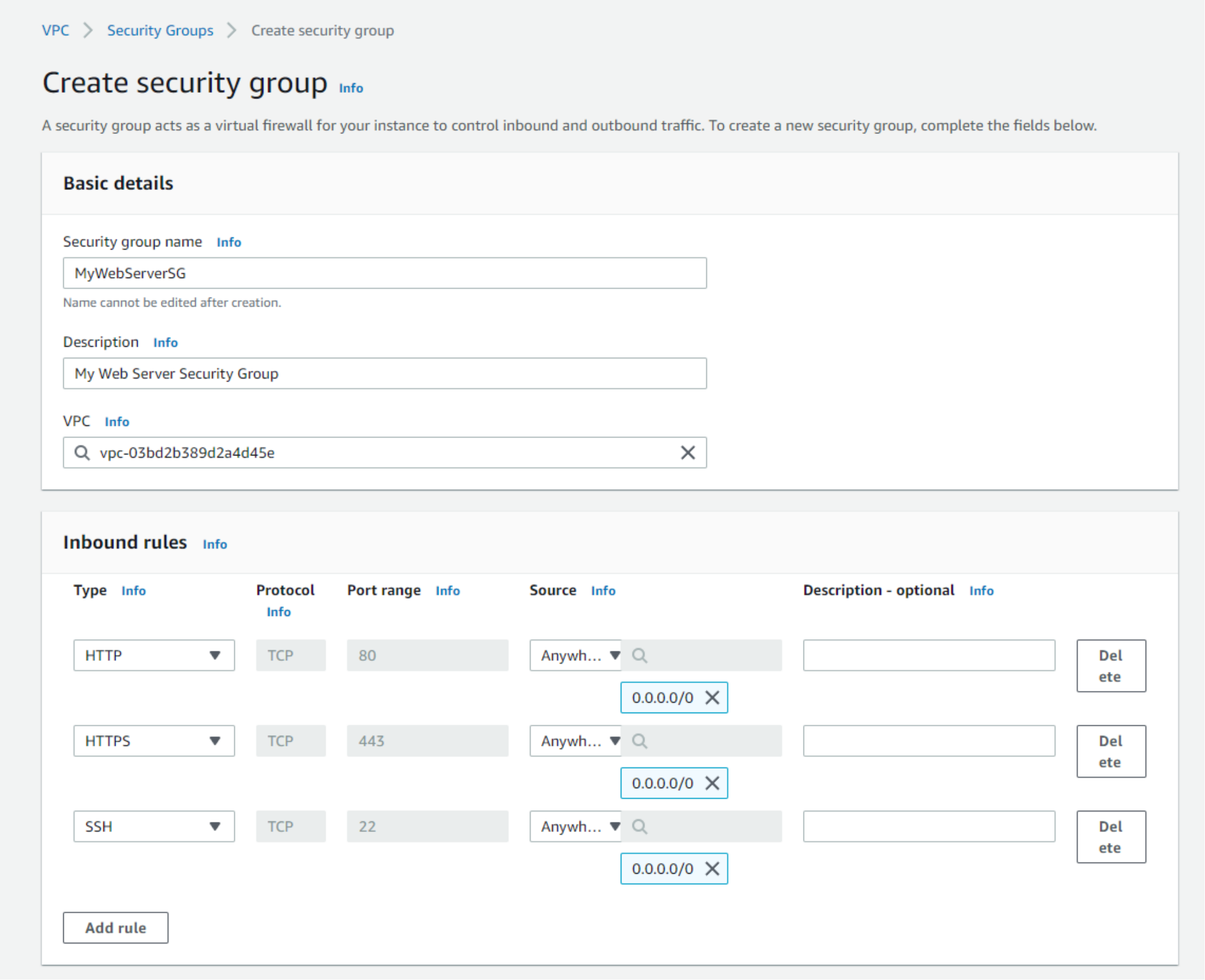
VPC: vpc-03bd2b389d2a4d45e

Inbound rules

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	Anywh... 0.0.0.0/0	
HTTPS	TCP	443	Anywh... 0.0.0.0/0	
SSH	TCP	22	Anywh... 0.0.0.0/0	

- 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
MyWebServerSG
Name cannot be edited after creation.

Description Info
My Web Server Security Group

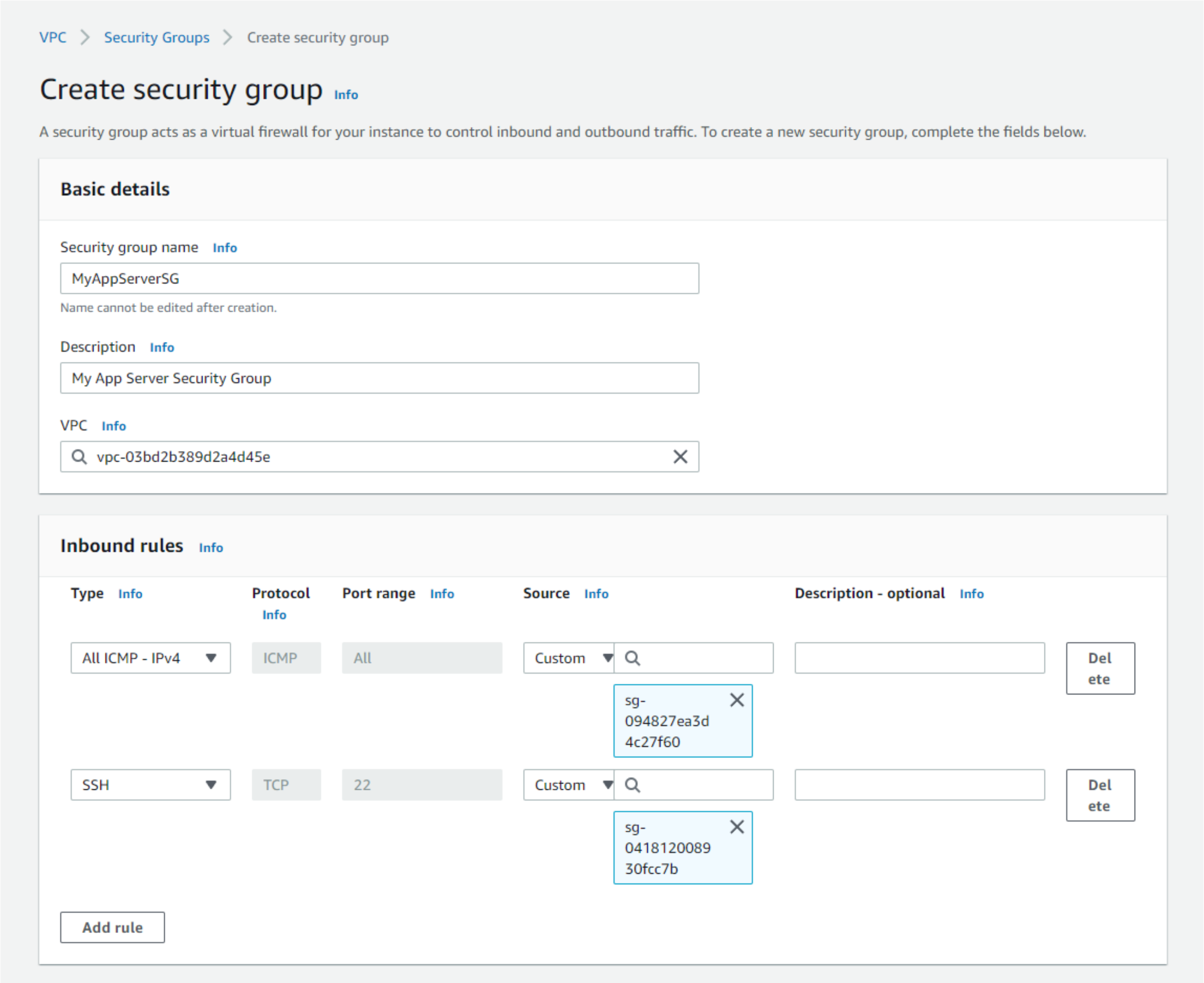
VPC Info
vpc-03bd2b389d2a4d45e

Inbound rules Info

Type	Protocol	Port range	Source	Description - optional	
HTTP	TCP	80	Anywh... 0.0.0.0/0		Delete
HTTPS	TCP	443	Anywh... 0.0.0.0/0		Delete
SSH	TCP	22	Anywh... 0.0.0.0/0		Delete

- 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: MyAppServerSG

Name cannot be edited after creation.

Description Info: My App Server Security Group

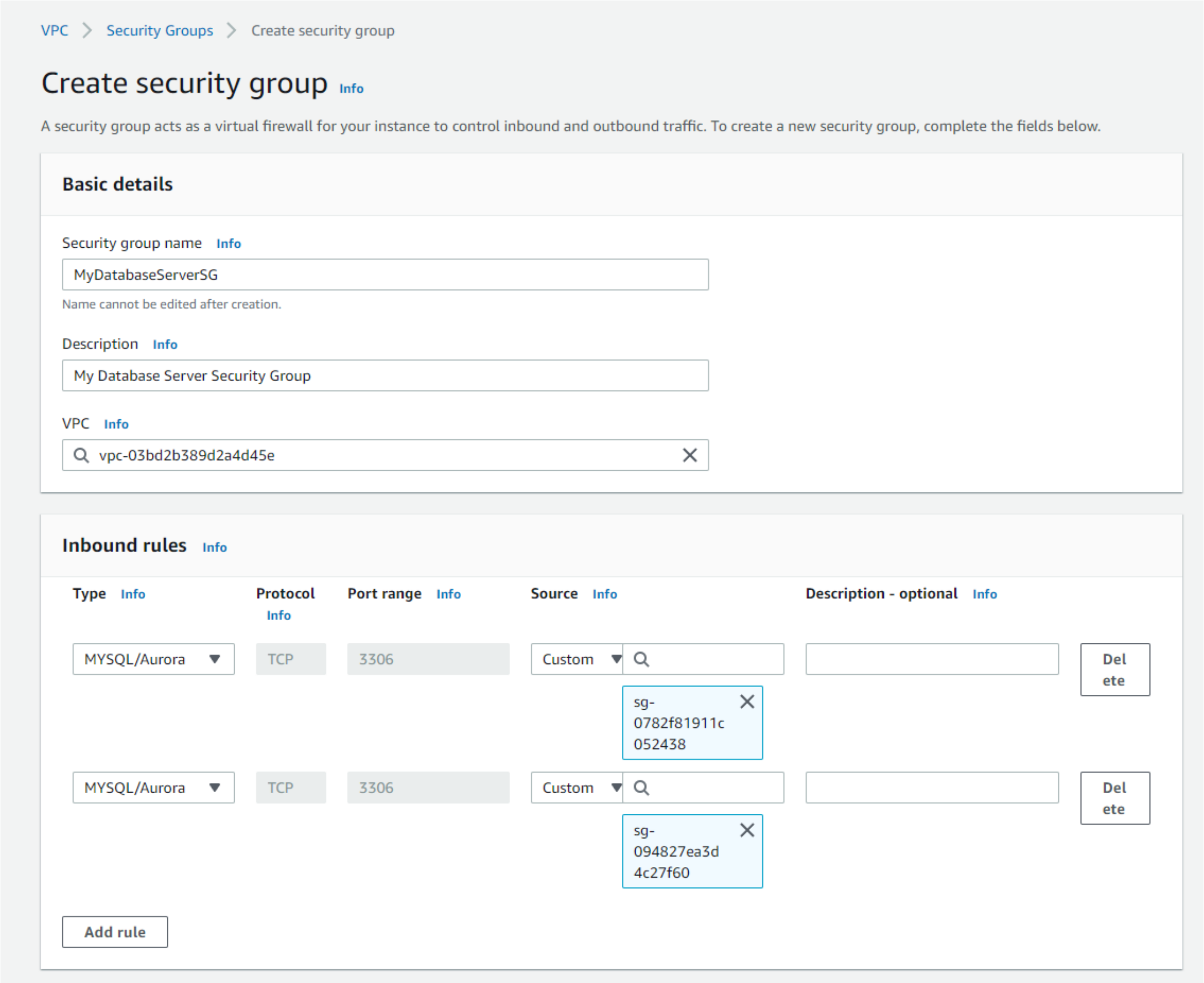
VPC Info: vpc-03bd2b389d2a4d45e

Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
All ICMP - IPv4	ICMP	All	Custom sg-094827ea3d4c27f60		Delete
SSH	TCP	22	Custom sg-041812008930fcc7b		Delete

- 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
MyDatabaseServerSG
Name cannot be edited after creation.

Description Info
My Database Server Security Group

VPC Info
vpc-03bd2b389d2a4d45e

Inbound rules Info

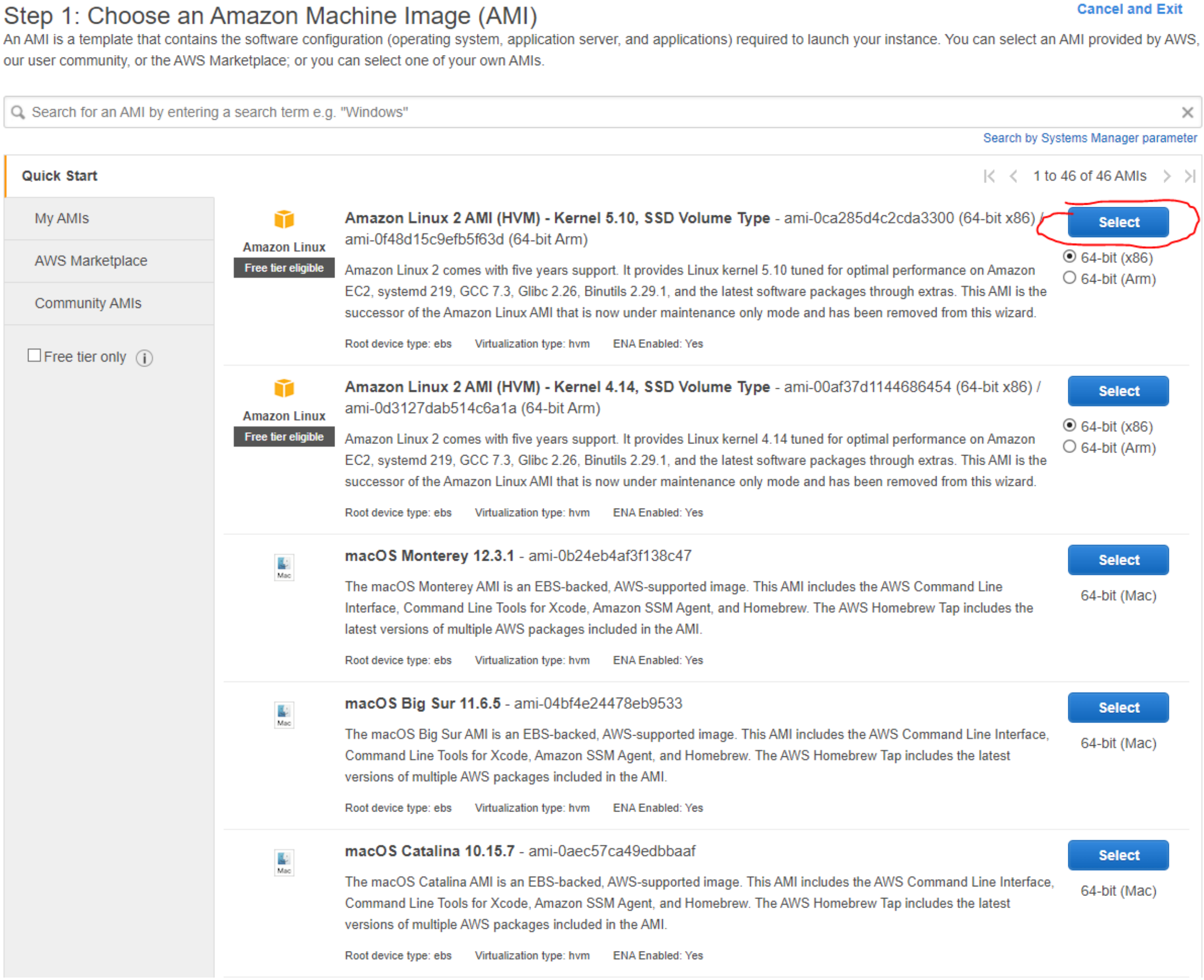
Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
MYSQL/Aurora ▼	TCP	3306	Custom ▼ sg-0782f81911c052438		Delete
MYSQL/Aurora ▼	TCP	3306	Custom ▼ sg-094827ea3d4c27f60		Delete

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

Step 2: Create Servers

- Create Bastion Host

- Select Amazon Linux 2 AMI



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Search for an AMI by entering a search term e.g. "Windows"
Search by Systems Manager parameter
Quick Start
My AMIs
AWS Marketplace
Community AMIs
□ Free tier only
1 to 46 of 46 AMIs

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type - ami-0ca285d4c2cda3300 (64-bit x86) / ami-0f48d15c9efb5f63d (64-bit Arm)

Amazon Linux 2 comes with five years support. It provides Linux kernel 5.10 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is now under maintenance only mode and has been removed from this wizard.

Root device type: ebs   Virtualization type: hvm   ENA Enabled: Yes

Amazon Linux 2 AMI (HVM) - Kernel 4.14, SSD Volume Type - ami-00af37d1144686454 (64-bit x86) / ami-0d3127dab514c6a1a (64-bit Arm)

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is now under maintenance only mode and has been removed from this wizard.

Root device type: ebs   Virtualization type: hvm   ENA Enabled: Yes

macOS Monterey 12.3.1 - ami-0b24eb4af3f138c47

The macOS Monterey AMI is an EBS-backed, AWS-supported image. This AMI includes the AWS Command Line Interface, Command Line Tools for Xcode, Amazon SSM Agent, and Homebrew. The AWS Homebrew Tap includes the latest versions of multiple AWS packages included in the AMI.

Root device type: ebs   Virtualization type: hvm   ENA Enabled: Yes

macOS Big Sur 11.6.5 - ami-04bf4e24478eb9533

The macOS Big Sur AMI is an EBS-backed, AWS-supported image. This AMI includes the AWS Command Line Interface, Command Line Tools for Xcode, Amazon SSM Agent, and Homebrew. The AWS Homebrew Tap includes the latest versions of multiple AWS packages included in the AMI.

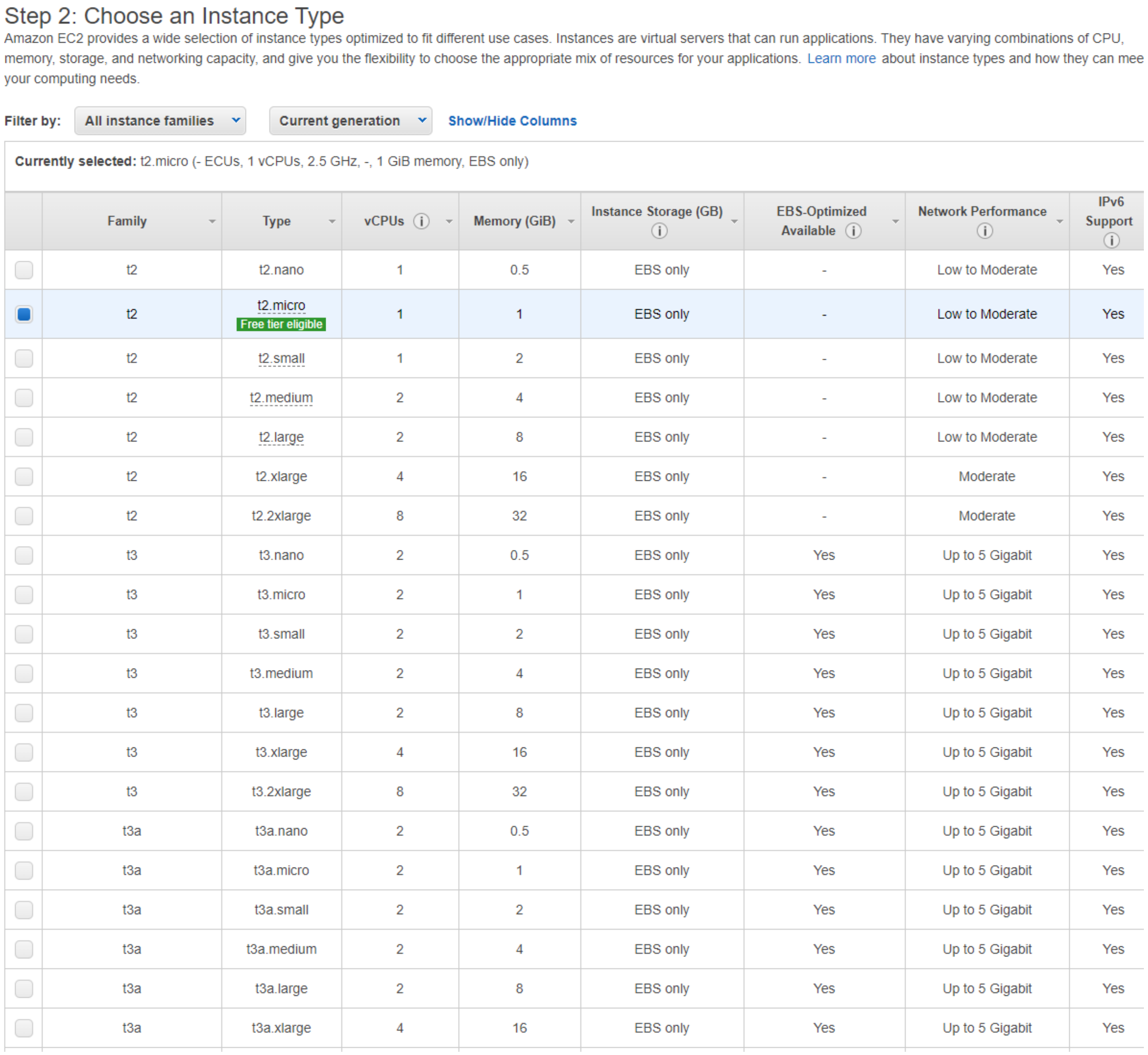
Root device type: ebs   Virtualization type: hvm   ENA Enabled: Yes

macOS Catalina 10.15.7 - ami-0aec57ca49edbbaaf

The macOS Catalina AMI is an EBS-backed, AWS-supported image. This AMI includes the AWS Command Line Interface, Command Line Tools for Xcode, Amazon SSM Agent, and Homebrew. The AWS Homebrew Tap includes the latest versions of multiple AWS packages included in the AMI.

Root device type: ebs   Virtualization type: hvm   ENA Enabled: Yes

- Select t2.micro



Step 2: Choose an Instance Type

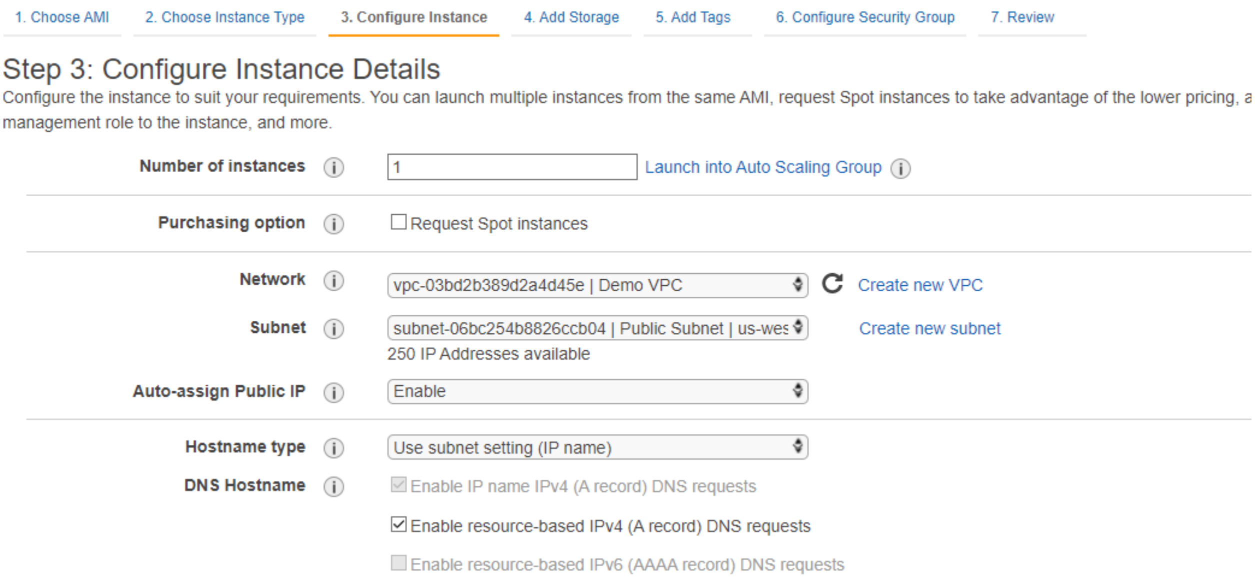
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can mee your computing needs.

Filter by: All instance families ▾ Current generation ▾ Show/Hide Columns

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
☐	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
☑	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
☐	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
☐	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
☐	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
☐	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
☐	t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
☐	t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
☐	t3	t3.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
☐	t3	t3.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes
☐	t3	t3.medium	2	4	EBS only	Yes	Up to 5 Gigabit	Yes
☐	t3	t3.large	2	8	EBS only	Yes	Up to 5 Gigabit	Yes
☐	t3	t3.xlarge	4	16	EBS only	Yes	Up to 5 Gigabit	Yes
☐	t3	t3.2xlarge	8	32	EBS only	Yes	Up to 5 Gigabit	Yes
☐	t3a	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
☐	t3a	t3a.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
☐	t3a	t3a.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes
☐	t3a	t3a.medium	2	4	EBS only	Yes	Up to 5 Gigabit	Yes
☐	t3a	t3a.large	2	8	EBS only	Yes	Up to 5 Gigabit	Yes
☐	t3a	t3a.xlarge	4	16	EBS only	Yes	Up to 5 Gigabit	Yes

- Put in your VPC and Public Subnet and enable auto assign public IP



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, a management role to the instance, and more.

Number of instances 1 Launch into Auto Scaling Group

Purchasing option □ Request Spot instances

Network vpc-03bd2b389d2a4d45e | Demo VPC Create new VPC

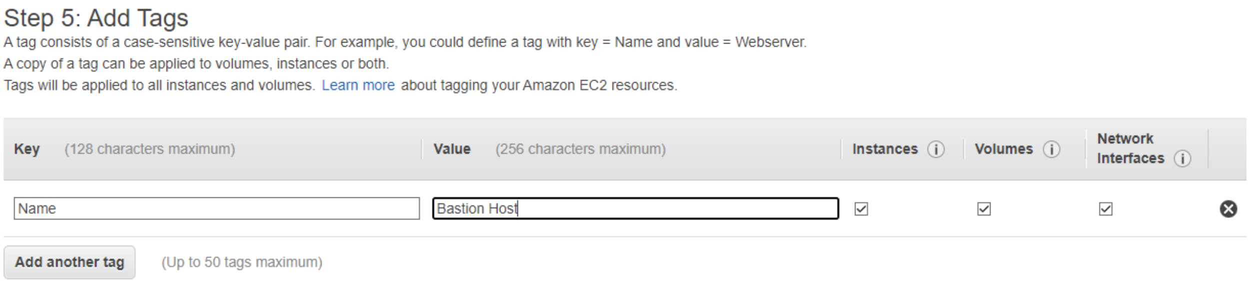
Subnet subnet-06bc254b8826ccb04 | Public Subnet | us-wes Create new subnet
250 IP Addresses available

Auto-assign Public IP Enable

Hostname type Use subnet setting (IP name)

DNS Hostname ☑ Enable IP name IPv4 (A record) DNS requests
☑ Enable resource-based IPv4 (A record) DNS requests
□ Enable resource-based IPv6 (AAAA record) DNS requests

- Storage leave default
- Add a name tag to let you know this is the Bastion Host

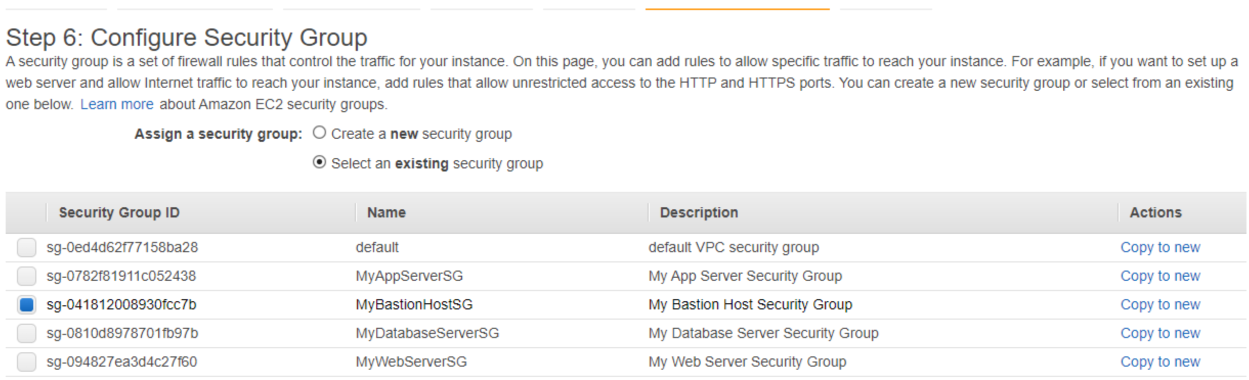


Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes	Network Interfaces	
Name	Bastion Host	☑	☑	☑	⊗

- Select an existing group and select your Bastion Host SG



Step 6: Configure Security Group

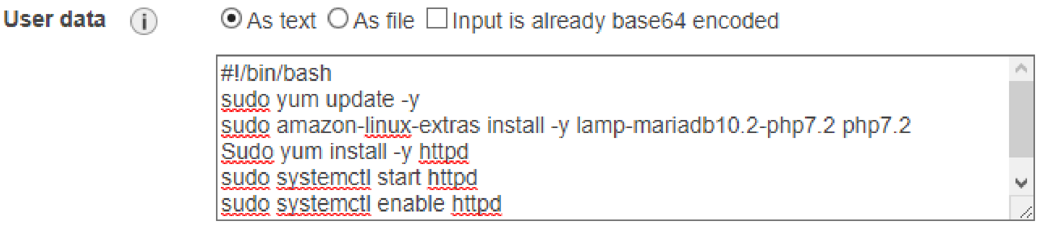
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ○ Create a **new** security group
● Select an **existing** security group

	Security Group ID	Name	Description	Actions
□	sg-0ed4d62f77158ba28	default	default VPC security group	Copy to new
□	sg-0782f81911c052438	MyAppServerSG	My App Server Security Group	Copy to new
☑	sg-041812008930fcc7b	MyBastionHostSG	My Bastion Host Security Group	Copy to new
□	sg-0810d8978701fb97b	MyDatabaseServerSG	My Database Server Security Group	Copy to new
□	sg-094827ea3d4c27f60	MyWebServerSG	My Web Server Security Group	Copy to new

- Launch and choose an existing keypair. This can be downloaded from the lab page
- To make the Web Server follow the same steps until you get to Step 3
- Follow along like previously and change your network, subnet, and enable auto assign public ip
- Then go to user data and type this into it to set up the web server
  - #!/bin/bash
  - sudo yum update -y

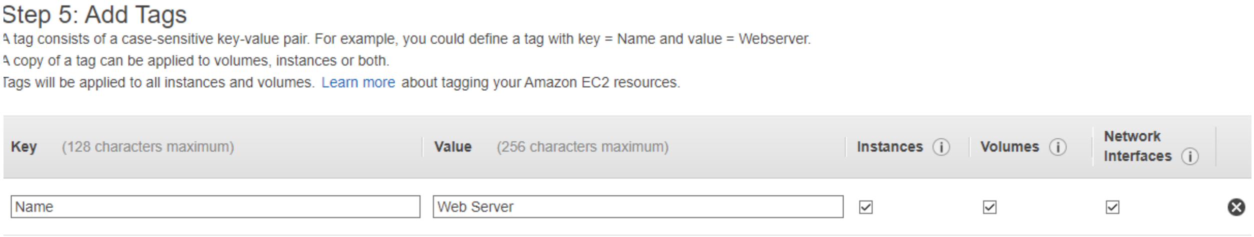
- sudo amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
- Sudo yum install -y httpd
- sudo systemctl start httpd
- sudo systemctl enable httpd



User data ● As text ○ As file □ Input is already base64 encoded

```
#!/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
```

- Storage leave default
- Give it a name tag letting you know it is the Web Server

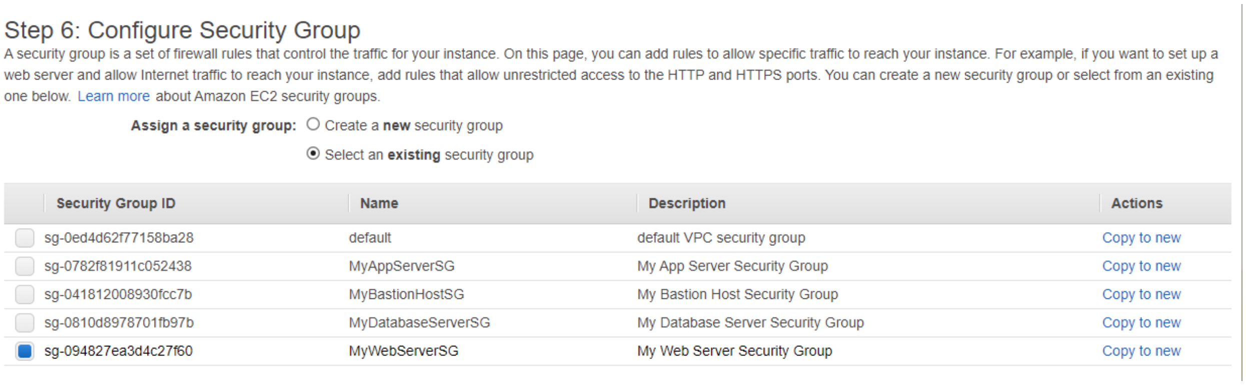


Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes	Network Interfaces
Name	Web Server	☑	☑	☑

- Select an existing security group and select your web server SG



Step 6: Configure Security Group

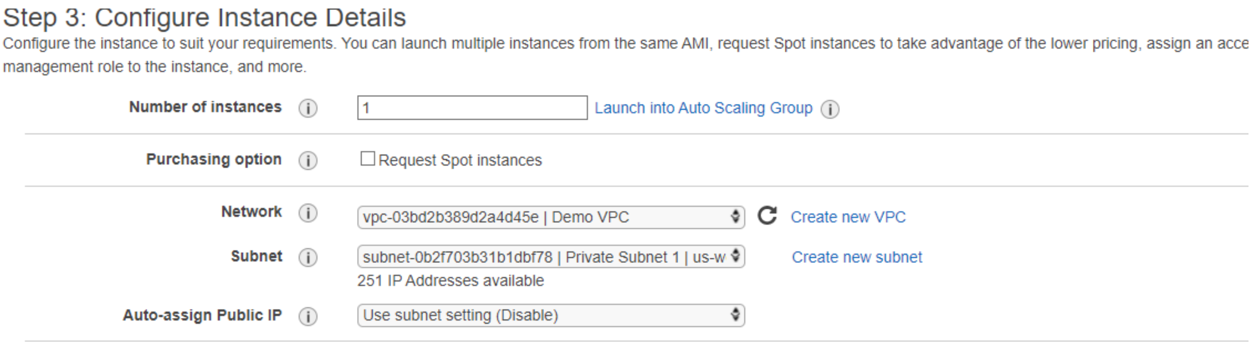
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ○ Create a **new** security group
● Select an **existing** security group

	Security Group ID	Name	Description	Actions
□	sg-0ed4d62f77158ba28	default	default VPC security group	Copy to new
□	sg-0782f81911c052438	MyAppServerSG	My App Server Security Group	Copy to new
□	sg-041812008930fcc7b	MyBastionHostSG	My Bastion Host Security Group	Copy to new
□	sg-0810d8978701fb97b	MyDatabaseServerSG	My Database Server Security Group	Copy to new
☑	sg-094827ea3d4c27f60	MyWebServerSG	My Web Server Security Group	Copy to new

- Just like before launch and use the existing keypair

- Follow the same steps once again to create the app server until you get to step 3
- Put in your VPC and then choose Private Subnet 1 for the subnet and leave auto assign public ip disabled

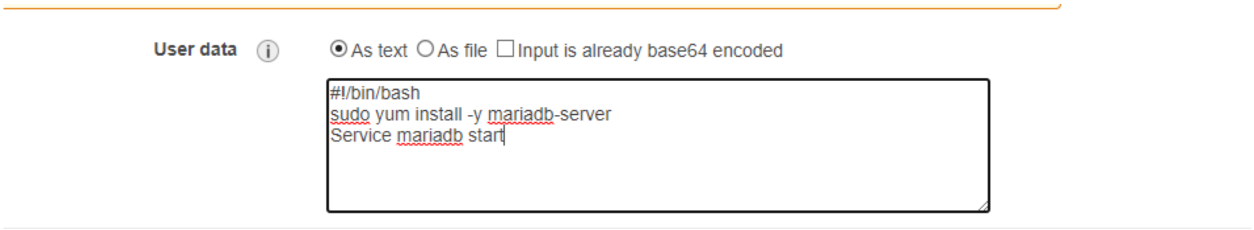


Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an acce management role to the instance, and more.

Number of instances ⓘ	1 Launch into Auto Scaling Group ⓘ
Purchasing option ⓘ	☐ Request Spot instances
Network ⓘ	vpc-03bd2b389d2a4d45e | Demo VPC ⟳ Create new VPC
Subnet ⓘ	subnet-0b2f703b31b1dbf78 | Private Subnet 1 | us-w Create new subnet 251 IP Addresses available
Auto-assign Public IP ⓘ	Use subnet setting (Disable)

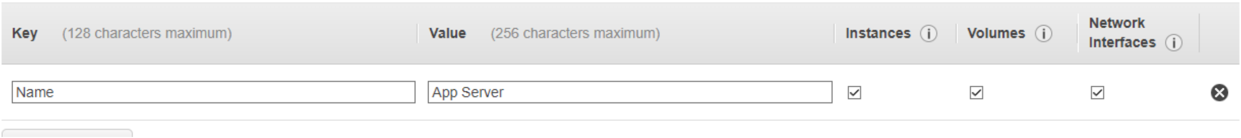
- Then go into metadata and type this out to set up a database server on our app server
  - #!/bin/bash
  - sudo yum install -y mariadb-server
  - Sudo service mariadb start (note that the image is incorrect, make sure to add sudo)



User data ⓘ ● As text ○ As file ☐ Input is already base64 encoded

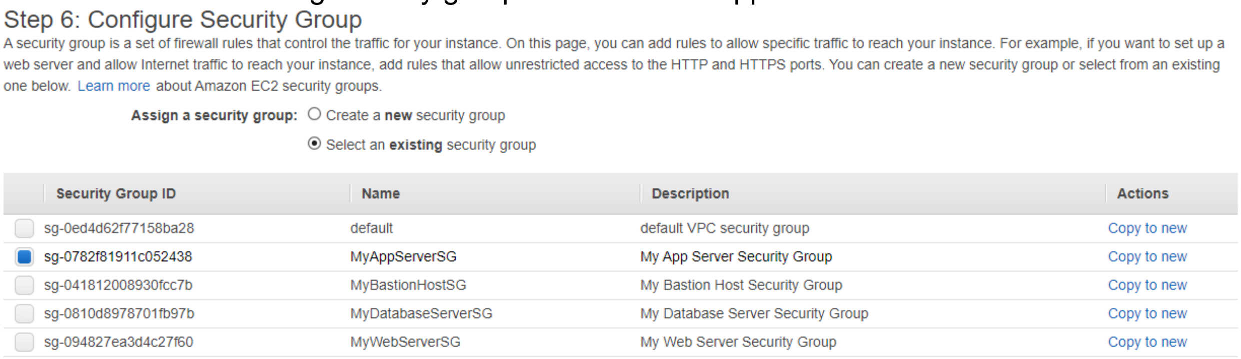
```
#!/bin/bash
sudo yum install -y mariadb-server
Service mariadb start
```

- Give it a name letting you know it is the App Server



Key (128 characters maximum)	Value (256 characters maximum)	Instances ⓘ	Volumes ⓘ	Network Interfaces ⓘ	
Name	App Server	☑	☑	☑	⊗

- Select an existing security group and select the app server SG



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ○ Create a **new** security group

● Select an **existing** security group

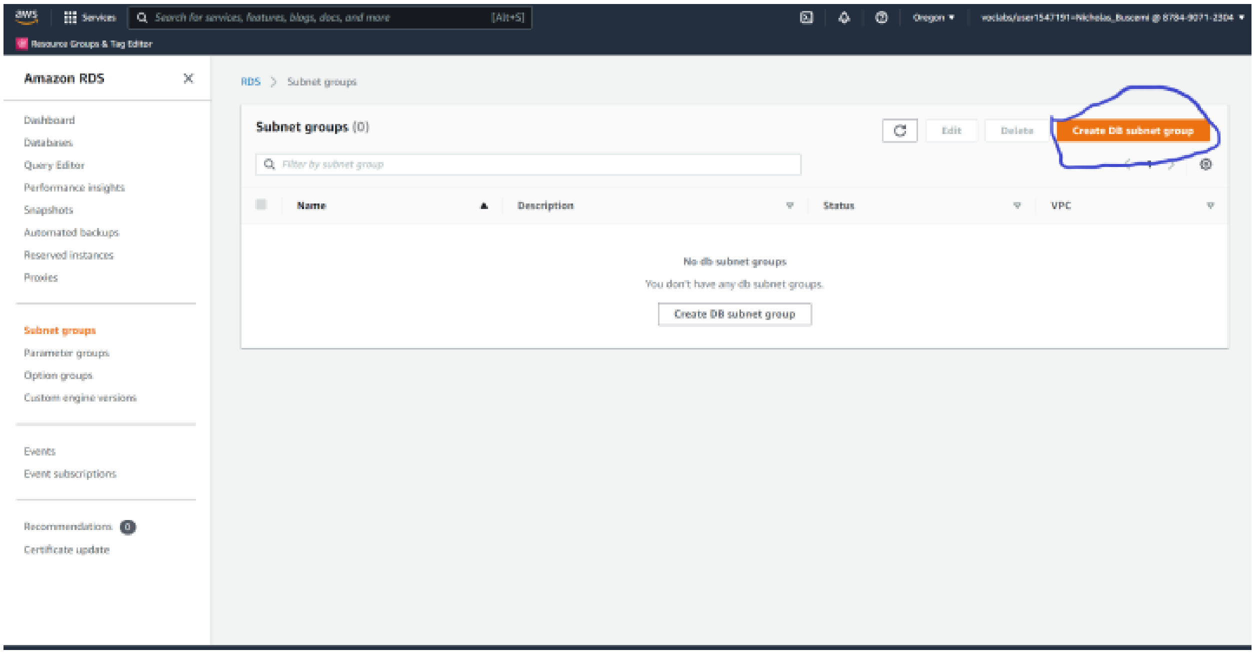
	Security Group ID	Name	Description	Actions
☐	sg-0ed4d62f77158ba28	default	default VPC security group	Copy to new
☑	sg-0782f81911c052438	MyAppServerSG	My App Server Security Group	Copy to new
☐	sg-041812008930fcc7b	MyBastionHostSG	My Bastion Host Security Group	Copy to new
☐	sg-0810d8978701fb97b	MyDatabaseServerSG	My Database Server Security Group	Copy to new
☐	sg-094827ea3d4c27f60	MyWebServerSG	My Web Server Security Group	Copy to new

- Just like before launch and use the existing keypair

Step 3: Create a Database

- Create a DB subnet group by first heading to the Amazon RDS service page on the AWS management console

- Click on Subnet Groups on the left hand side and the click on “Create DB subnet group”

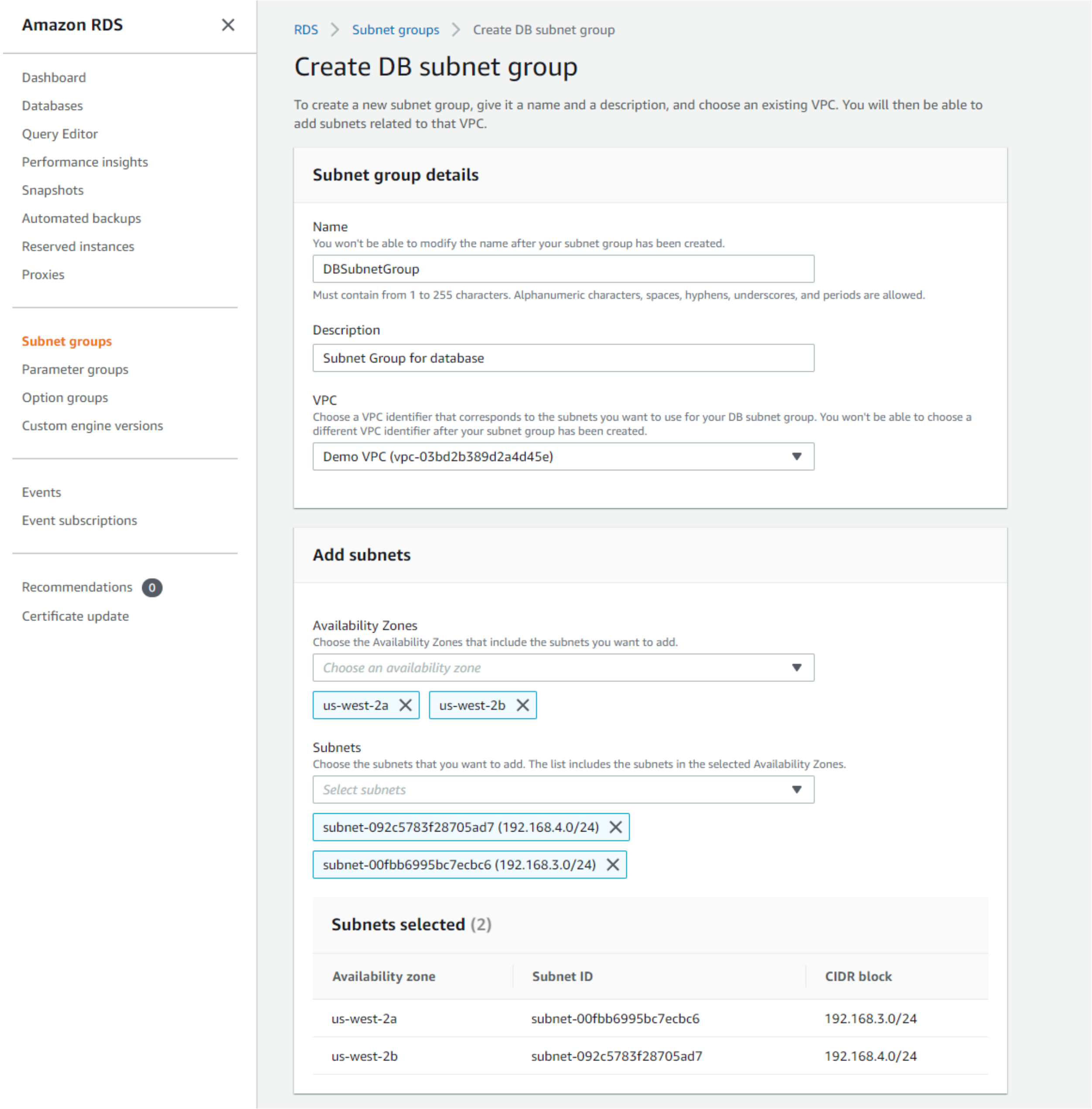


No db subnet groups

You don't have any db subnet groups.

- 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



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

Description
Subnet Group for database

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.
Demo VPC (vpc-03bd2b389d2a4d45e)

Add subnets

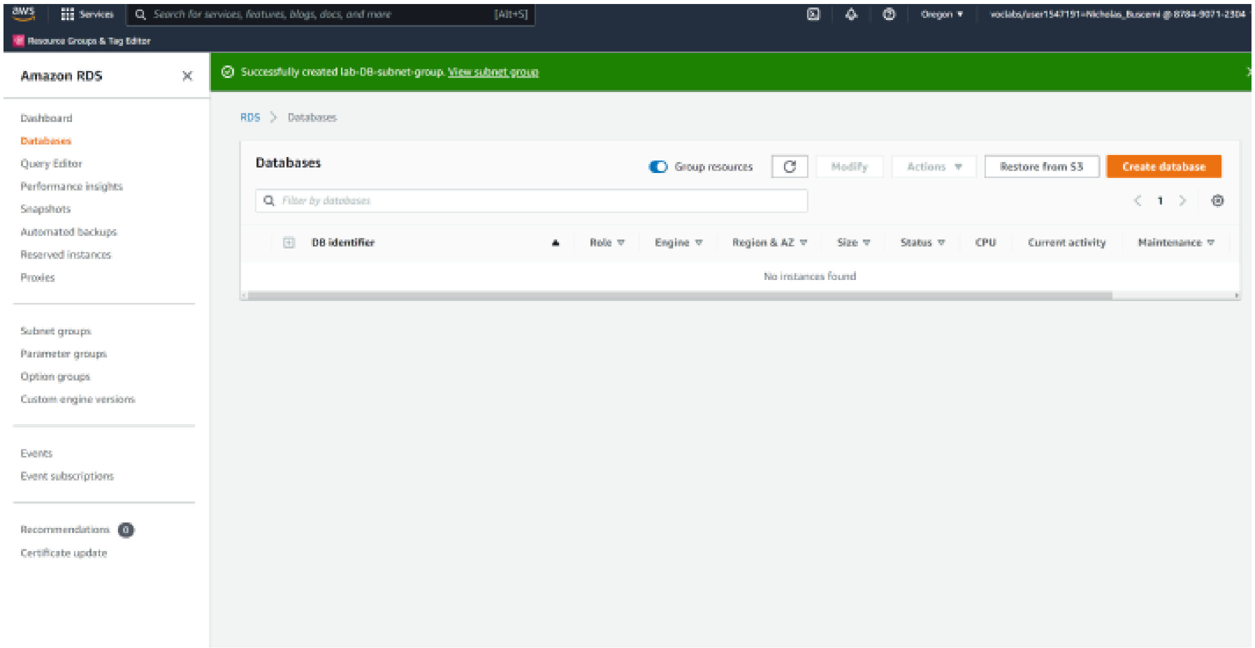
Availability Zones
Choose the Availability Zones that include the subnets you want to add.
Choose an availability zone
us-west-2a
us-west-2b

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

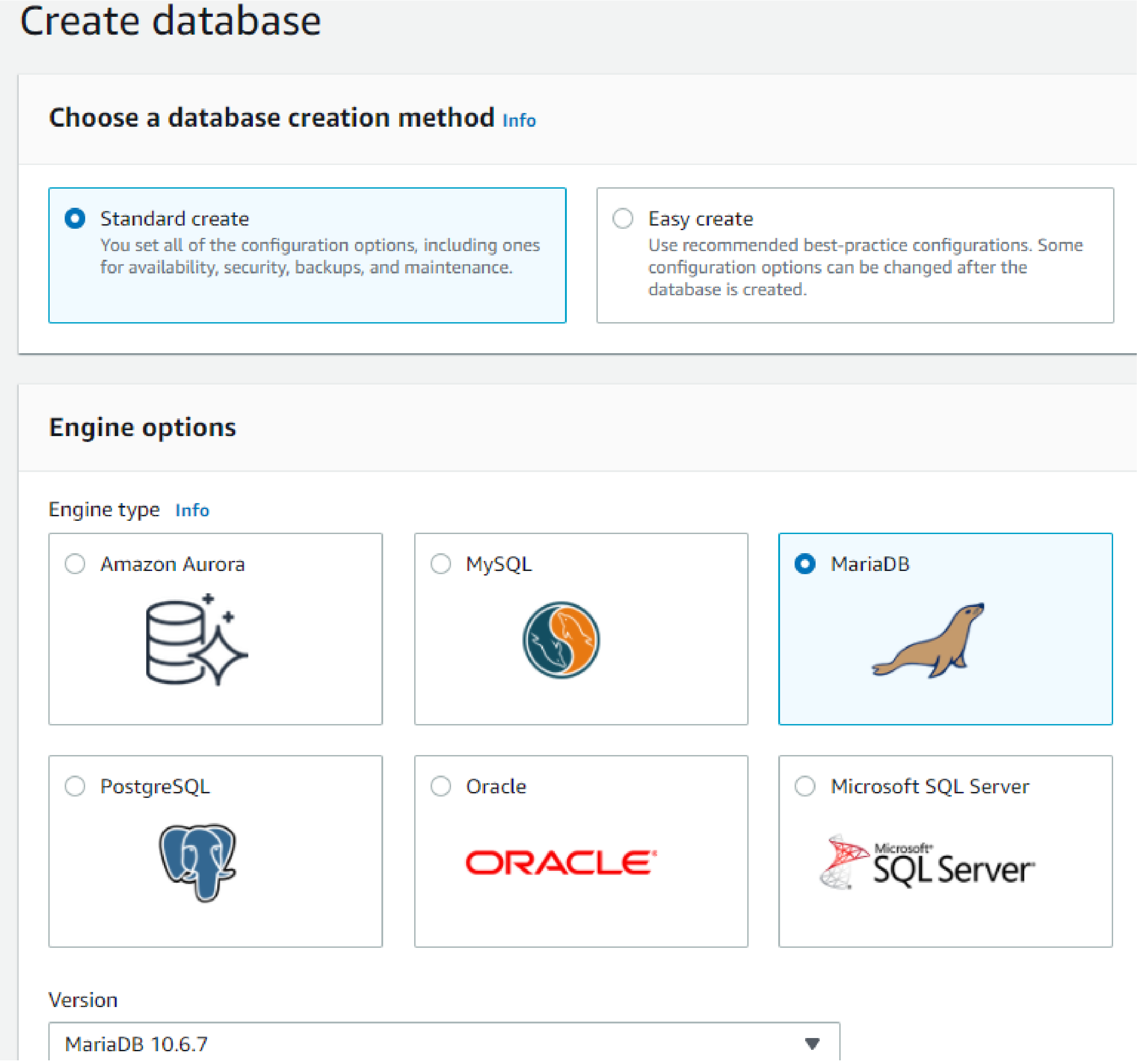


Successfully created lab-DB-subnet-group. View subnet group

Databases

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

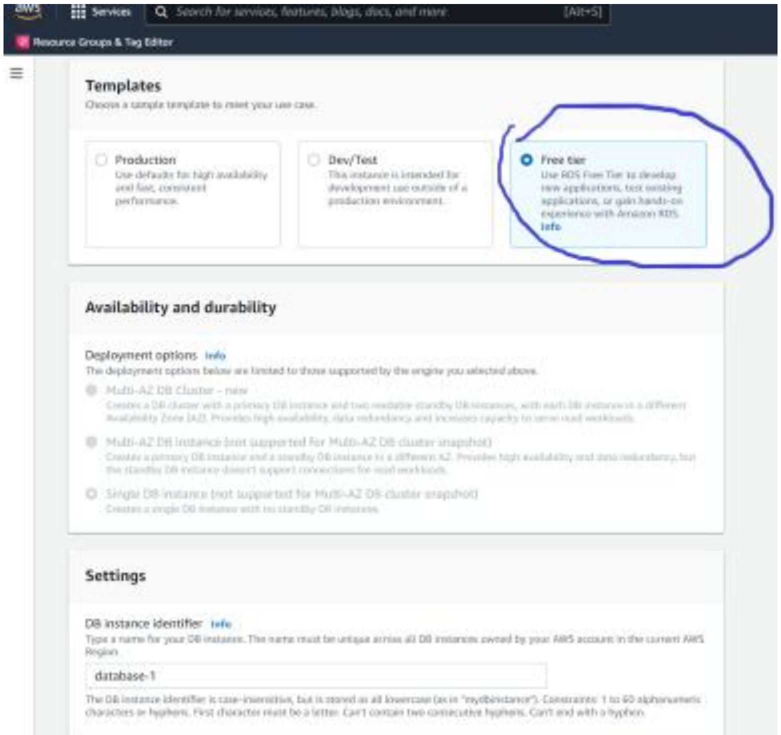
○ Oracle

○ Microsoft SQL Server

Version

MariaDB 10.6.7 ▼

- Make sure you click on Free tier here


aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Resource Groups & Tag Editor

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 instance.

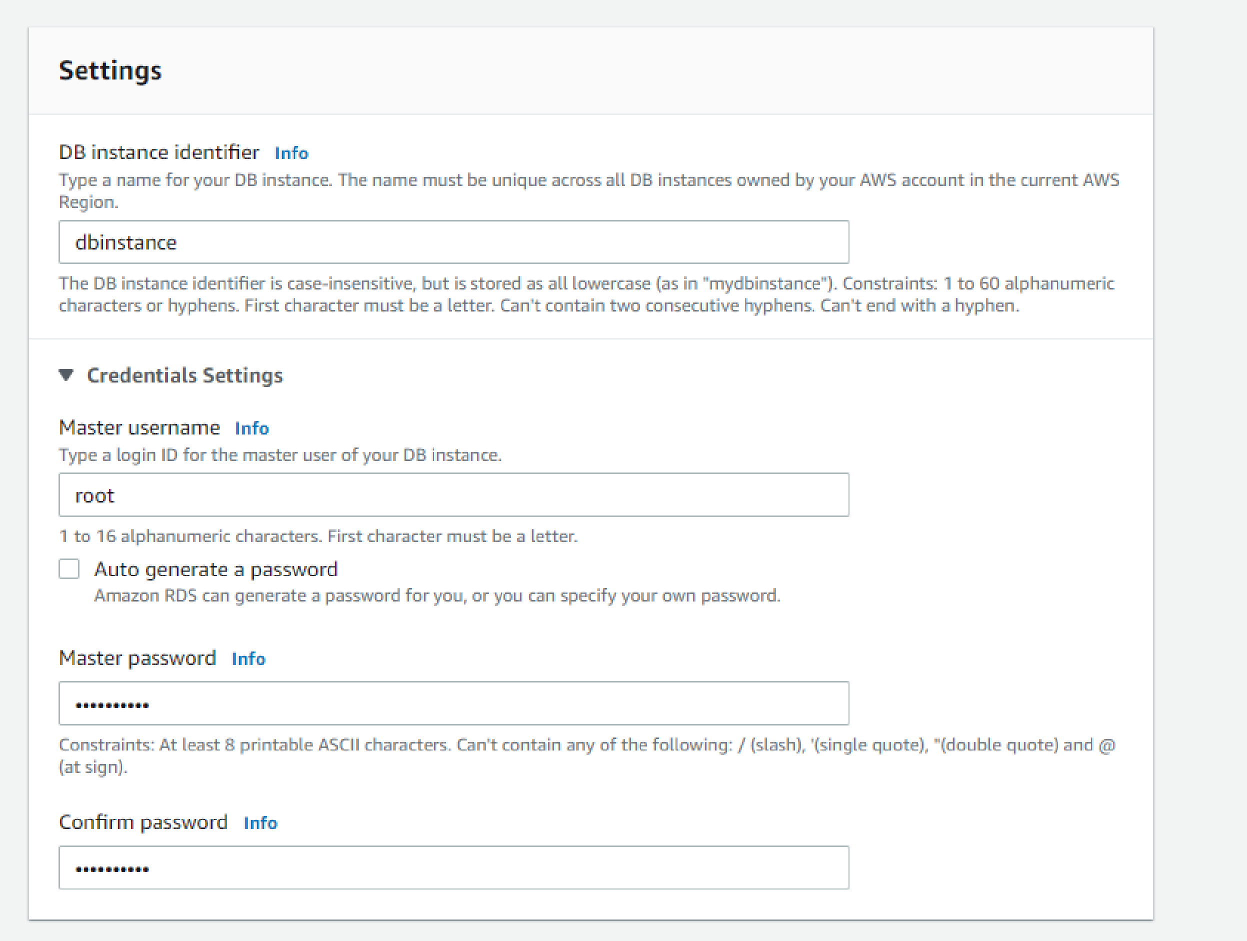
Settings

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.

database-1

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.

dbinstance

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.

root

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

••••••••••

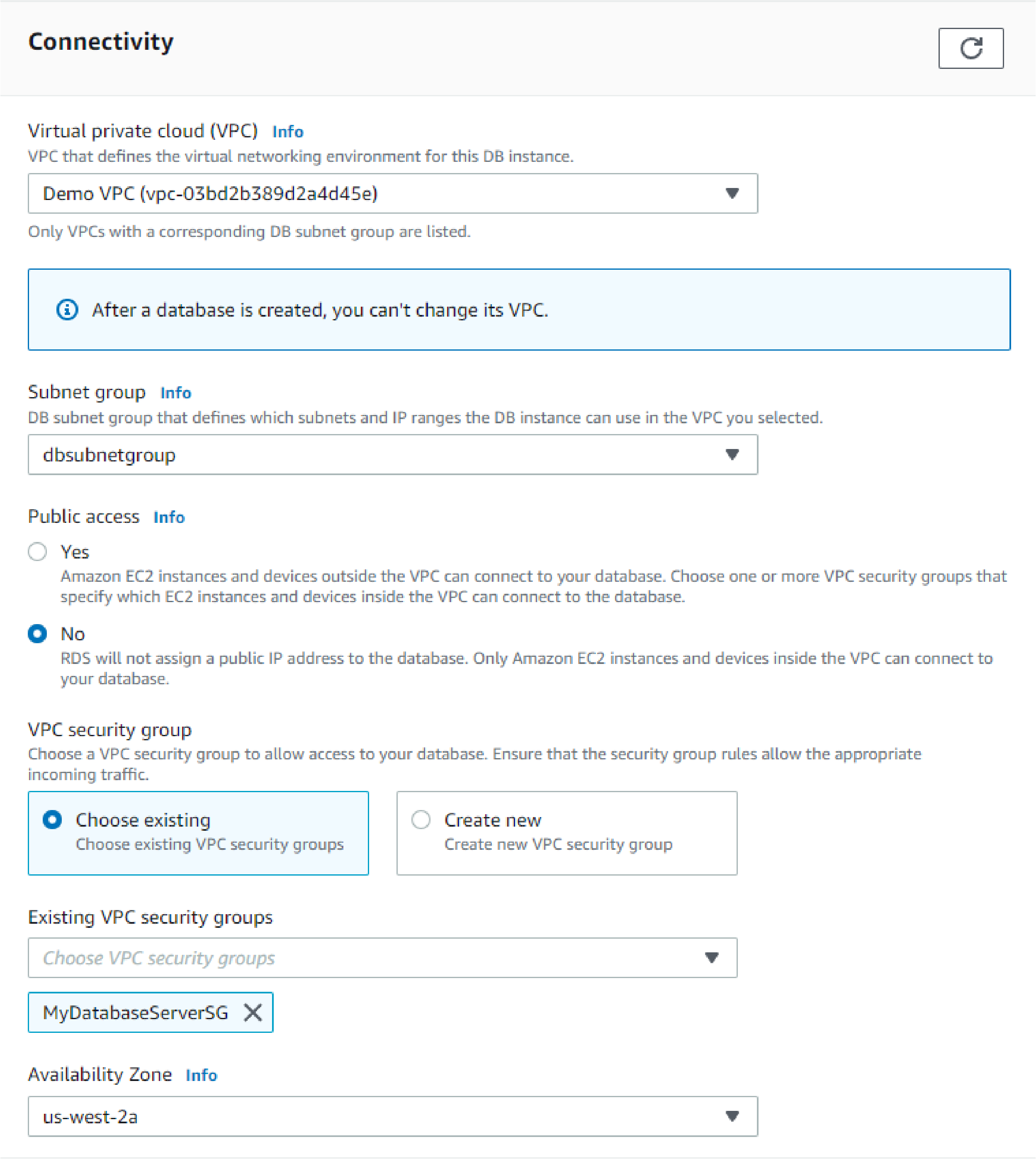
Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), '(single quote), "(double quote) and @ (at sign).

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

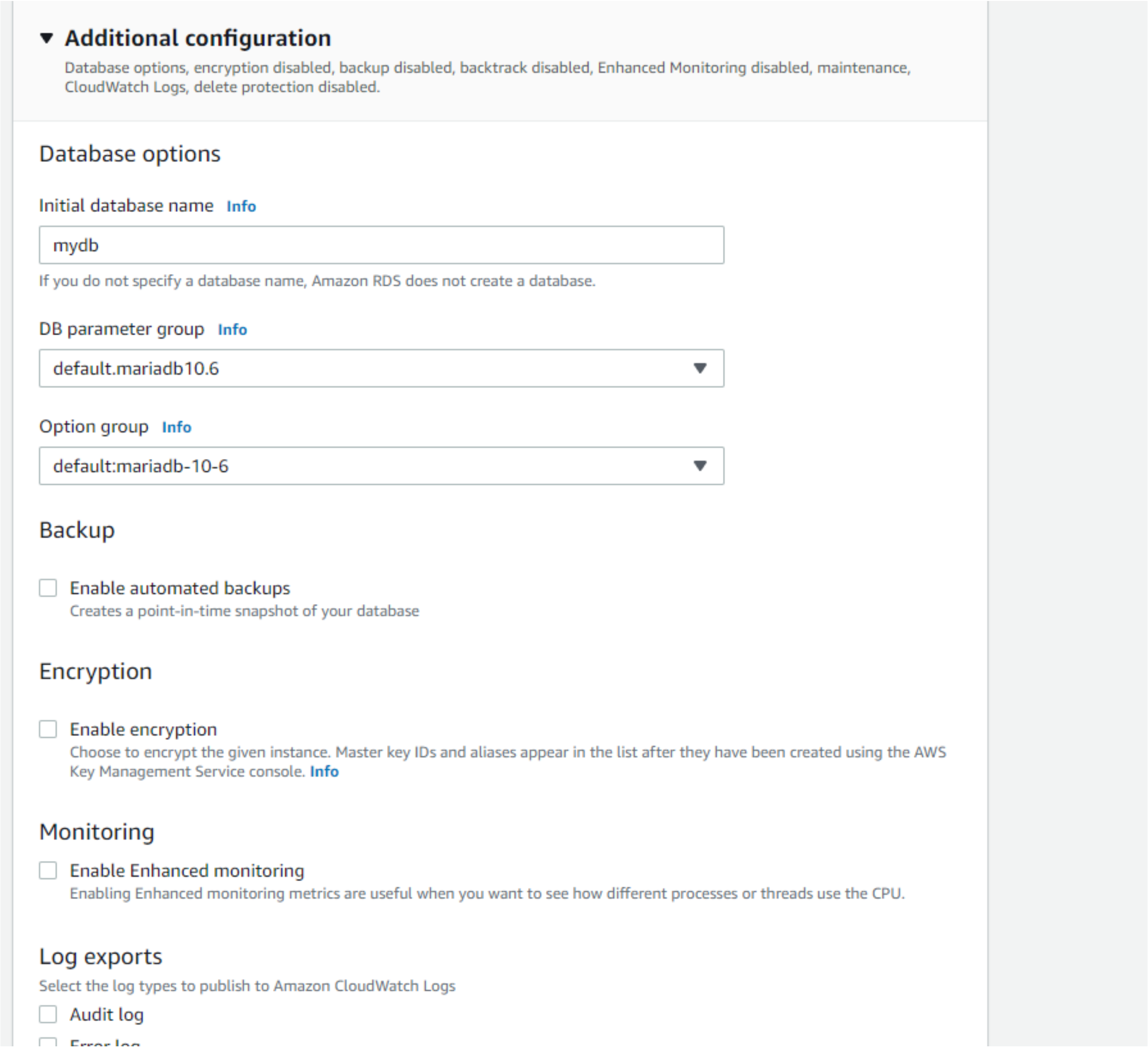
MyDatabaseServerSG ✕

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

mydb

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

DB parameter group Info

default.mariadb10.6 ▼

Option group Info

default:mariadb-10-6 ▼

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.

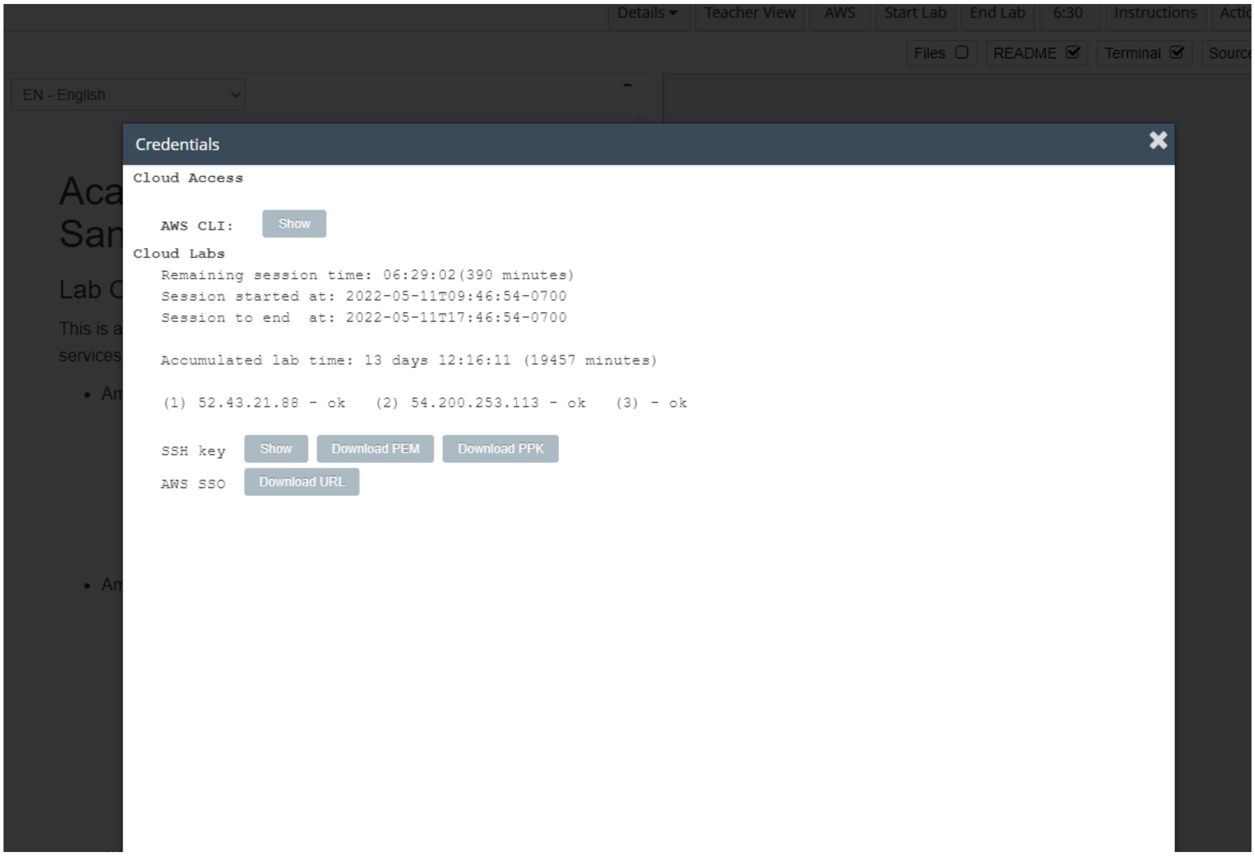
Log exports

Select the log types to publish to Amazon CloudWatch Logs

□ Audit log
□ Error log

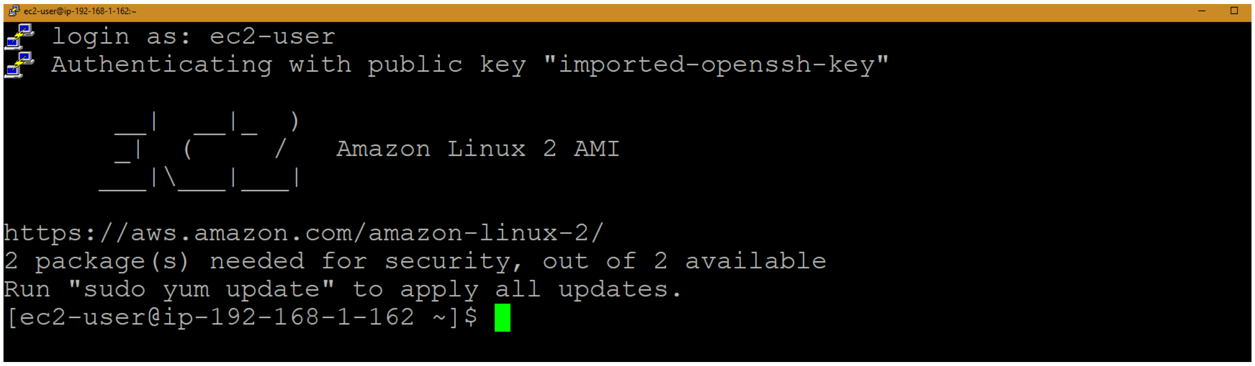
Step 4: Test connections

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



Credentials

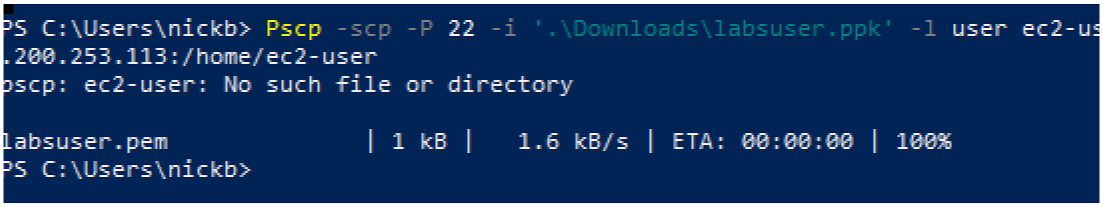
```
Cloud Access

   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
```



```
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 ~]$ 
```

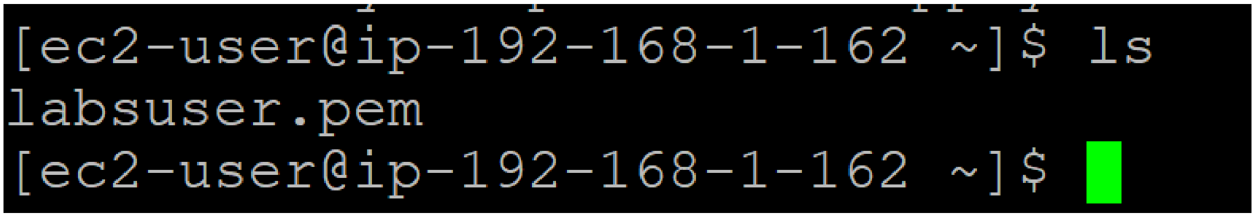
- This is for windows only as I only have a windows machine to work on, sorry mac and linux users
- Go into your powershell and type this command out
    - Pscp -scp -P 22 -i ’.\Downloads\labsuser.ppk’ -| user ec2-user ‘.\Downloads\labsuser.pem’ ec2-user@bastion-host-public-ip:/home/ec2-user

    - Replace bastion-host-public-ip with the public ip address of your bastion host
- Hit enter and it should upload those keys to your bastion host for use on other servers



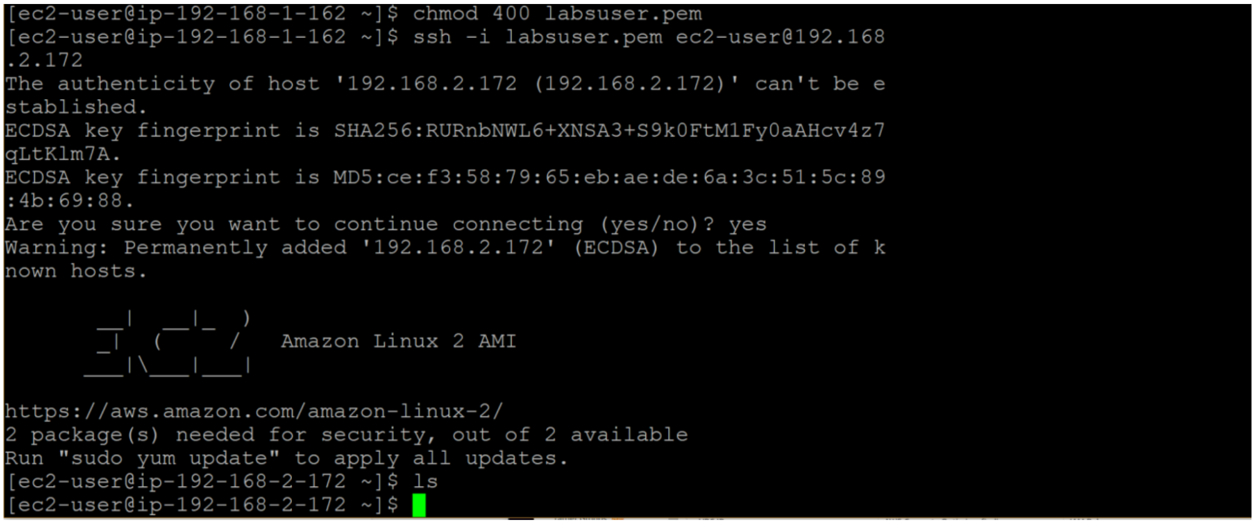
```
PS C:\Users\nickb> Pscp -scp -P 22 -i '.\Downloads\labsuser.ppk' -l user ec2-us
.200.253.113:/home/ec2-user
pscp: ec2-user: No such file or directory

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

- Test on your ssh to see if the file is uploaded by using ls. Should return something like this



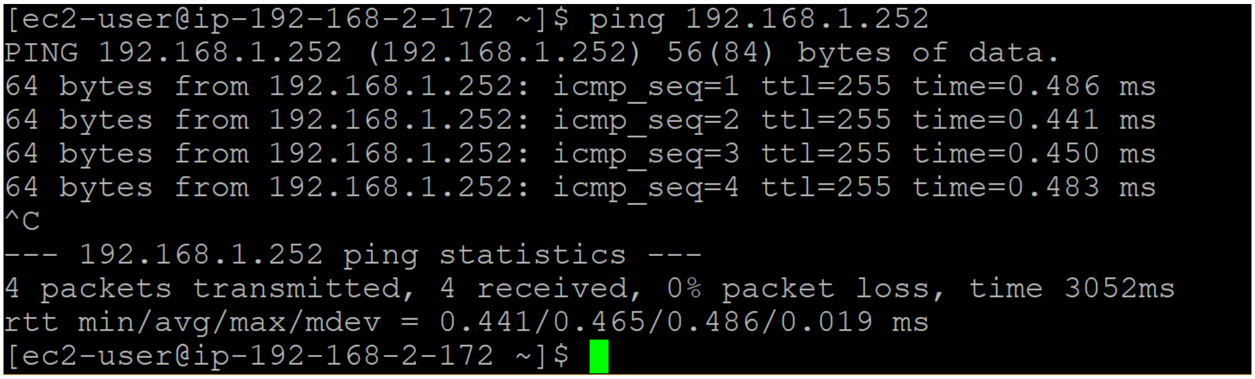
```
[ec2-user@ip-192-168-1-162 ~]$ ls
labsuser.pem
[ec2-user@ip-192-168-1-162 ~]$ 
```

- Change file permissions for the file we just downloaded to our bastion host by typing
    - chmod 400 labsuser.pem
- Then ssh into our app server by typing
    - ssh -i my-key-pair.pem ec2-user@app-server-private-ip
    - Replace my-key-pair with the name of your key
    - Replace app-server-private-ip with your app server’s private ip address
- Type yes when it prompts you to
- Use ls to see that you are now ssh into a different server since there is no more key



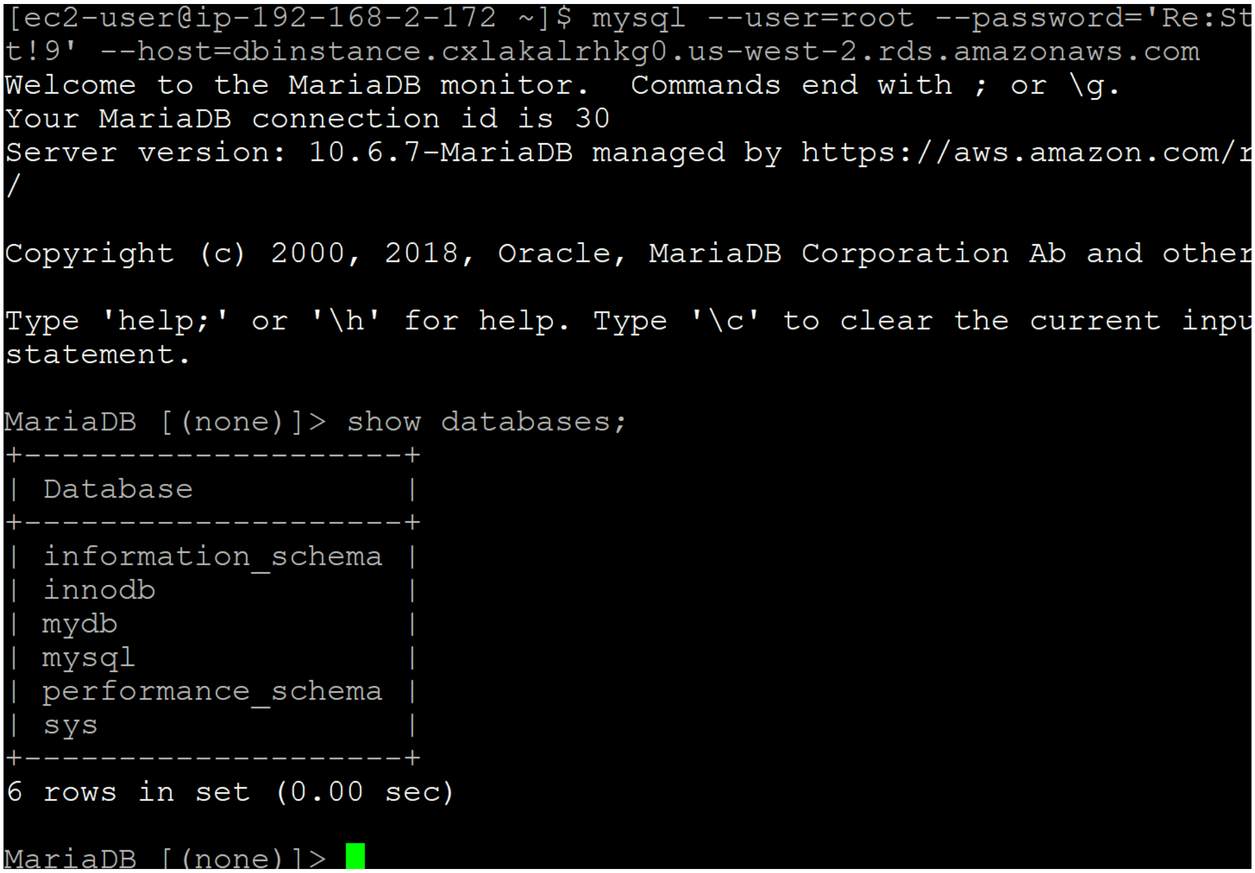
```
[ec2-user@ip-192-168-1-162 ~]$ chmod 400 labsuser.pem
[ec2-user@ip-192-168-1-162 ~]$ ssh -i labsuser.pem ec2-user@192.168
.2.172
The authenticity of host '192.168.2.172 (192.168.2.172)' can't be e
stablished.
ECDSA key fingerprint is SHA256:RURnbNWL6+XNSA3+S9k0FtM1Fy0aAHcv4z7
qLtKlm7A.
ECDSA key 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



```
[ec2-user@ip-192-168-2-172 ~]$ mysql --user=root --password='Re:St
t!9' --host=dbinstance.cxlakalrhkg0.us-west-2.rds.amazonaws.com
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 30
Server version: 10.6.7-MariaDB managed by https://aws.amazon.com/r
/

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

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

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| innodb             |
| mydb               |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
6 rows in set (0.00 sec)

MariaDB [(none)]>
```

- This concludes the lab