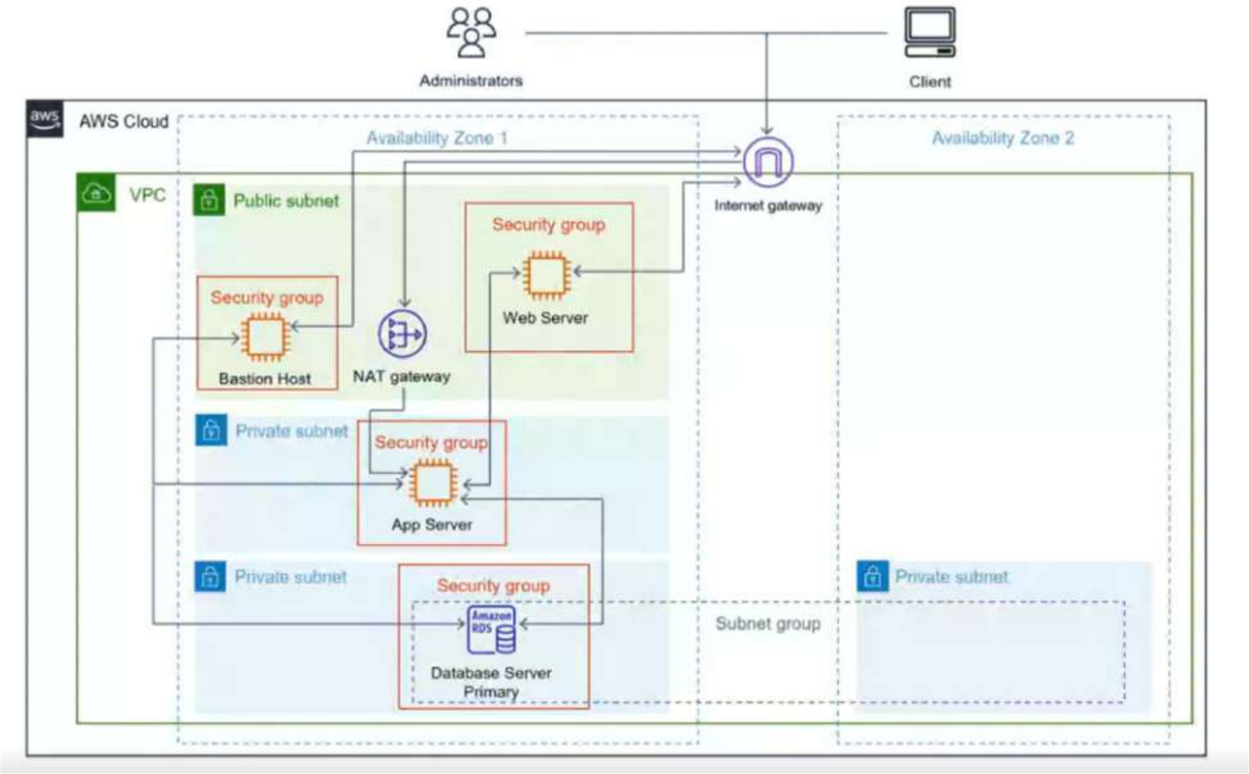
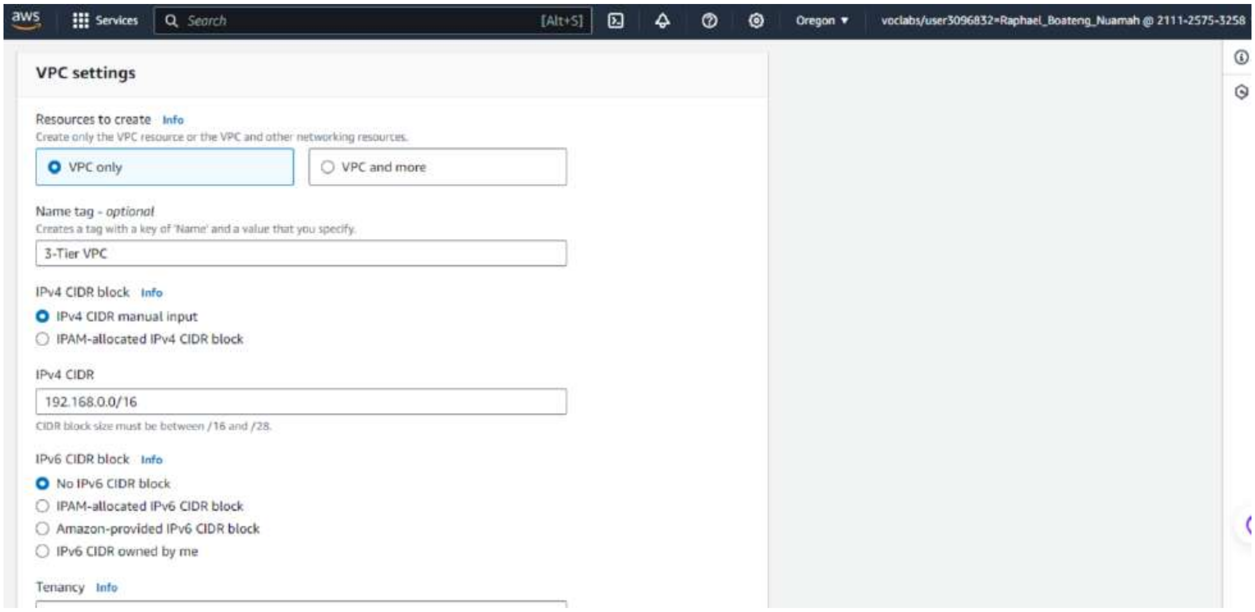
Tier 3 Project



Make VPC

- 4 subnets (1 public, 3 private)
- Enable in subnet settings public ip addresses
- Make it highly available (use 2 availability zones, the final private subnet can be the only one in a different subnet)
- Allocate an Elastic IP
- Create a nat gateway
- Create an internet gateway and attach it to your VPC
- Make route tables for your public and private subnets and attach an internet gateway and nat gateway to them respectively
- Make security groups for Bastion Host, web server, app server, and database
- Make sure to go back to security groups after making them and adding security groups to link them together, for example in the app server security group adding a rule for the database security group after creating the database security group.

Creating the VPC



VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
● VPC only ○ VPC and more

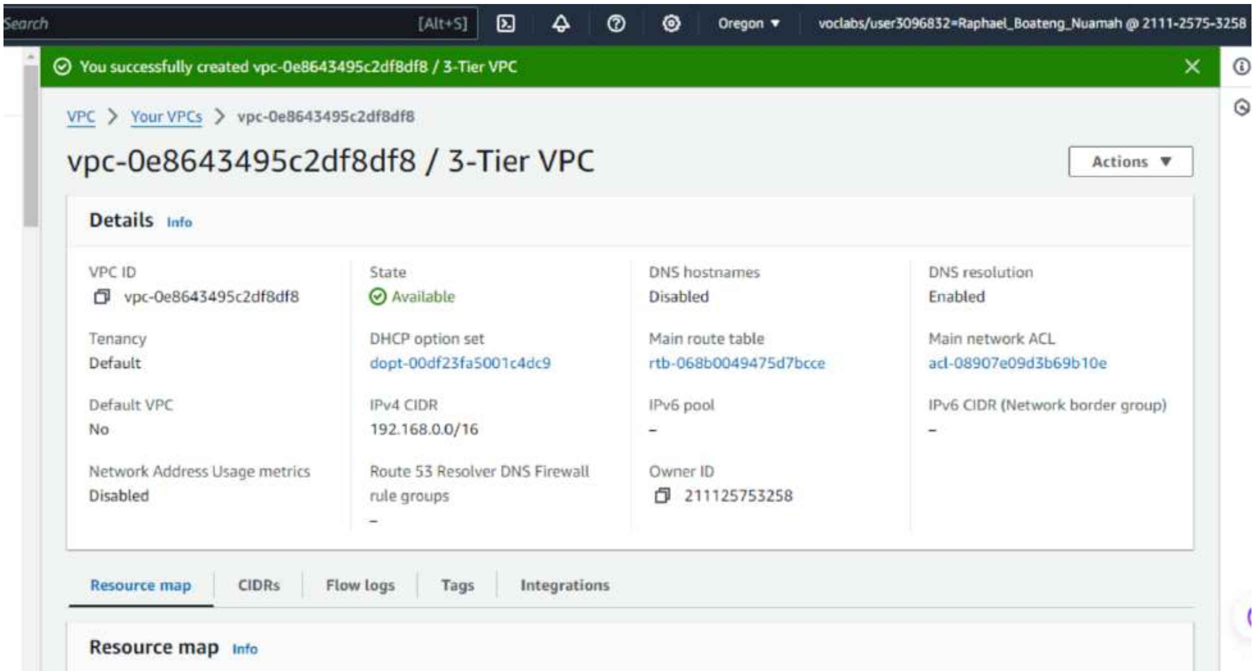
Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
3-Tier VPC

IPv4 CIDR block Info
● IPv4 CIDR manual input
○ IPAM-allocated IPv4 CIDR block

IPv4 CIDR
192.168.0.0/16
CIDR block size must be between /16 and /28.

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



Search
[Alt+S]
Oregon ▼
voclabs/user3096832=Raphael_Boateng_Nuamah @ 2111-2575-3258
VPC > Your VPCs > vpc-0e8643495c2df8df8
Actions ▼

You successfully created vpc-0e8643495c2df8df8 / 3-Tier VPC

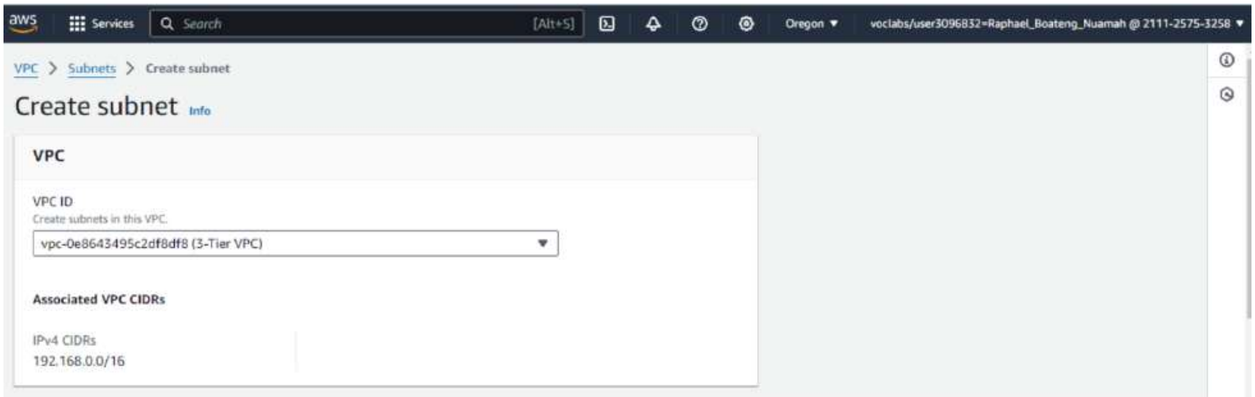
vpc-0e8643495c2df8df8 / 3-Tier VPC

Details Info

VPC ID vpc-0e8643495c2df8df8	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-00df23fa5001c4dc9	Main route table rtb-068b0049475d7bcce	Main network ACL acl-08907e09d3b69b10e
Default VPC No	IPv4 CIDR 192.168.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 211125753258	

Resource map Info

Creating the subnets(1 public and 3 private)



VPC > Subnets > Create subnet

Create subnet Info

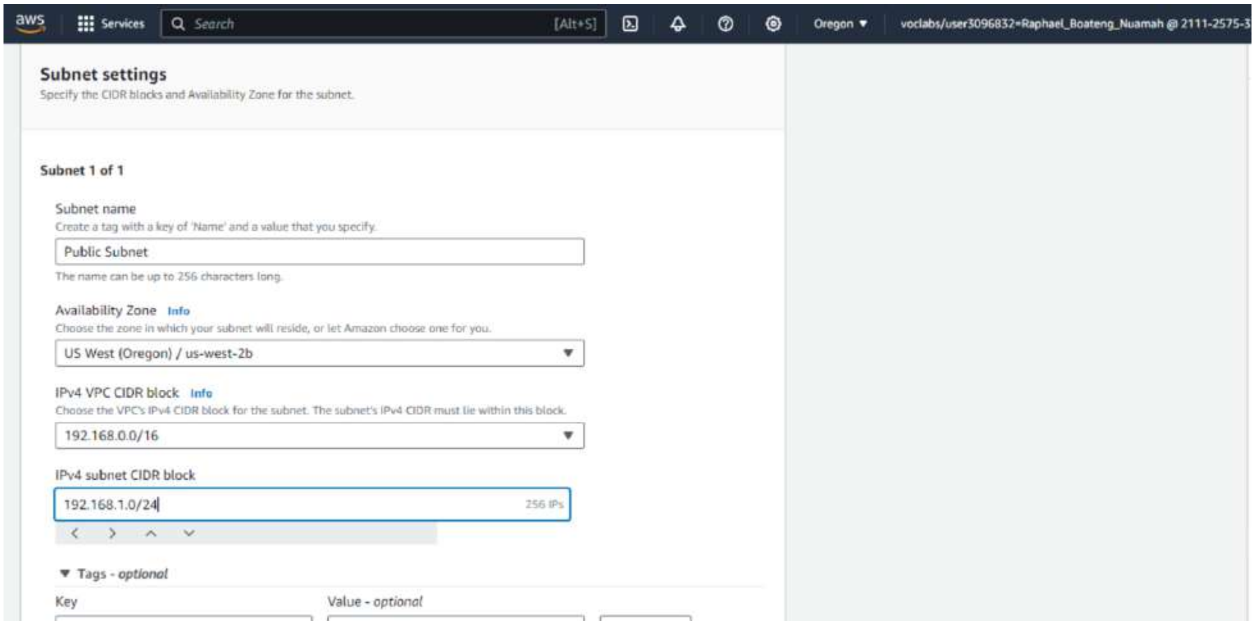
VPC

VPC ID
Create subnets in this VPC.
vpc-0e8643495c2df8df8 (3-Tier 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-2b

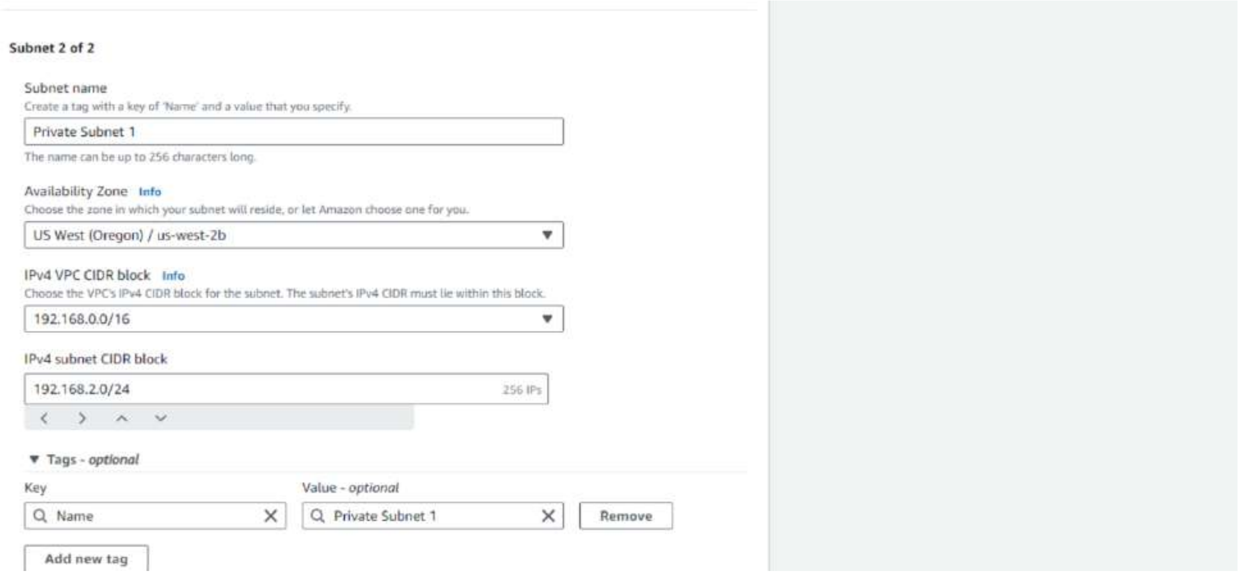
IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
192.168.0.0/16

IPv4 subnet CIDR block
192.168.1.0/24 256 IPs

▼ Tags - *optional*

Key Value - *optional*

- 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-2b

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
192.168.0.0/16

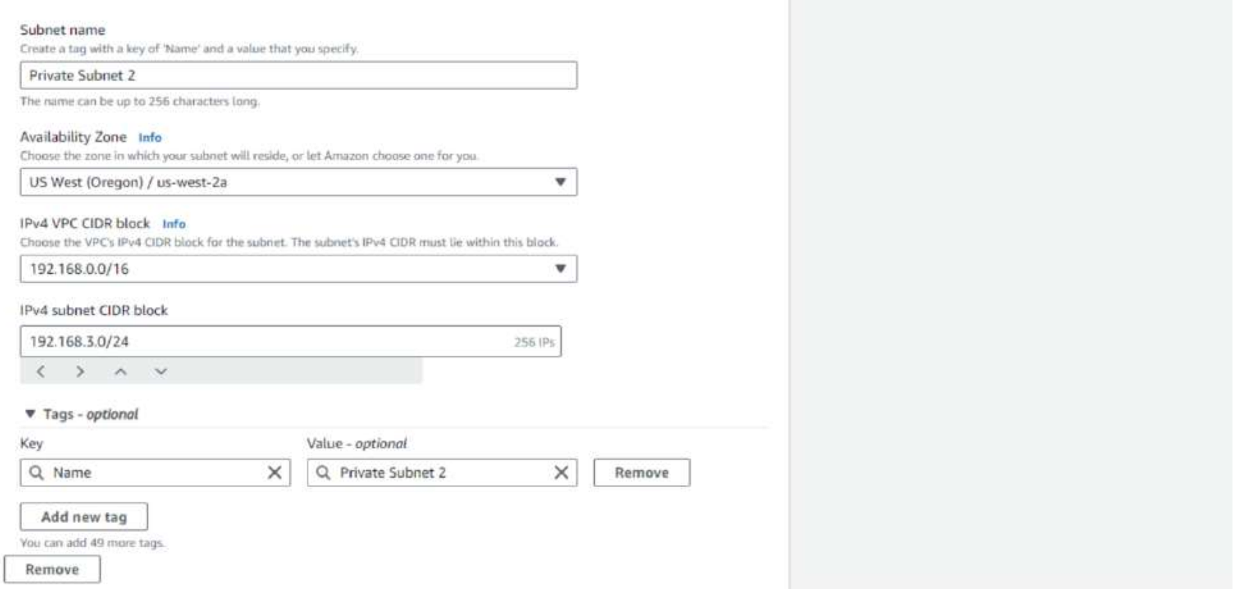
IPv4 subnet CIDR block
192.168.2.0/24 256 IPs

▼ Tags - *optional*

Key	Value - *optional*	
Name	Private Subnet 1	Remove

Add new tag

- 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 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 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
192.168.0.0/16

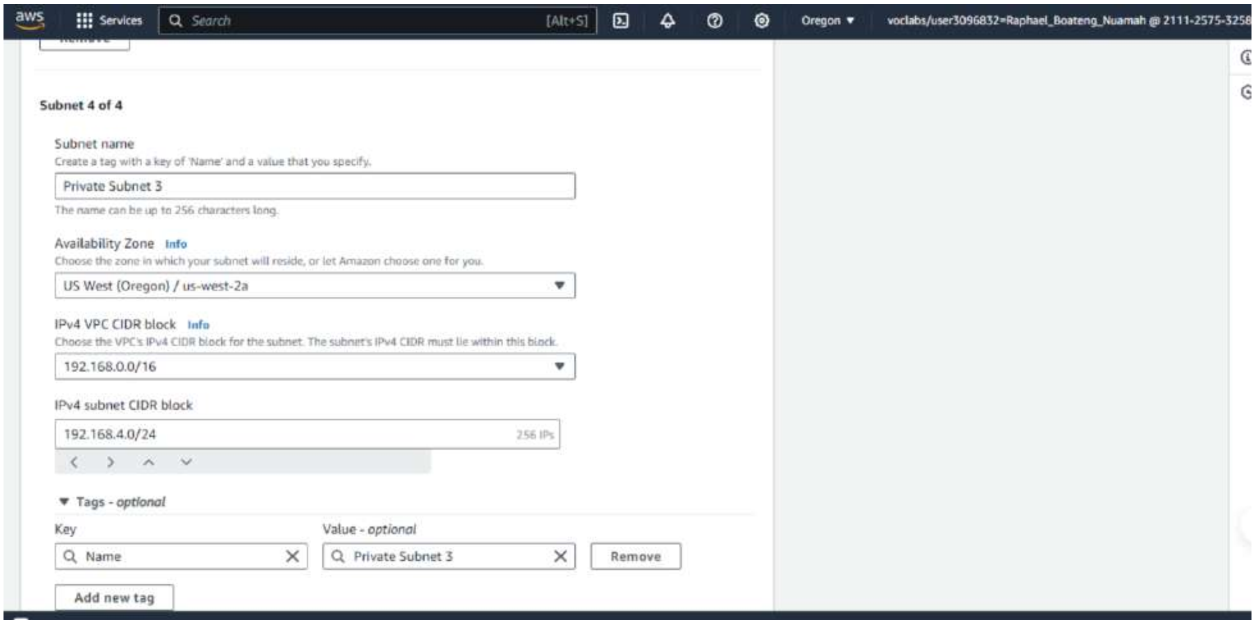
IPv4 subnet CIDR block
192.168.3.0/24 256 IPs

▼ Tags - *optional*

Key	Value - *optional*	
Name	Private Subnet 2	Remove

Add new tag
You can add 49 more tags.
Remove

- 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-2a

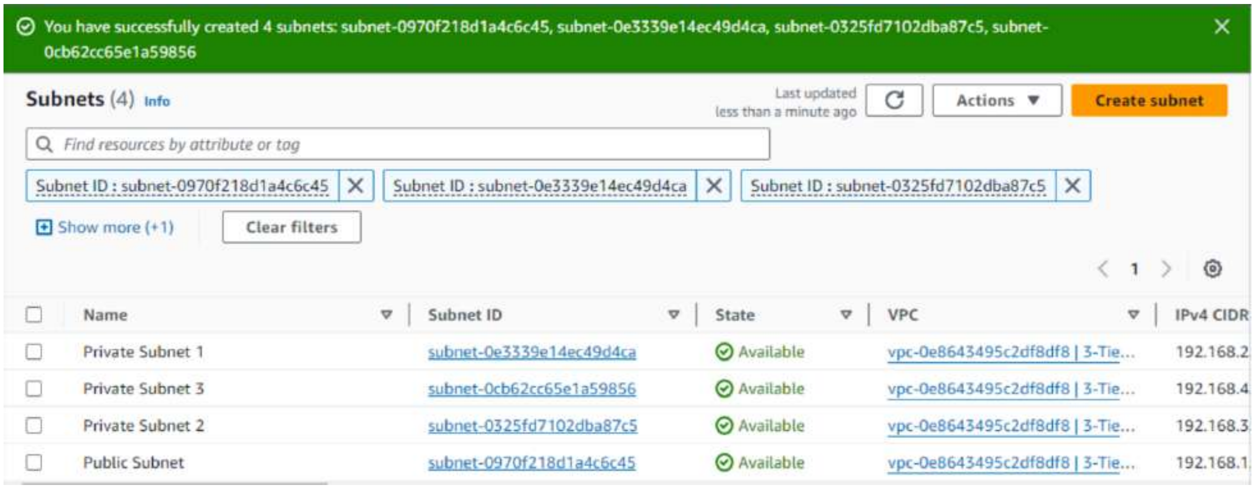
IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
192.168.0.0/16

IPv4 subnet CIDR block
192.168.4.0/24 256 IPs

▼ Tags - *optional*

Key	Value - *optional*	
Name	Private Subnet 3	Remove

Add new tag



You have successfully created 4 subnets: subnet-0970f218d1a4c6c45, subnet-0e3339e14ec49d4ca, subnet-0325fd7102dba87c5, subnet-0cb62cc65e1a59856

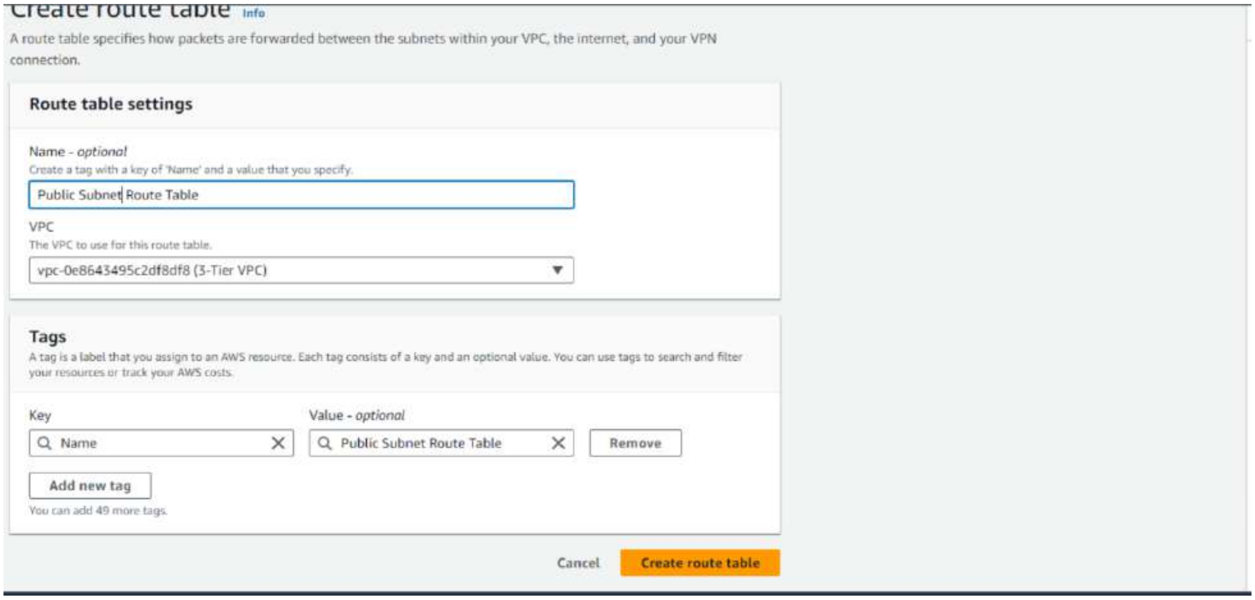
Subnets (4) Info

Last updated less than a minute ago

Actions ▼
Create subnet
Find resources by attribute or tag
Subnet ID : subnet-0970f218d1a4c6c45
Subnet ID : subnet-0e3339e14ec49d4ca
Subnet ID : subnet-0325fd7102dba87c5
Show more (+1)
Clear filters
1

□	Name	Subnet ID	State	VPC	IPv4 CIDR
□	Private Subnet 1	subnet-0e3339e14ec49d4ca	Available	vpc-0e8643495c2df8df8 | 3-Tie...	192.168.2
□	Private Subnet 3	subnet-0cb62cc65e1a59856	Available	vpc-0e8643495c2df8df8 | 3-Tie...	192.168.4
□	Private Subnet 2	subnet-0325fd7102dba87c5	Available	vpc-0e8643495c2df8df8 | 3-Tie...	192.168.3
□	Public Subnet	subnet-0970f218d1a4c6c45	Available	vpc-0e8643495c2df8df8 | 3-Tie...	192.168.1

- 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”



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

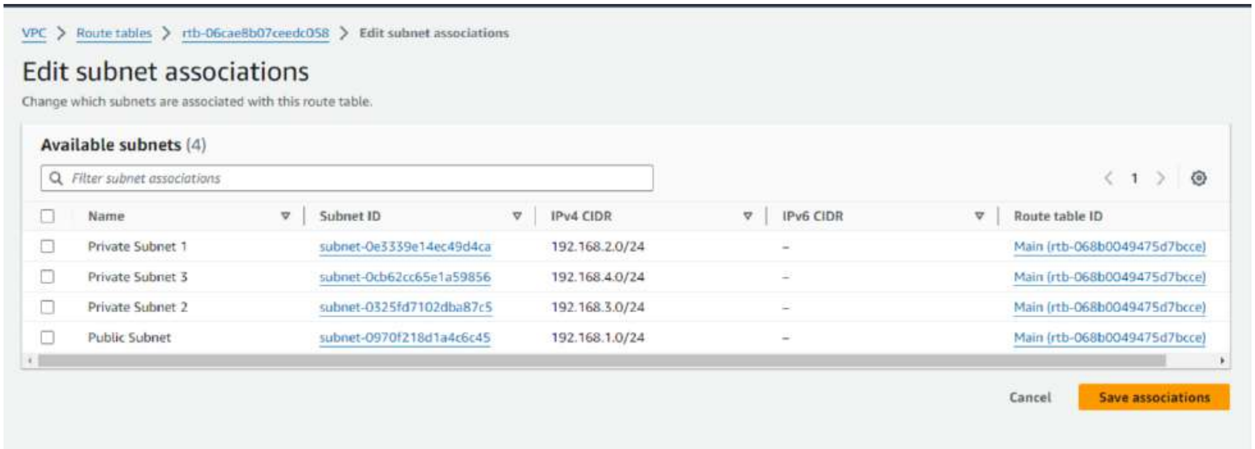
Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
Public Subnet Route Table

VPC
The VPC to use for this route table.
vpc-0e8643495c2df8df8 (3-Tier 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	Public Subnet Route Table	Remove

Add new tag
You can add 49 more tags.



VPC > Route tables > rtb-06cae8b07ceedc058 > Edit subnet associations

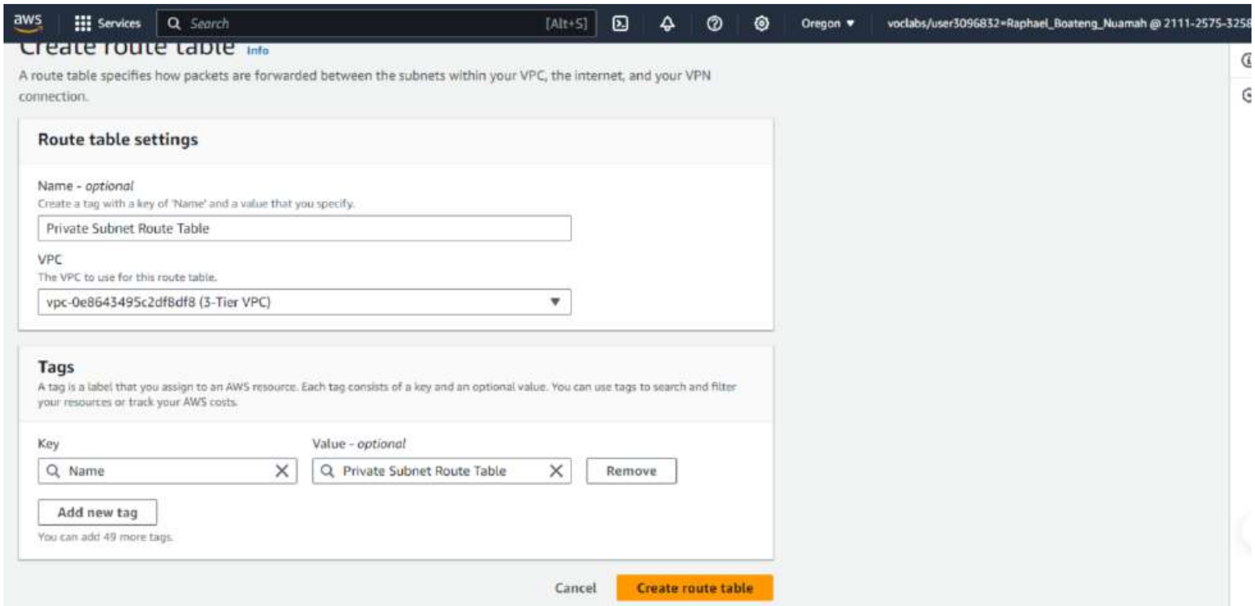
Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (4)

Filter subnet associations

□	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
□	Private Subnet 1	subnet-0e3339e14ec49d4ca	192.168.2.0/24	–	Main (rtb-068b0049475d7bcce)
□	Private Subnet 3	subnet-0cb62cc65e1a59856	192.168.4.0/24	–	Main (rtb-068b0049475d7bcce)
□	Private Subnet 2	subnet-0325fd7102dba87c5	192.168.3.0/24	–	Main (rtb-068b0049475d7bcce)
□	Public Subnet	subnet-0970f218d1a4c6c45	192.168.1.0/24	–	Main (rtb-068b0049475d7bcce)



voclabs/user3096832=Raphael_Boateng_Nuamah @ 2111-2575-3258

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.
Private Subnet Route Table

VPC
The VPC to use for this route table.
vpc-0e8643495c2df8df8 (3-Tier VPC) ▼

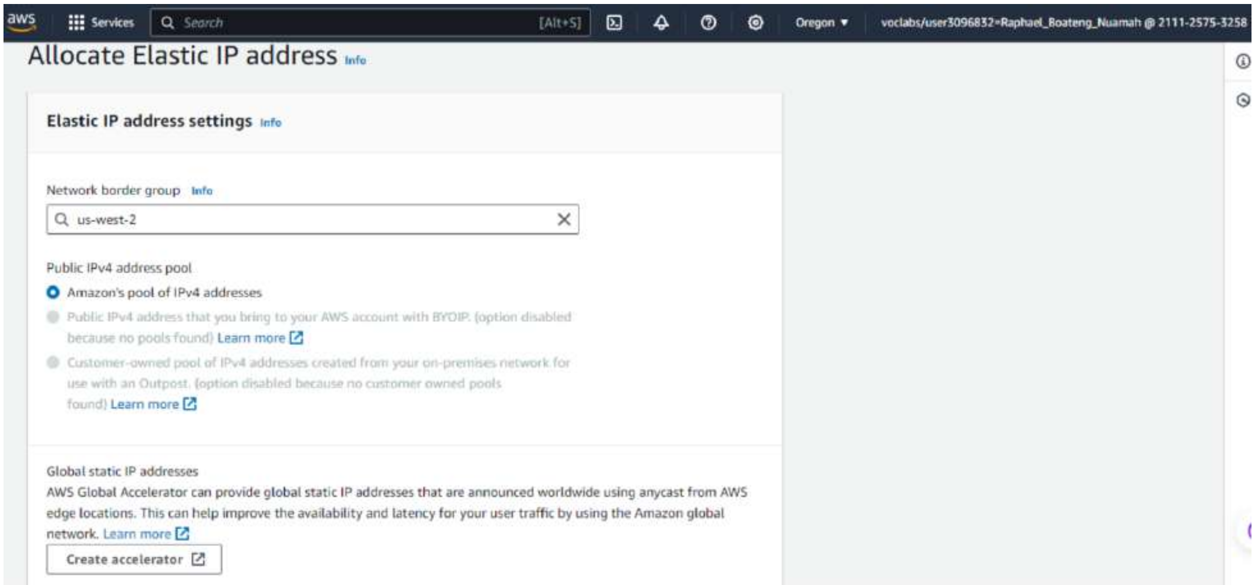
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*	
Name	Private Subnet Route Table	Remove

Add new tag
You can add 49 more tags.

NB: Do not forget to associate your Route table to their respective subnets

Allocate an Elastic IP



Allocate Elastic IP address

Elastic IP address settings

Network border group

us-west-2

Public IPv4 address pool

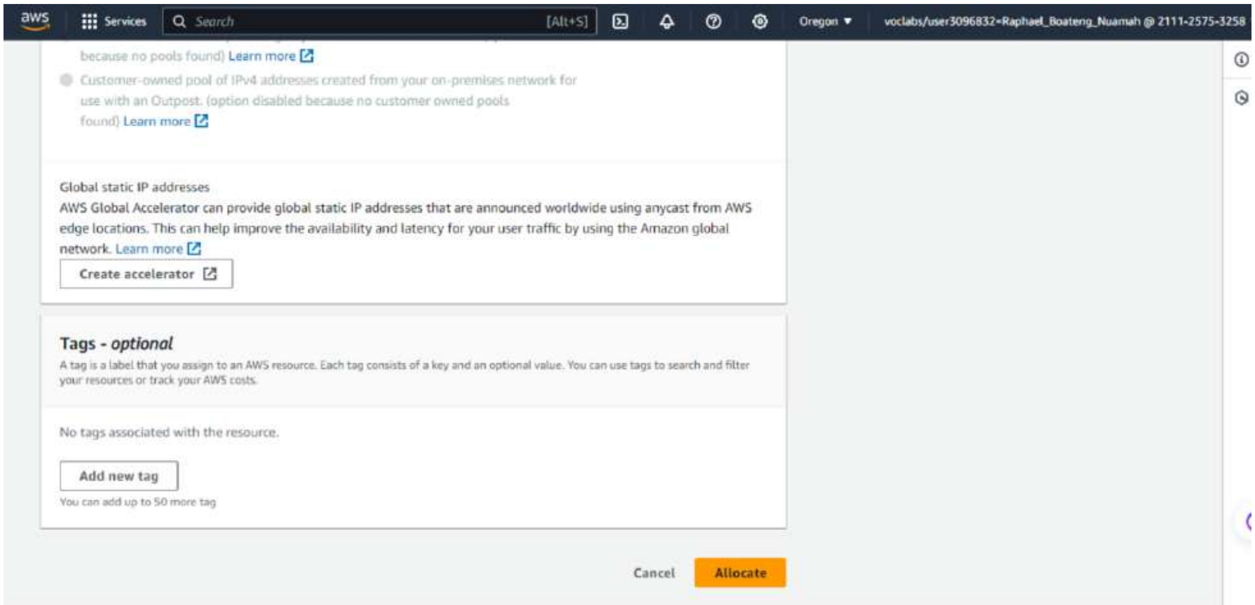
● Amazon's pool of IPv4 addresses

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

○ Customer-owned pool of IPv4 addresses created from your on-premises network for use with an Outpost. (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



because no pools found) Learn more

○ Customer-owned pool of IPv4 addresses created from your on-premises network for use with an Outpost. (option disabled because no customer owned pools found) Learn more

Global static IP addresses

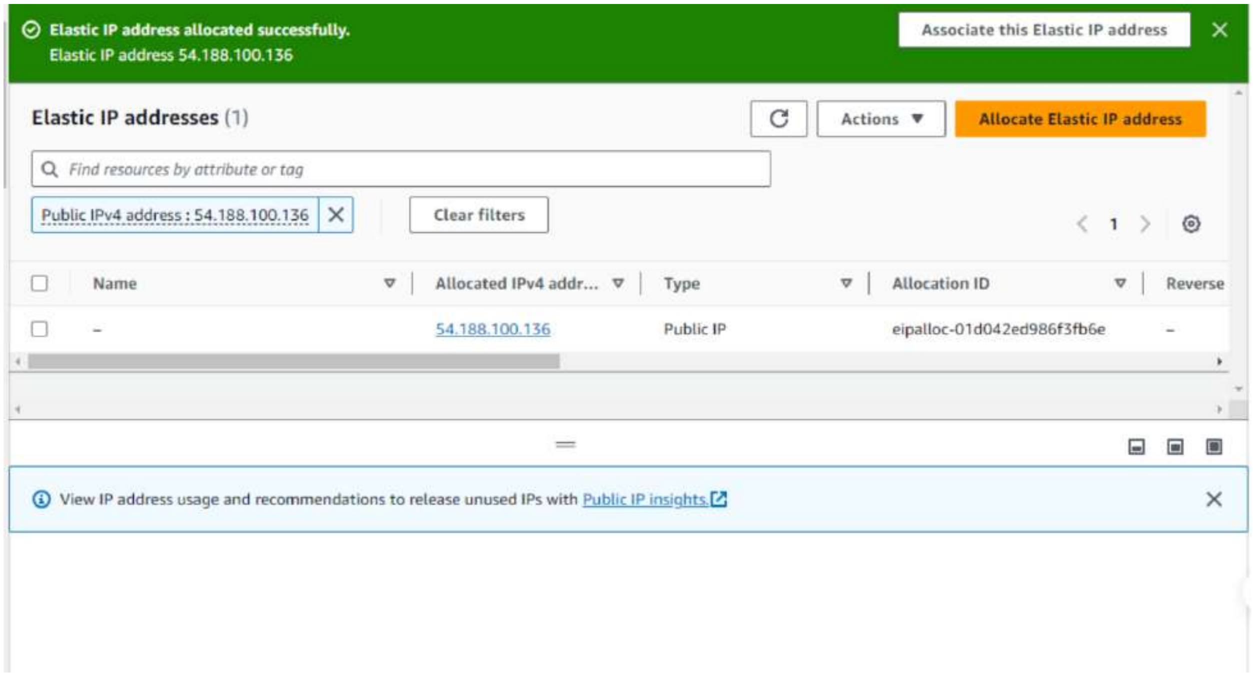
AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. Learn more

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

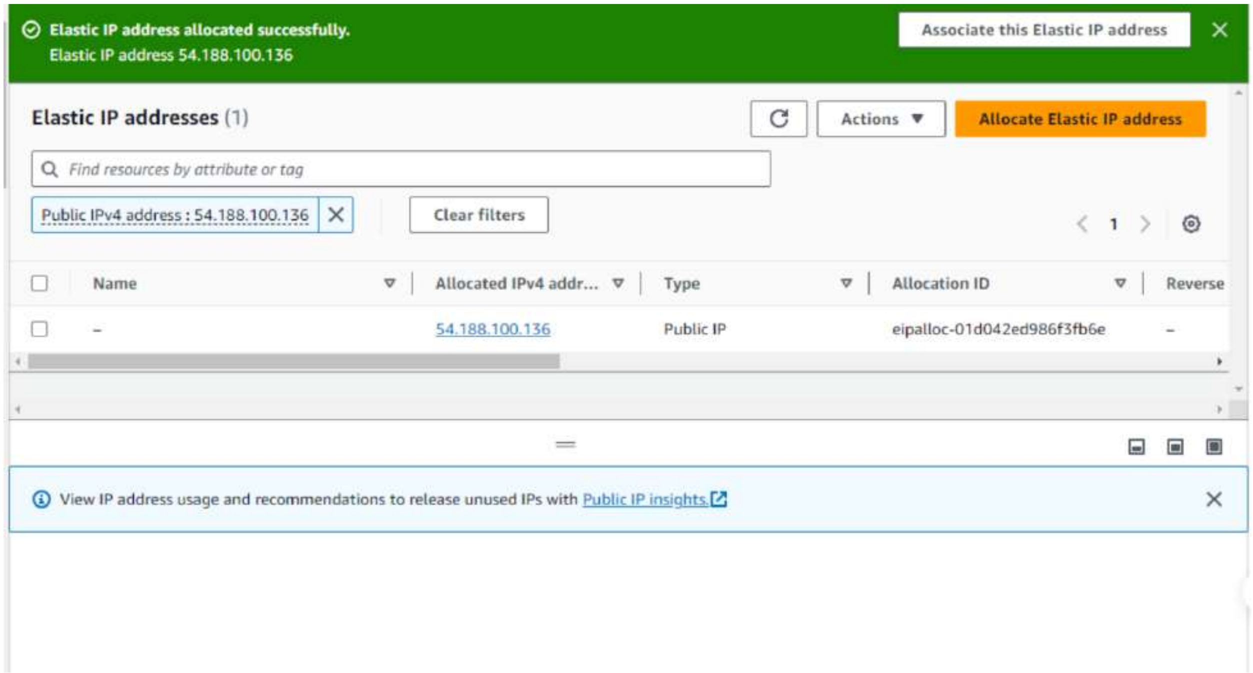


Elastic IP address allocated successfully.
Elastic IP address 54.188.100.136

Associate this Elastic IP address
Elastic IP addresses (1)
Actions
Allocate Elastic IP address
Find resources by attribute or tag
Public IPv4 address : 54.188.100.136
Clear filters

Name	Allocated IPv4 addr...	Type	Allocation ID	Reverse
–	54.188.100.136	Public IP	eipalloc-01d042ed986f3fb6e	–

View IP address usage and recommendations to release unused IPs with Public IP insights

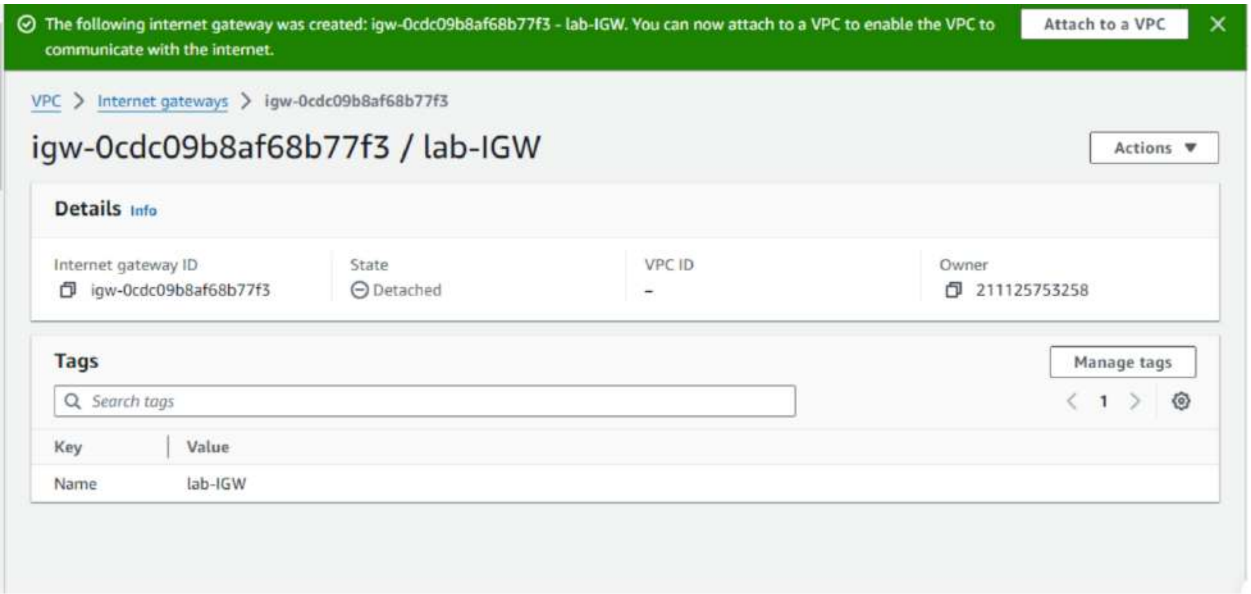


Elastic IP address allocated successfully.
Elastic IP address 54.188.100.136

Name	Allocated IPv4 addr...	Type	Allocation ID	Reverse
–	54.188.100.136	Public IP	eipalloc-01d042ed986f3fb6e	–

View IP address usage and recommendations to release unused IPs with Public IP insights

- 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”
- 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-0cdc09b8af68b77f3 - lab-IGW. You can now attach to a VPC to enable the VPC to communicate with the internet.

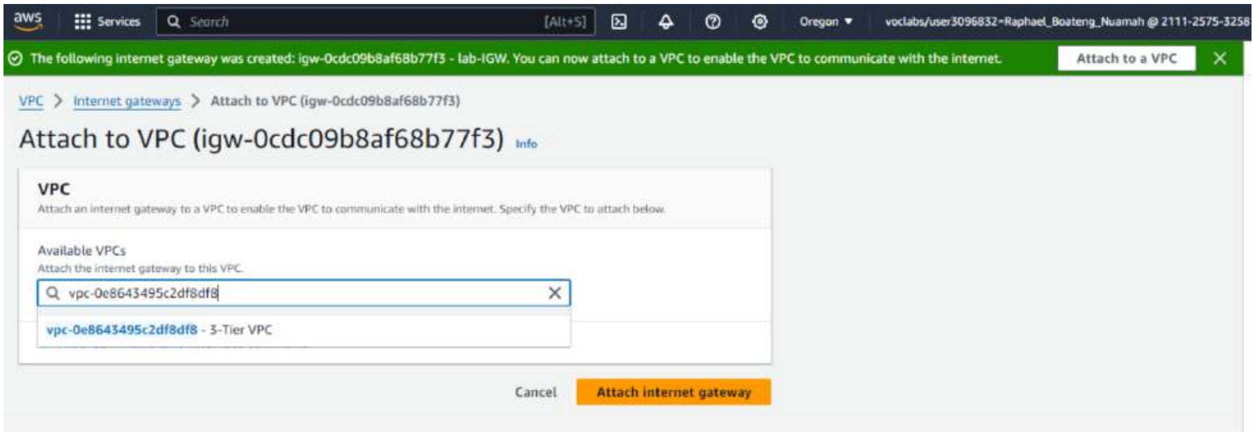
igw-0cdc09b8af68b77f3 / lab-IGW

Details Info

Internet gateway ID	State	VPC ID	Owner
igw-0cdc09b8af68b77f3	Detached	-	211125753258

Tags

Key	Value
Name	lab-IGW



aws
Services
Search
[Alt+S]
Oregon ▼

voclabs/user3096832=Raphael_Boateng_Nuamah @ 2111-2575-3258

The following internet gateway was created: igw-0cdc09b8af68b77f3 - lab-IGW. You can now attach to a VPC to enable the VPC to communicate with the internet.

Attach to a VPC
VPC > Internet gateways > Attach to VPC (igw-0cdc09b8af68b77f3)

Attach to VPC (igw-0cdc09b8af68b77f3) Info

VPC

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

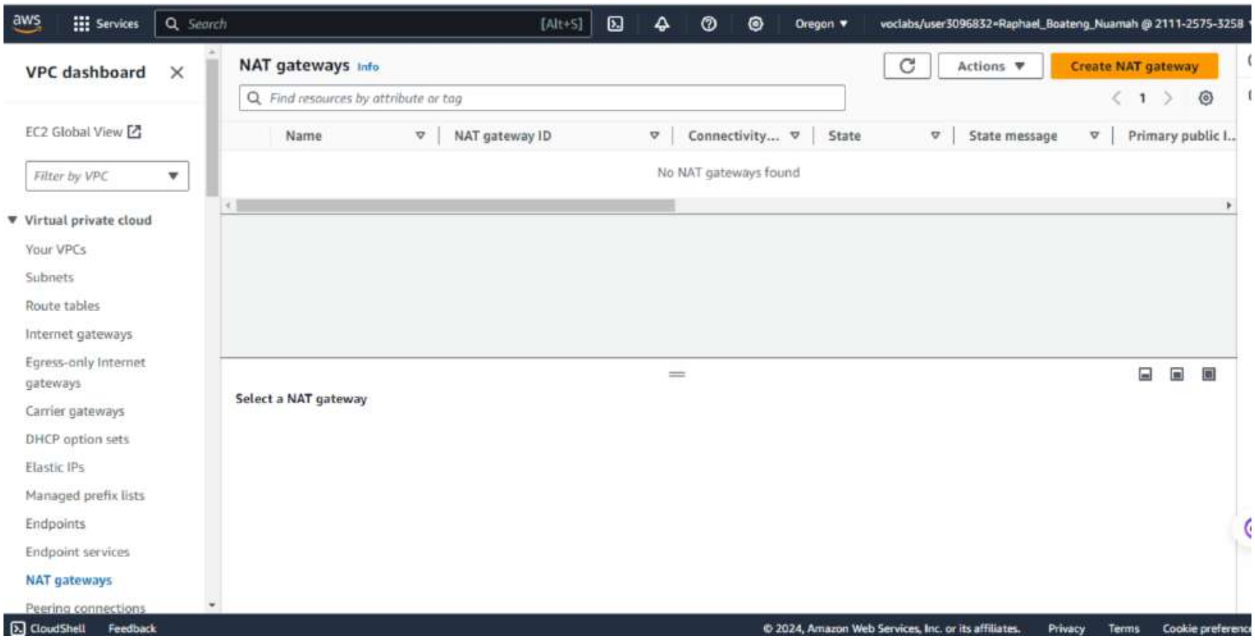
Available VPCs

Attach the internet gateway to this VPC.

vpc-0e8643495c2df8df8

vpc-0e8643495c2df8df8 - 3-Tier VPC

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



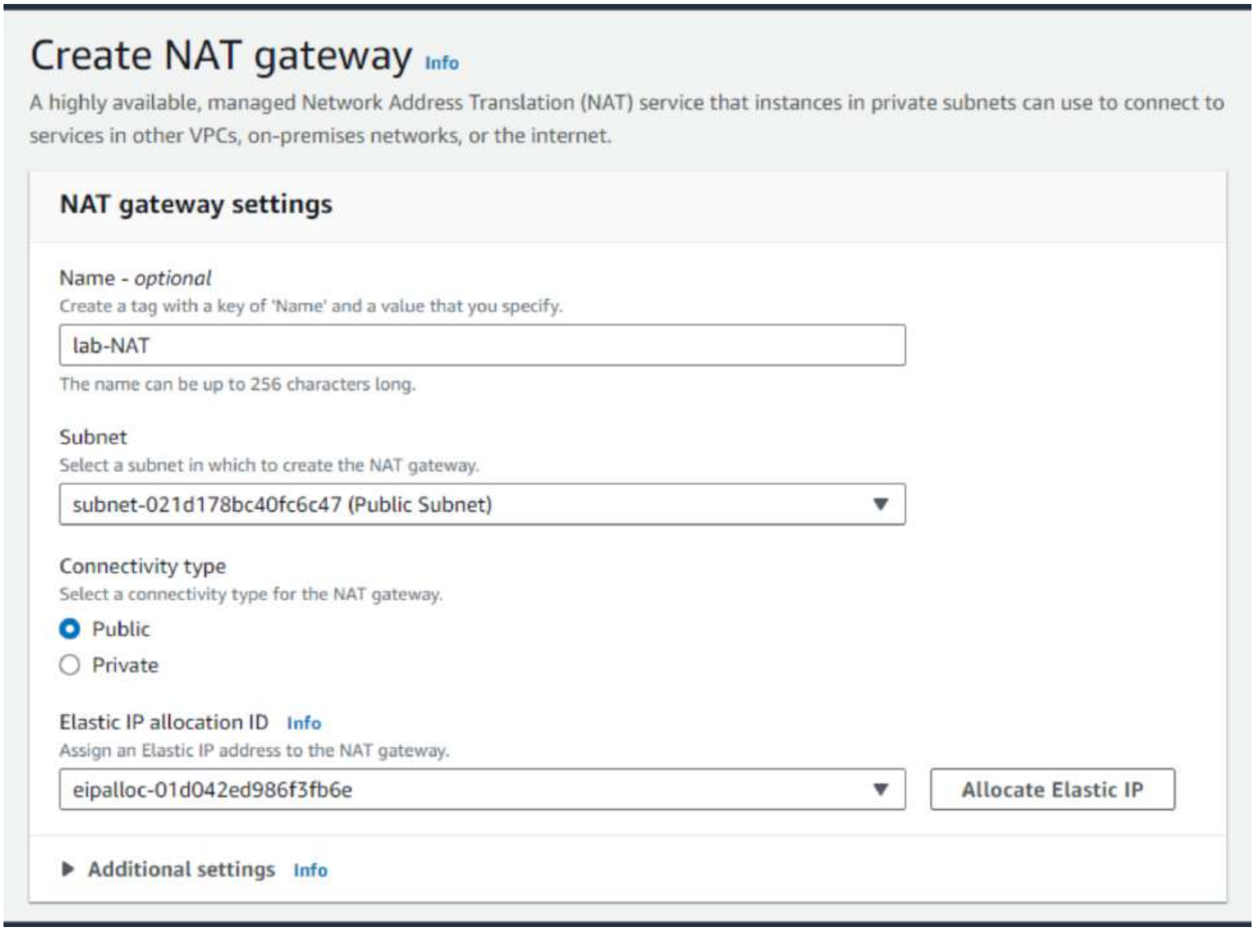
NAT gateways Info

Name	NAT gateway ID	Connectivity...	State	State message	Primary public I..

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”



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-NAT
The name can be up to 256 characters long.

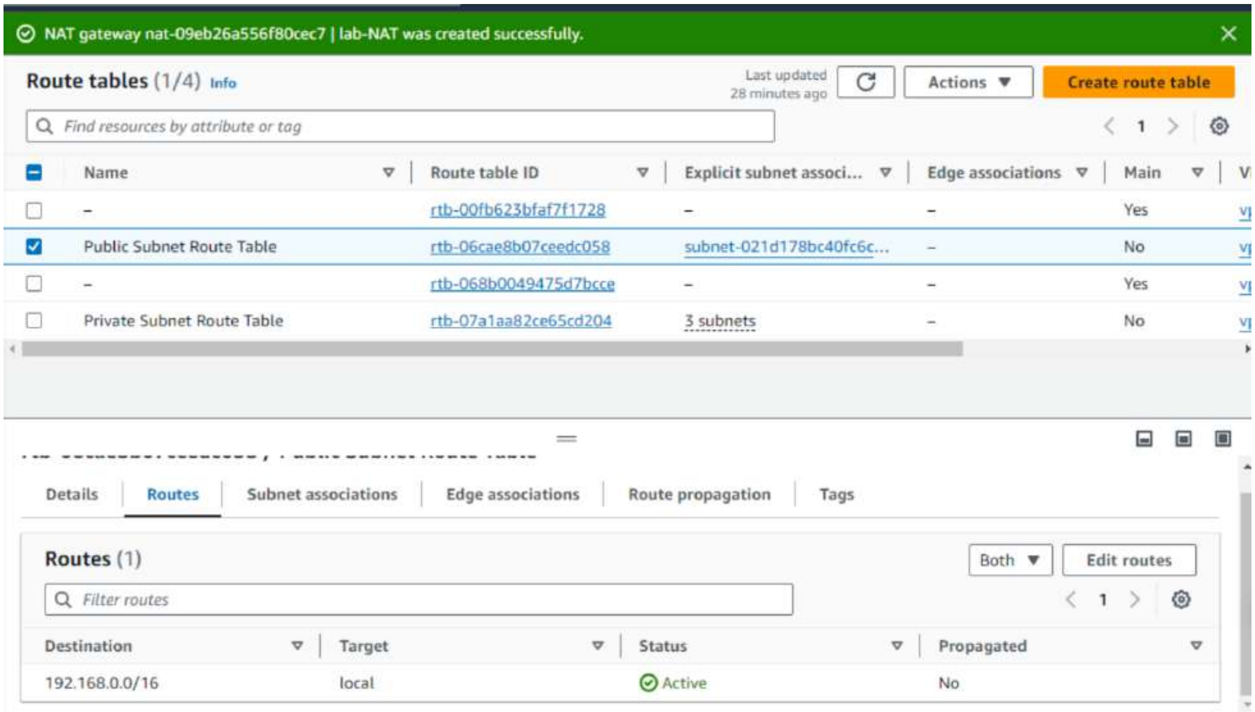
Subnet
Select a subnet in which to create the NAT gateway.
subnet-021d178bc40fc6c47 (Public Subnet) ▼

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-01d042ed986f3fb6e ▼

- 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



NAT gateway nat-09eb26a556f80cec7 | lab-NAT was created successfully.

Route tables (1/4) Info

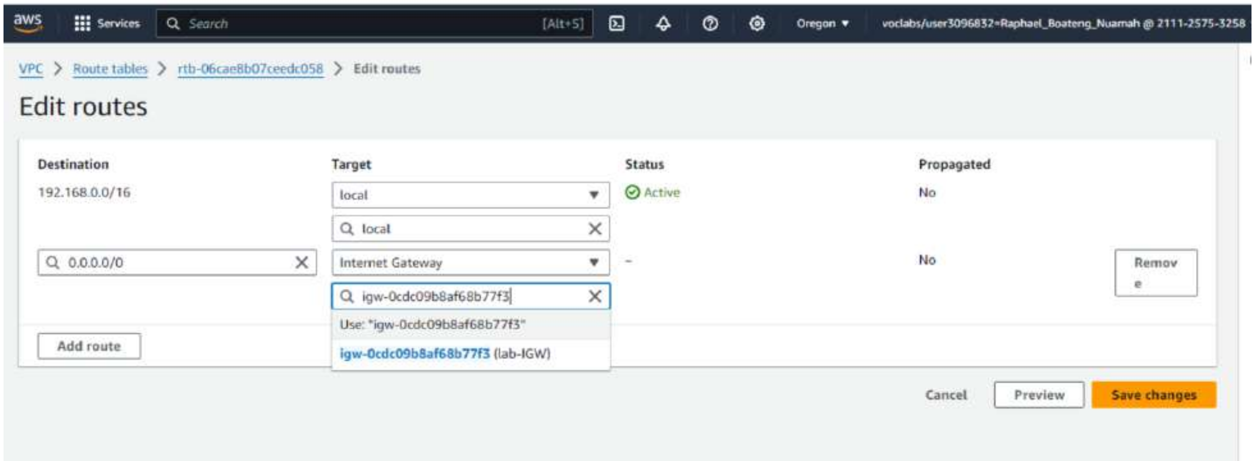
Last updated 28 minutes ago

☐	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	V
☐	–	rtb-00fb623bfaf7f1728	–	–	Yes	v
☑	Public Subnet Route Table	rtb-06cae8b07ceedc058	subnet-021d178bc40fc6c...	–	No	v
☐	–	rtb-068b0049475d7bcce	–	–	Yes	v
☐	Private Subnet Route Table	rtb-07a1aa82ce65cd204	3 subnets	–	No	v

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”



VPC > Route tables > rtb-06cae8b07ceedc058 > Edit routes

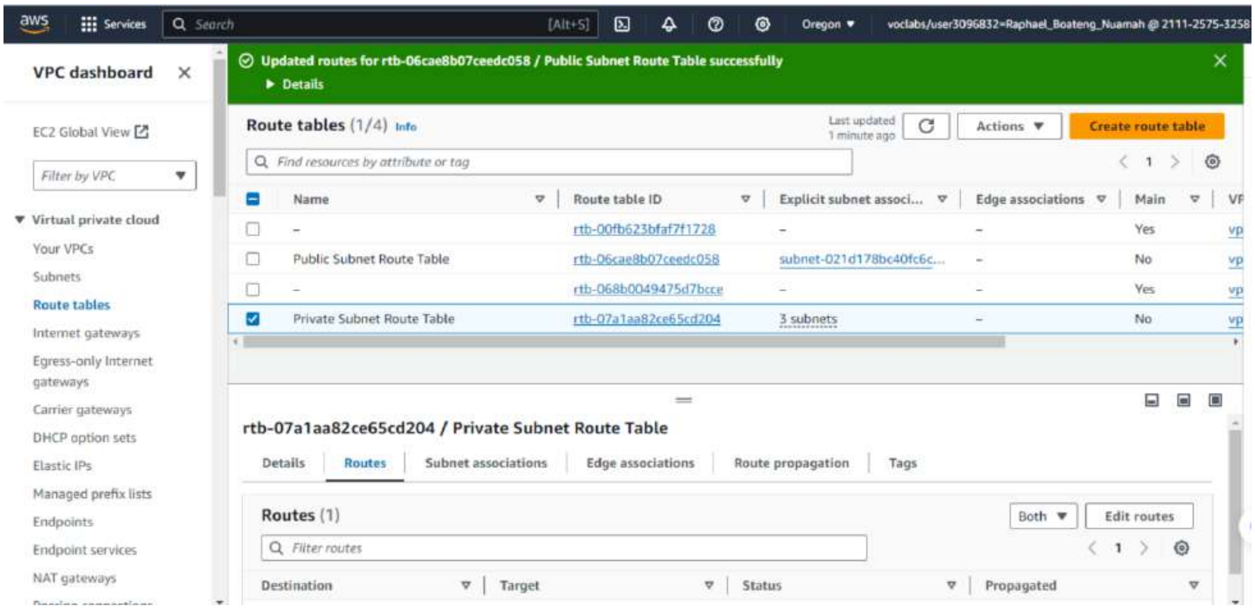
Edit routes

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No
0.0.0.0/0	Internet Gateway igw-0cdc09b8af68b77f3	-	No

Use: "igw-0cdc09b8af68b77f3"

igw-0cdc09b8af68b77f3 (lab-IGW)

- Go to edit the routes of the private table



Updated routes for rtb-06cae8b07ceedc058 / Public Subnet Route Table successfully

▶ Details

Route tables (1/4) Info

Last updated 1 minute ago

Find resources by attribute or tag

	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VP
□	–	rtb-00fb623bfaf7f1728	–	–	Yes	vp
□	Public Subnet Route Table	rtb-06cae8b07ceedc058	subnet-021d178bc40fc6c...	–	No	vp
□	–	rtb-068b0049475d7bcce	–	–	Yes	vp
☑	Private Subnet Route Table	rtb-07a1aa82ce65cd204	3 subnets	–	No	vp

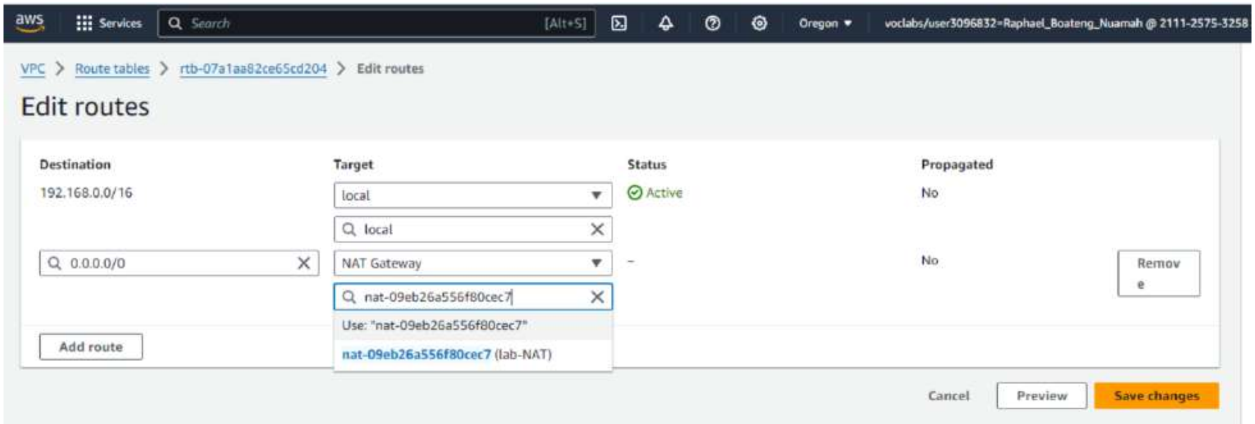
rtb-07a1aa82ce65cd204 / Private Subnet Route Table

Routes (1)

Filter routes

Destination	Target	Status	Propagated

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



VPC > Route tables > rtb-07a1aa82ce65cd204 > Edit routes

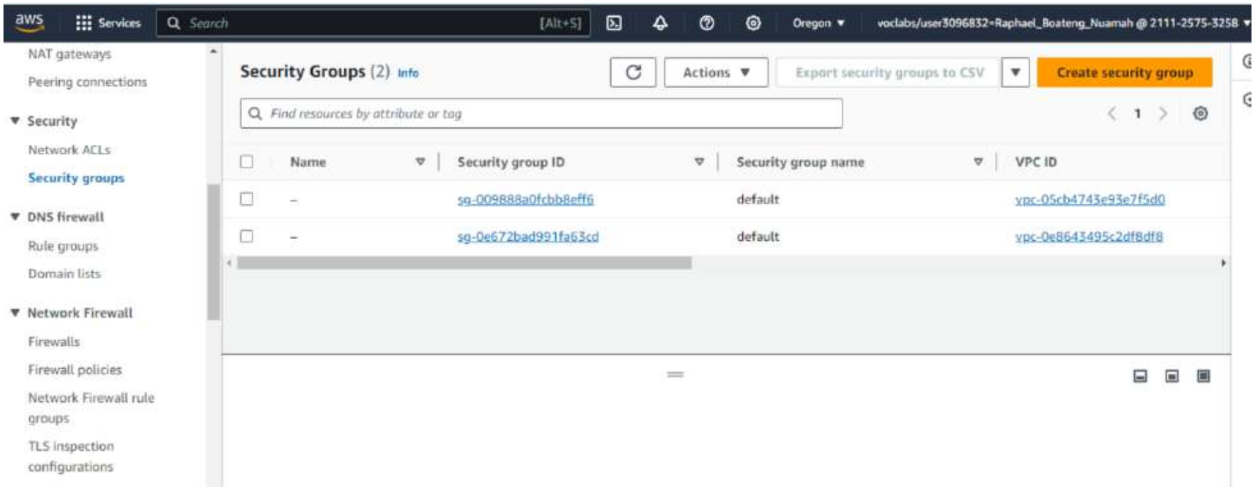
Edit routes

Destination	Target	Status	Propagated
192.168.0.0/16	local	Active	No
0.0.0.0/0	NAT Gateway nat-09eb26a556f80cec7	-	No

Use: "nat-09eb26a556f80cec7"

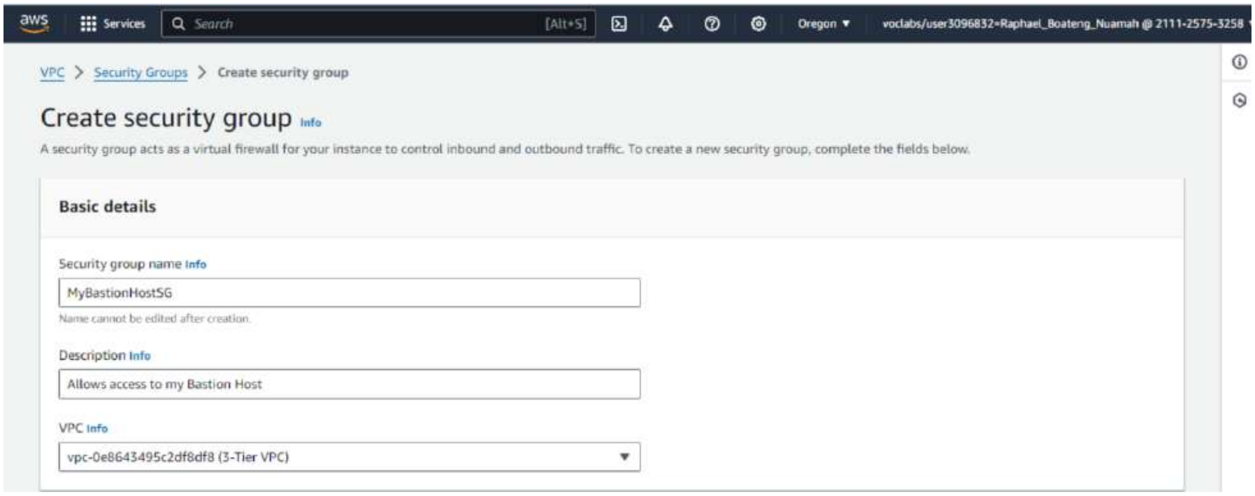
nat-09eb26a556f80cec7 (lab-NAT)

- 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
□	–	sg-009888a0fcbb8eff6	default	vpc-05cb4743e93e7f5d0
□	–	sg-0e672bad991fa63cd	default	vpc-0e8643495c2df8df8

- 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


aws
Services
Search
[Alt+S]
Oregon ▾
voclabs/user3096832=Raphael_Boateng_Nuamah @ 2111-2575-3258
VPC > Security Groups > Create security group
Info
Basic details
Info
Info
Info

Create security group

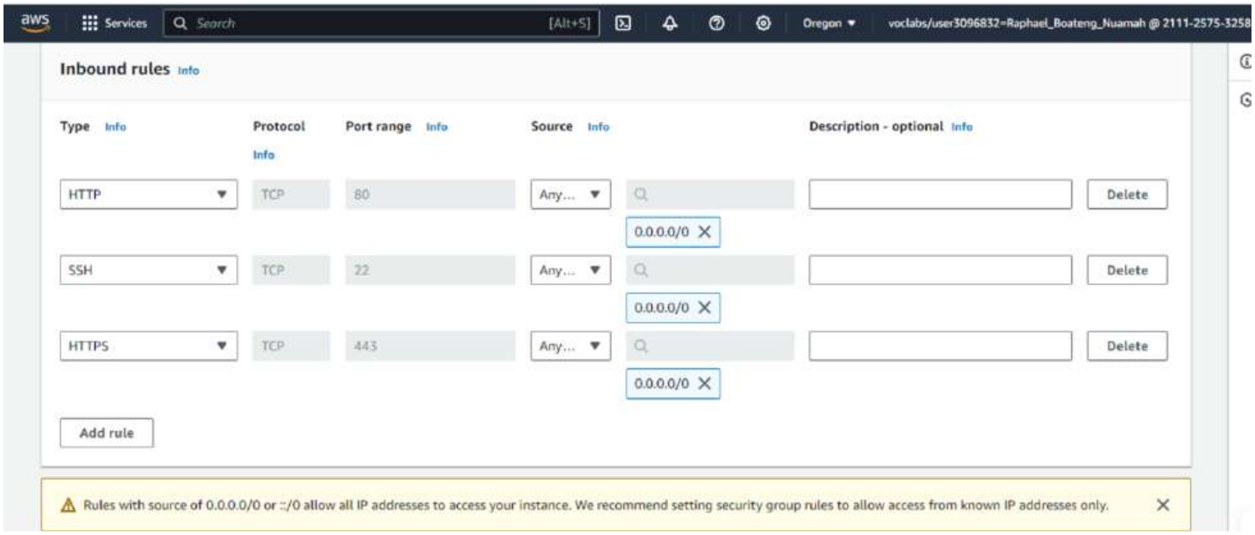
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Security group name: MyBastionHostSG

Name cannot be edited after creation.

Description: Allows access to my Bastion Host

VPC: vpc-0e8643495c2df8df8 (3-Tier VPC) ▾



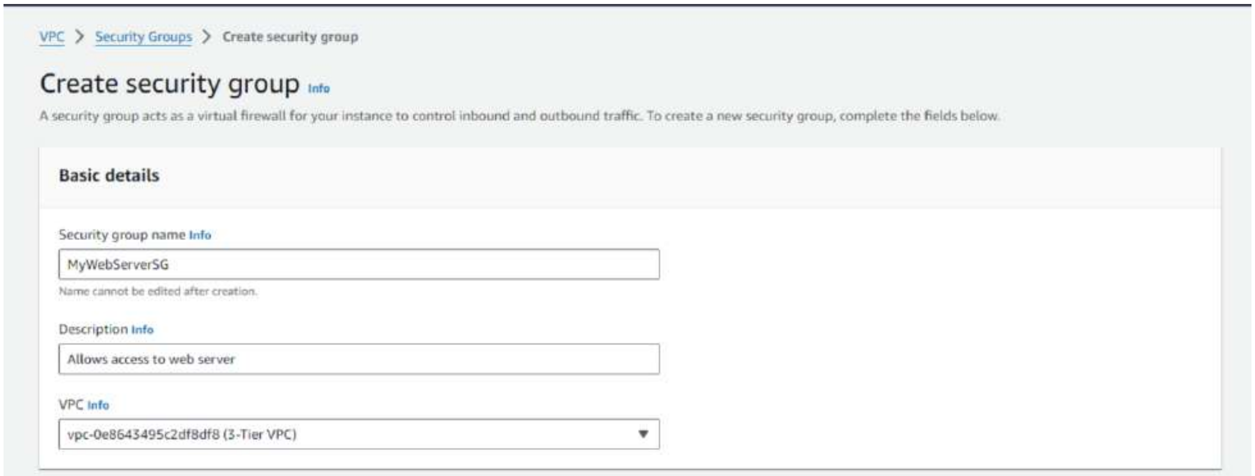
Inbound rules Info

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

Add rule

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. ✕

- 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

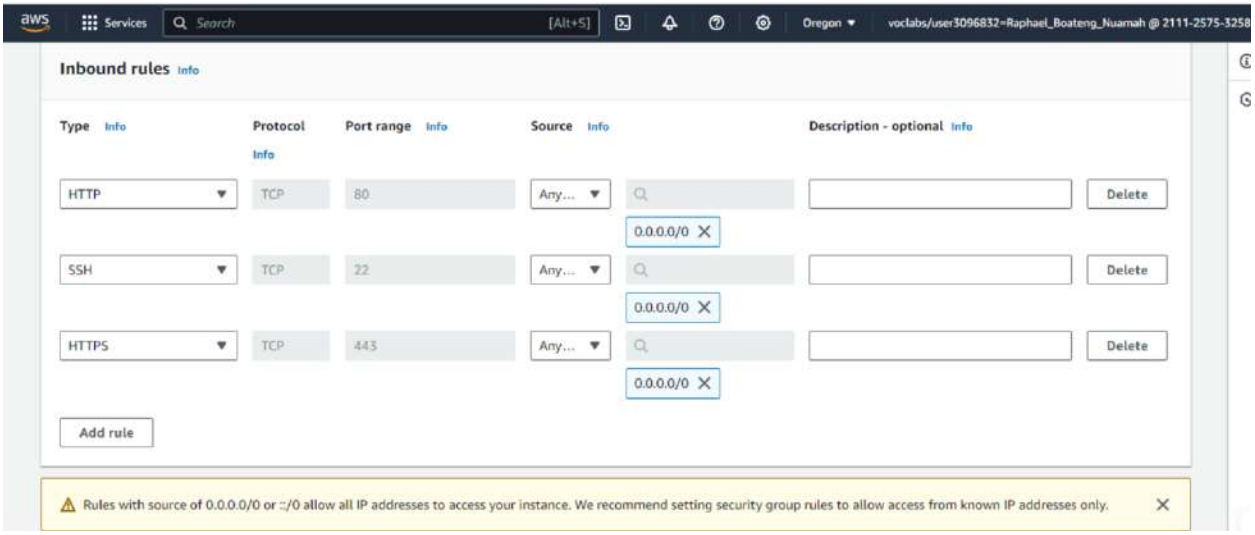
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info
MyWebServerSG
Name cannot be edited after creation.

Description Info
Allows access to web server

VPC Info
vpc-0e8643495c2df8df8 (3-Tier VPC) ▾



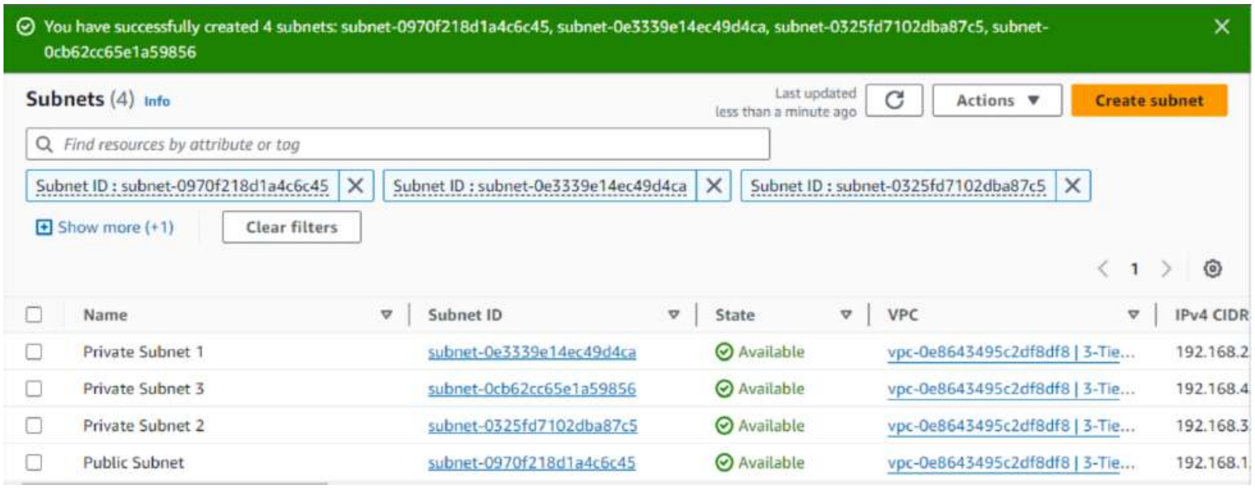
Inbound rules Info

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

Add rule

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

- 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

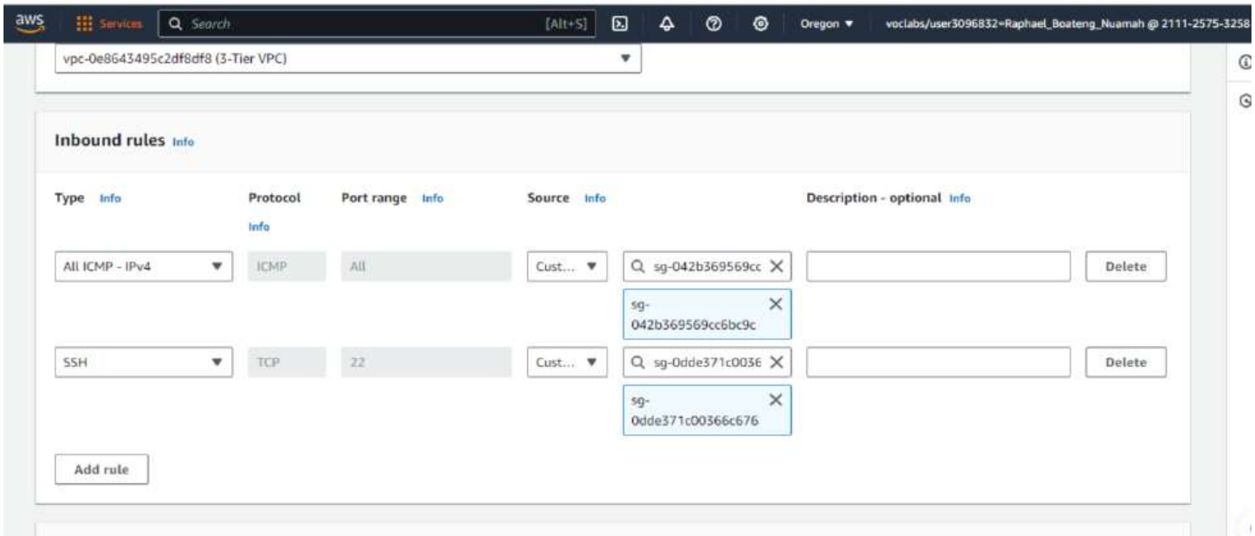


You have successfully created 4 subnets: subnet-0970f218d1a4c6c45, subnet-0e3339e14ec49d4ca, subnet-0325fd7102dba87c5, subnet-0cb62cc65e1a59856

Subnets (4) Info

Subnet ID : subnet-0970f218d1a4c6c45 | Subnet ID : subnet-0e3339e14ec49d4ca | Subnet ID : subnet-0325fd7102dba87c5

☐	Name	Subnet ID	State	VPC	IPv4 CIDR
☐	Private Subnet 1	subnet-0e3339e14ec49d4ca	✓ Available	vpc-0e8643495c2df8df8 | 3-Tie...	192.168.2
☐	Private Subnet 3	subnet-0cb62cc65e1a59856	✓ Available	vpc-0e8643495c2df8df8 | 3-Tie...	192.168.4
☐	Private Subnet 2	subnet-0325fd7102dba87c5	✓ Available	vpc-0e8643495c2df8df8 | 3-Tie...	192.168.3
☐	Public Subnet	subnet-0970f218d1a4c6c45	✓ Available	vpc-0e8643495c2df8df8 | 3-Tie...	192.168.1



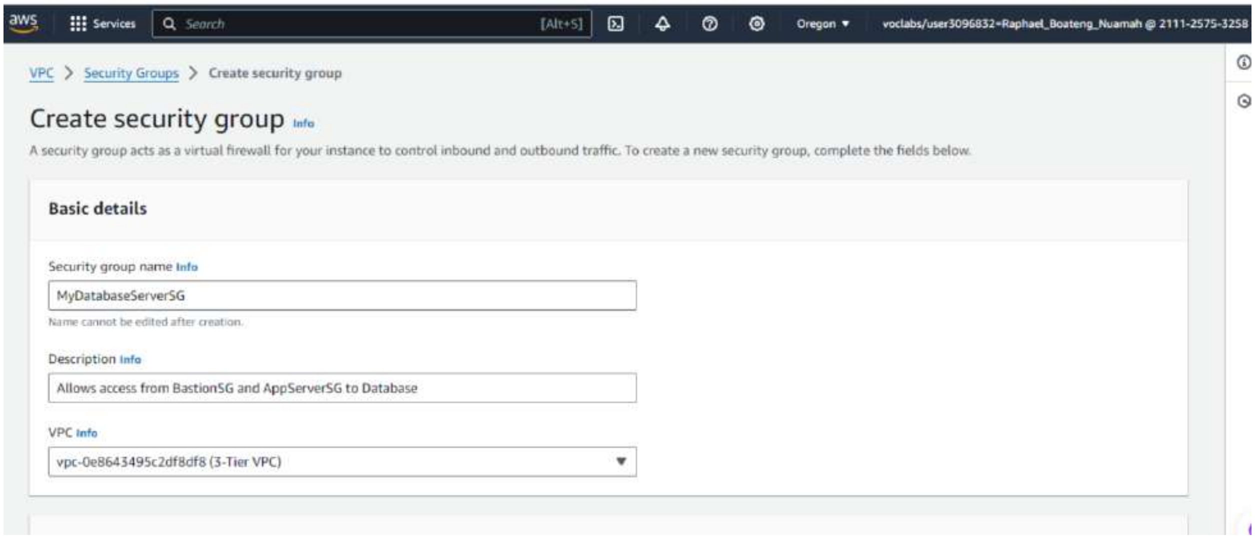
vpc-0e8643495c2df8df8 (3-Tier VPC)

Inbound rules Info

Type	Protocol	Port range	Source		Description - optional	
All ICMP - IPv4	ICMP	All	Cust...	sg-042b369569cc sg-042b369569cc6bc9c		Delete
SSH	TCP	22	Cust...	sg-0dde371c0036 sg-0dde371c00366c676		Delete

Add rule

- 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


aws
Services
Search
[Alt+S]
Oregon ▼
voclabs/user3096832=Raphael_Boateng_Nuamah @ 2111-2575-3258
VPC > Security Groups > Create security group

Create security group Info

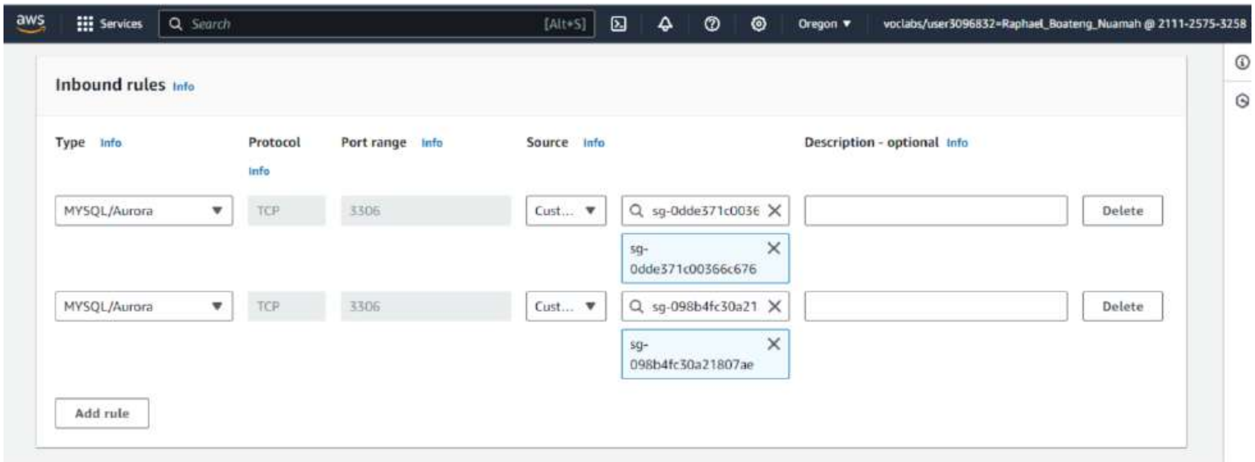
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info
MyDatabaseServerSG
Name cannot be edited after creation.

Description Info
Allows access from BastionSG and AppServerSG to Database

VPC Info
vpc-0e8643495c2df8df8 (3-Tier VPC)



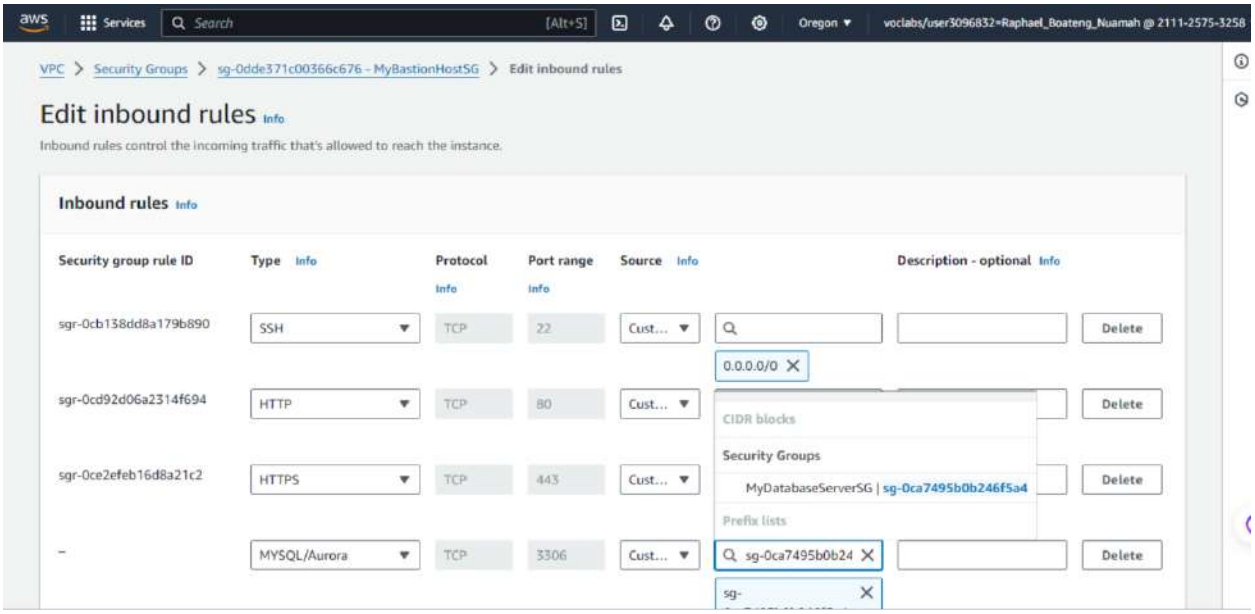
aws | Services | Search [Alt+S] | Oregon ▼ | voclabs/user3096832=Raphael_Boateng_Nuamah @ 2111-2575-3258

Inbound rules Info

Type	Protocol	Port range	Source		Description - optional	
MYSQL/Aurora ▼	TCP	3306	Cust... ▼	sg-0dde371c0036 ✕ sg-0dde371c00366c676 ✕		Delete
MYSQL/Aurora ▼	TCP	3306	Cust... ▼	sg-098b4fc30a21 ✕ sg-098b4fc30a21807ae ✕		Delete

Add rule

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



aws | Services | Search [Alt+S] | Oregon ▼ | voclabs/user3096832=Raphael_Boateng_Nuamah @ 2111-2575-3258

VPC > Security Groups > sg-0dde371c00366c676 - MyBastionHostSG > Edit inbound rules

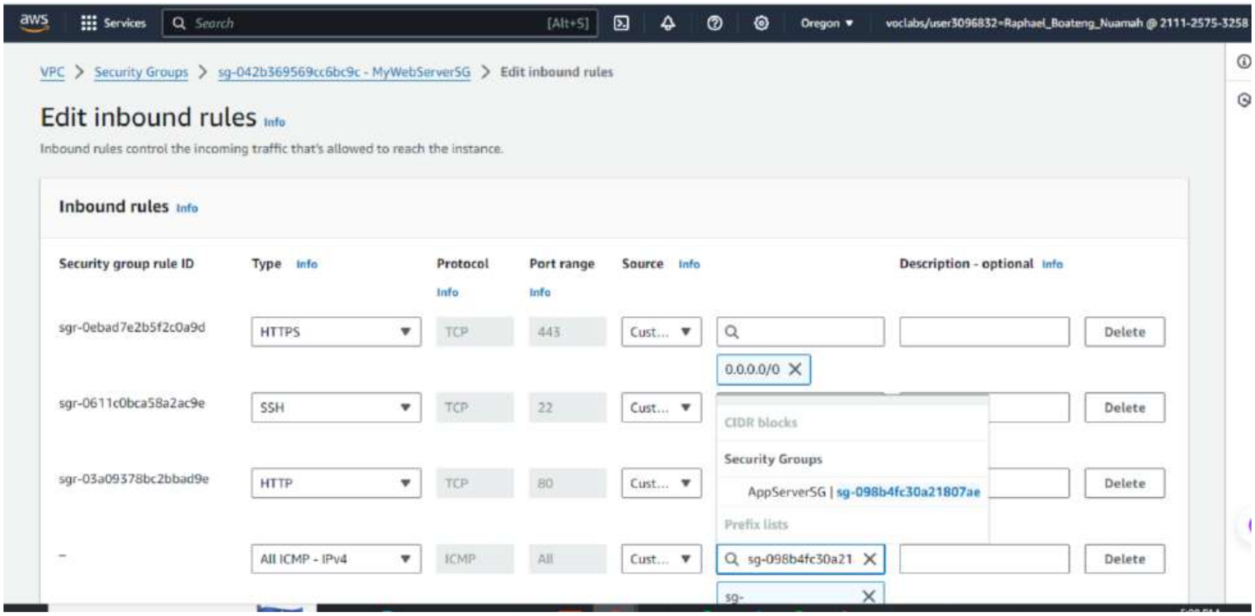
Edit inbound rules Info

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

Inbound rules Info

Security group rule ID	Type	Protocol	Port range	Source		Description - optional	
sgr-0cb138dd8a179b890	SSH ▼	TCP	22	Cust... ▼	0.0.0.0/0 ✕		Delete
sgr-0cd92d06a2314f694	HTTP ▼	TCP	80	Cust... ▼			Delete
sgr-0ce2efeb16d8a21c2	HTTPS ▼	TCP	443	Cust... ▼			Delete
-	MYSQL/Aurora ▼	TCP	3306	Cust... ▼	sg-0ca7495b0b24 ✕ sg- ✕		Delete

Include web server inbound rules and add one more for All ICMP - IPv4 and a source of your app server SG



VPC > Security Groups > sg-042b369569cc6bc9c - MyWebServerSG > Edit inbound rules

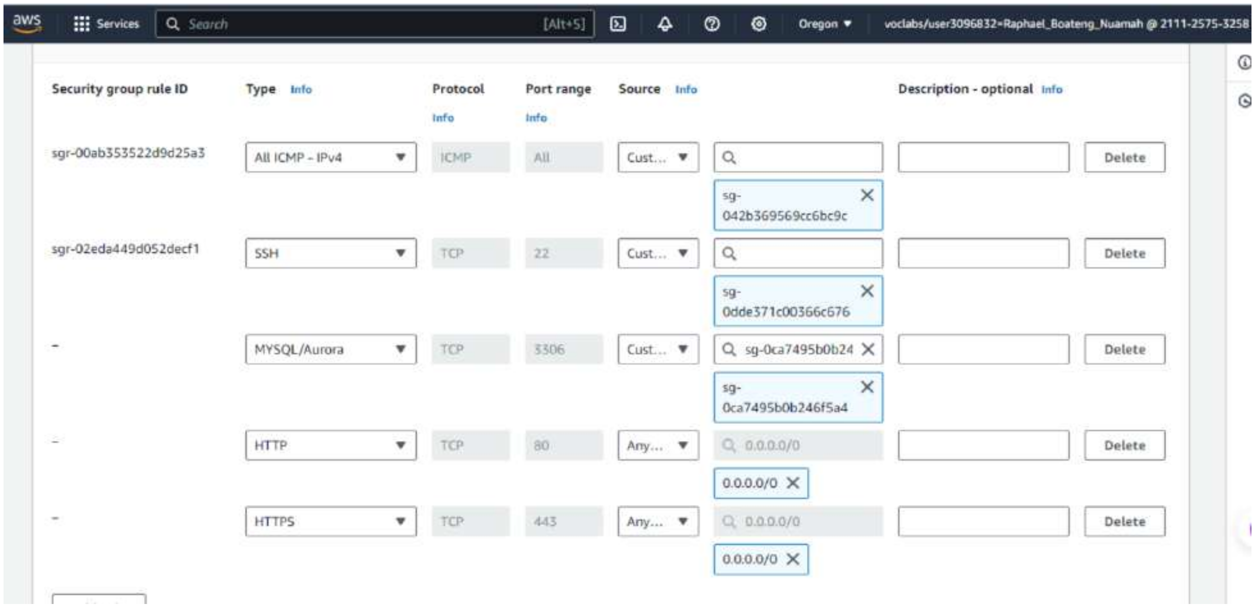
Edit inbound rules Info

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	
sgr-0ebad7e2b5f2c0a9d	HTTPS ▾	TCP	443	Cust... ▾	0.0.0.0/0 ✕		Delete
sgr-0611c0bca58a2ac9e	SSH ▾	TCP	22	Cust... ▾	CIDR blocks Security Groups AppServerSG | sg-098b4fc30a21807ae Prefix lists		Delete
sgr-03a09378bc2bbad9e	HTTP ▾	TCP	80	Cust... ▾			Delete
-	All ICMP - IPv4 ▾	ICMP	All	Cust... ▾	sg-098b4fc30a21 ✕ sg- ✕		Delete

- Include 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

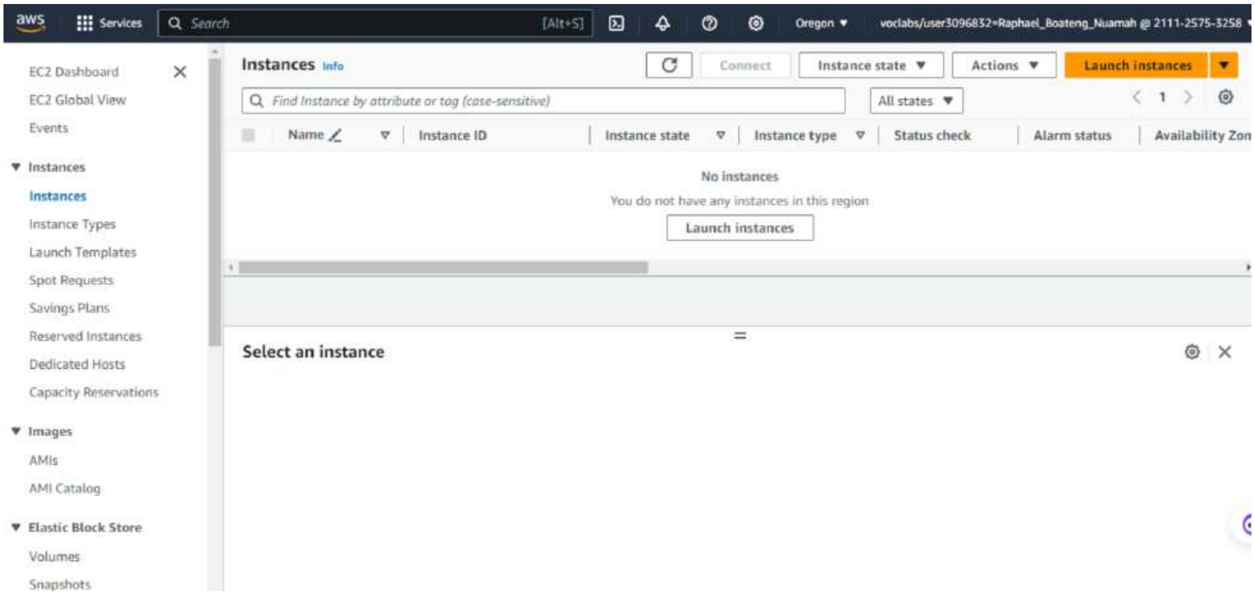


Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-00ab353522d9d25a3	All ICMP - IPv4 ▾	ICMP	All	Cust... ▾	sg-042b369569cc6bc9c ✕		Delete
sgr-02eda449d052decf1	SSH ▾	TCP	22	Cust... ▾	sg-0dde371c00366c676 ✕		Delete
-	MYSQL/Aurora ▾	TCP	3306	Cust... ▾	sg-0ca7495b0b24 ✕ sg-0ca7495b0b246f5a4 ✕		Delete
-	HTTP ▾	TCP	80	Any... ▾	0.0.0.0/0 0.0.0.0/0 ✕		Delete
-	HTTPS ▾	TCP	443	Any... ▾	0.0.0.0/0 0.0.0.0/0 ✕		Delete

Step 2: Create Servers

Create Bastion Host

- EC2 instance
    - Amazon linux 2 ami
    - T2.micro
    - Use your vpc and public subnet
    - Use Security Group for Bastion Host made in VPC Setup

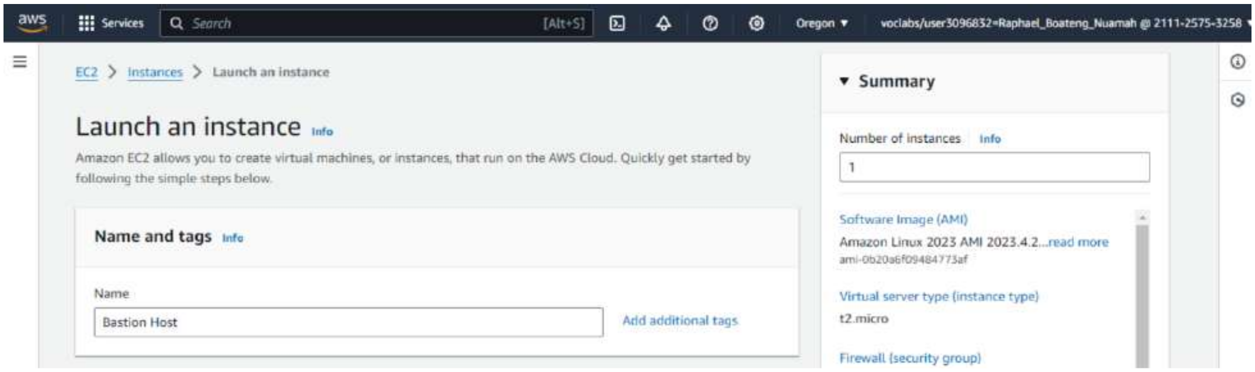


Instances Info

No instances

You do not have any instances in this region

Select an instance


aws
Services
Search
[Alt+S]
Oregon ▼
voclabs/user3096832=Raphael_Boateng_Nuamah @ 2111-2575-3258
EC2 > Instances > Launch an instance
Info
Add additional tags

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name: Bastion Host

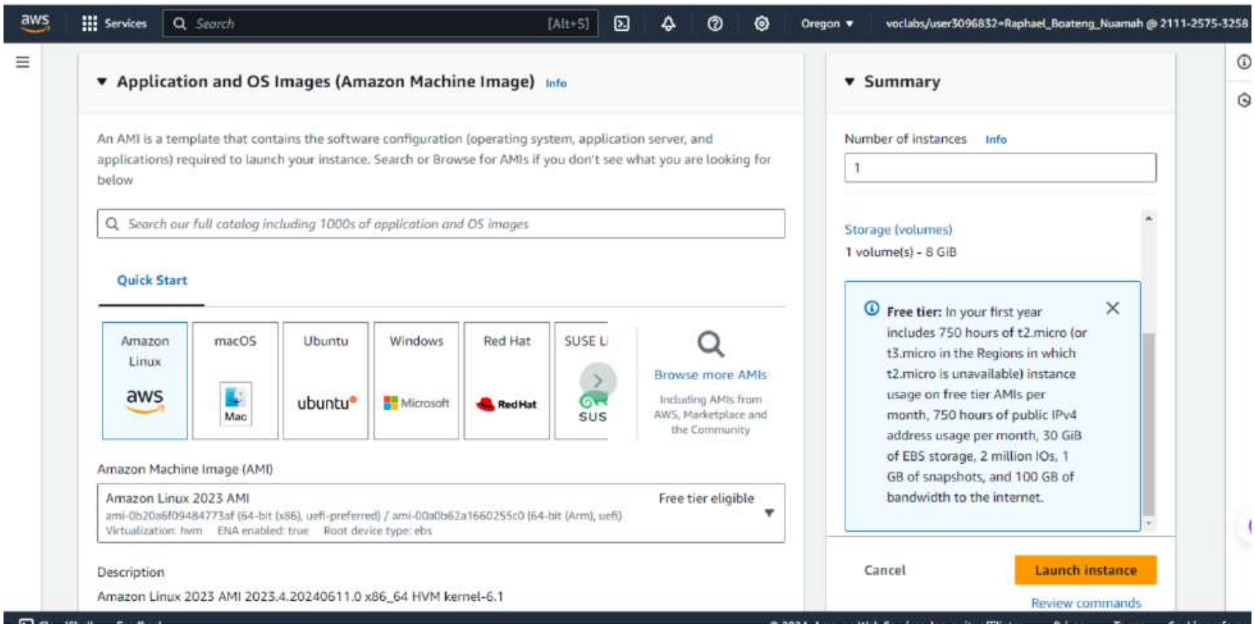
▼ Summary

Number of instances Info: 1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.4.2...read more
ami-0b20a6f09484773af

Virtual server type (instance type)
t2.micro

Firewall (security group)



▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI — Free tier eligible
ami-0b20a6f09484773af (64-bit (x86), uefi-preferred) / ami-00a0b62a1660255c0 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

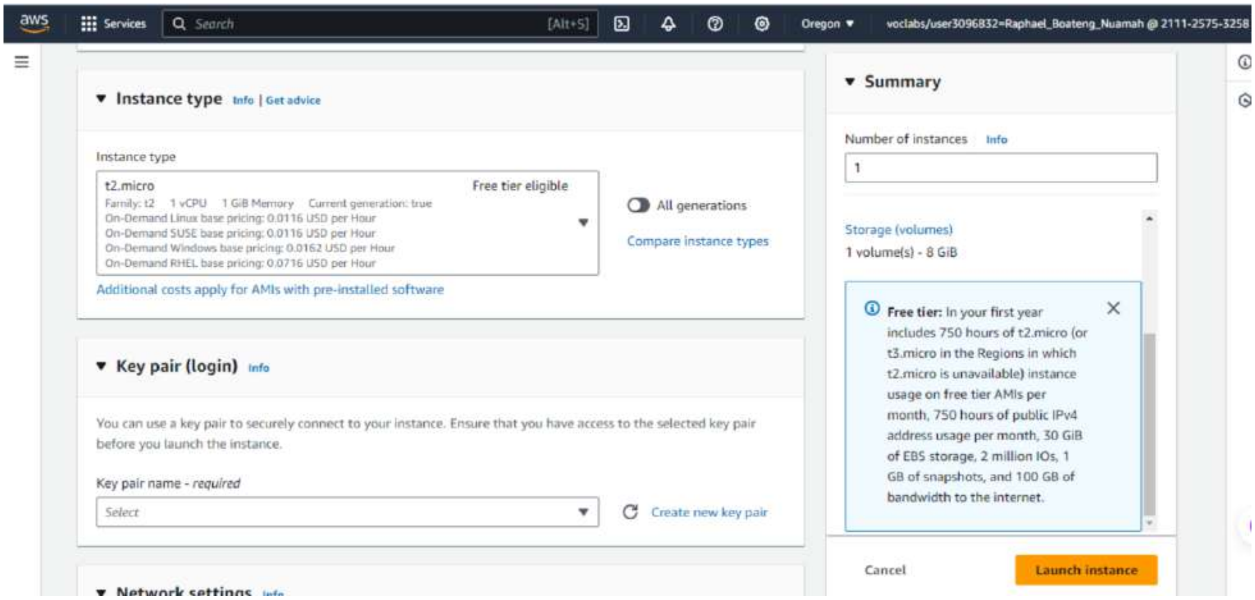
Amazon Linux 2023 AMI 2023.4.20240611.0 x86_64 HVM kernel-6.1

▼ Summary

Number of instances Info: 1

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 t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.



▼ 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

▼ 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*

Select

Create new key pair

▼ Network settings Info

▼ Summary

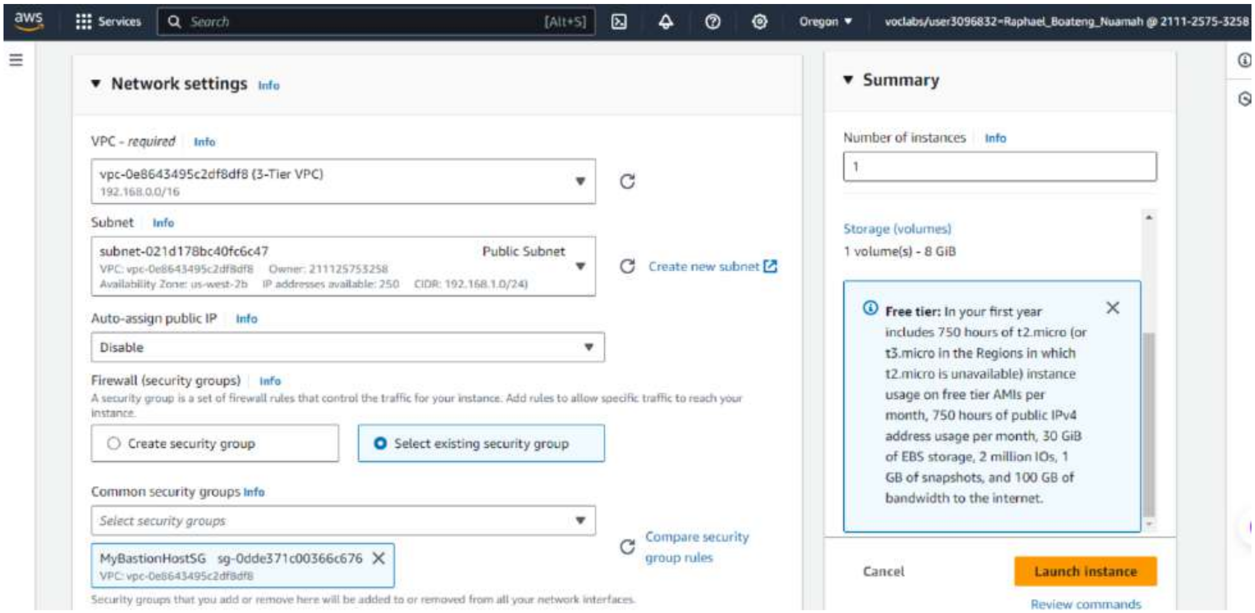
Number of instances Info

1

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 t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.



▼ Network settings Info

VPC - *required* Info

vpc-0e8643495c2df8df8 (3-Tier VPC)
192.168.0.0/16

Subnet Info

subnet-021d178bc40fc6c47 Public Subnet
VPC: vpc-0e8643495c2df8df8 Owner: 211125753258
Availability Zone: us-west-2b IP addresses available: 250 CIDR: 192.168.1.0/24)

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

MyBastionHostSG sg-0dde371c00366c676 ✕
VPC: vpc-0e8643495c2df8df8

Compare security group rules

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

▼ Summary

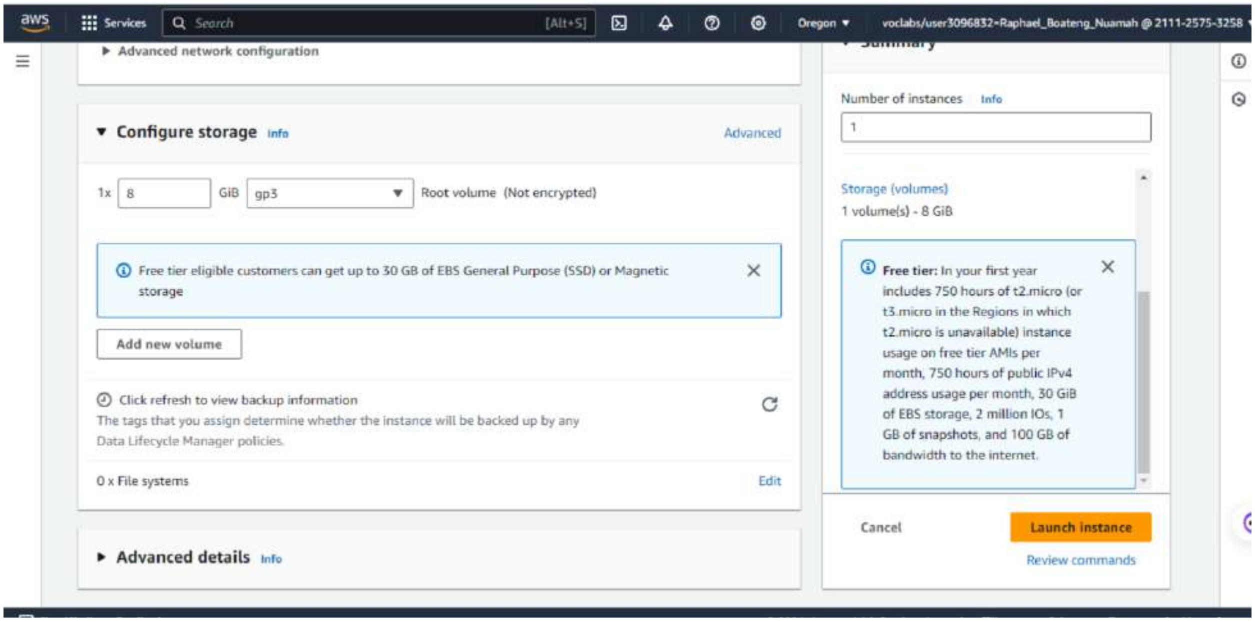
Number of instances Info

1

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 t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.



Configure storage

1x 8 GiB gp3 Root volume (Not encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Click refresh to view backup information
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems

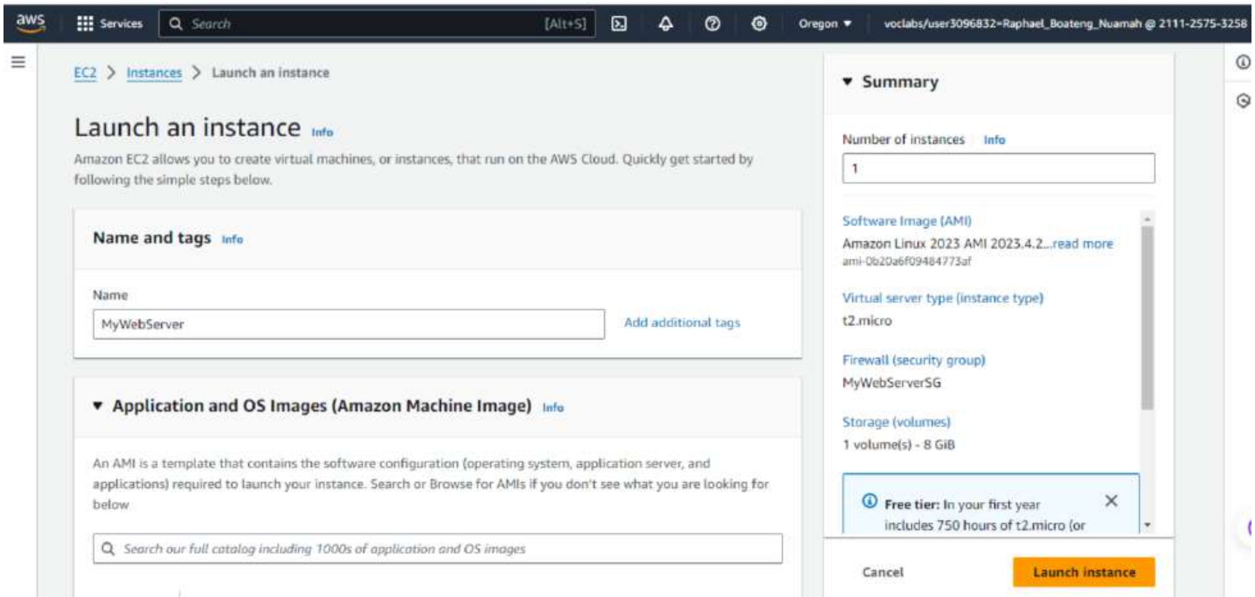
Number of instances: 1

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 t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Create Web Server

- EC2 instance
  - Amazon linux 2 ami
  - T2.micro
  - Use your vpc and public subnet
  - In user data
    - #!/bin/bash
    - sudo yum update -y
    - sudo amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
    - Sudo yum install -y httpd
    - Use sudo systemctl start httpd to start up the webserver
    - Use sudo systemctl enable httpd to do it on reboot
  - Use Security Group for Web Server made in VPC Setup



EC2 > Instances > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name: MyWebServer

Add additional tags

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

▼ Summary

Number of instances Info: 1

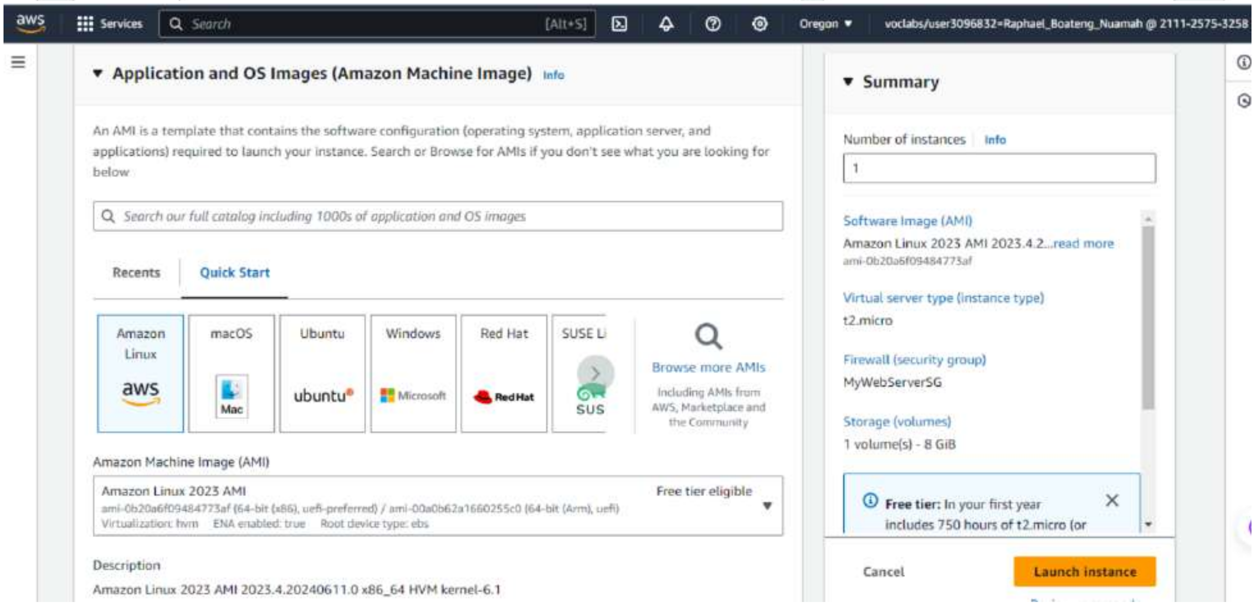
Software Image (AMI)
Amazon Linux 2023 AMI 2023.4.2...read more
ami-0b20a6f09484773af

Virtual server type (instance type)
t2.micro

Firewall (security group)
MyWebServerSG

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or



▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI — Free tier eligible
ami-0b20a6f09484773af (64-bit (x86), uefi-preferred) / ami-00a0b62a1660255c0 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description
Amazon Linux 2023 AMI 2023.4.20240611.0 x86_64 HVM kernel-6.1

▼ Summary

Number of instances Info: 1

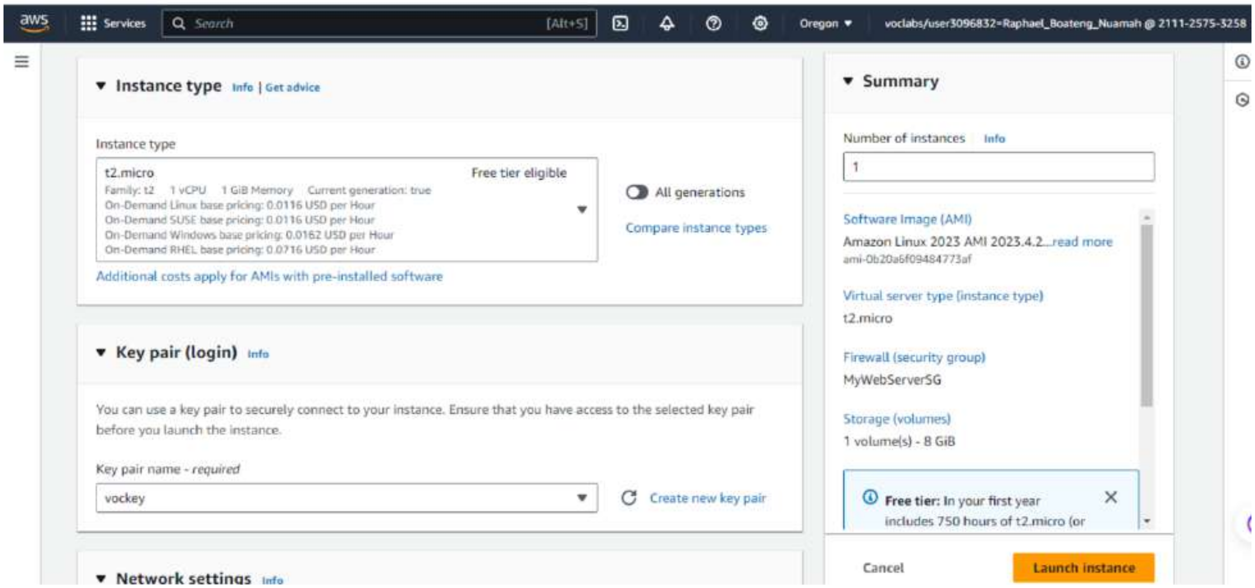
Software Image (AMI)
Amazon Linux 2023 AMI 2023.4.2...read more
ami-0b20a6f09484773af

Virtual server type (instance type)
t2.micro

Firewall (security group)
MyWebServerSG

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or



▾ 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

▾ 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

▾ Network settings Info

▾ Summary

Number of instances Info: 1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.4.2...read more
ami-0b20a6f09484773af

Virtual server type (instance type)
t2.micro

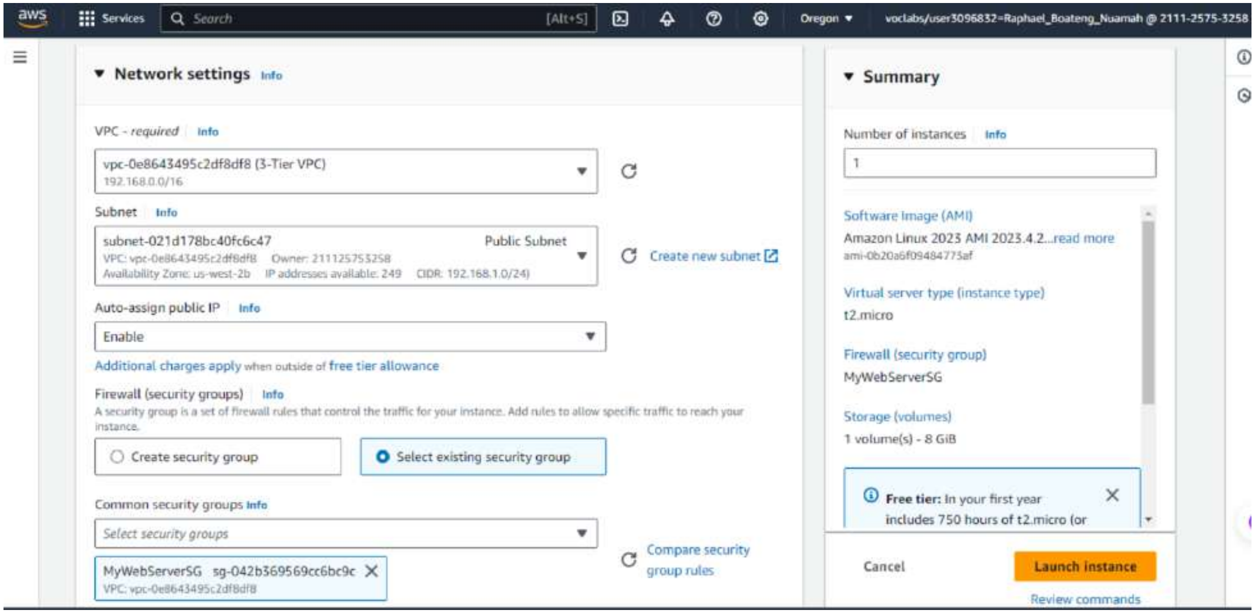
Firewall (security group)
MyWebServerSG

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or

Cancel

Launch instance



▾ Network settings Info

VPC - *required* Info

vpc-0e8643495c2df8df8 (3-Tier VPC)
192.168.0.0/16

Subnet Info

subnet-021d178bc40fc6c47 — Public Subnet
VPC: vpc-0e8643495c2df8df8 Owner: 211125753258
Availability Zone: us-west-2b IP addresses available: 249 CIDR: 192.168.1.0/24)

Create new subnet

Auto-assign public IP Info: Enable

Additional charges apply when outside of free tier allowance

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

MyWebServerSG sg-042b369569cc6bc9c
VPC: vpc-0e8643495c2df8df8

Compare security group rules

▾ Summary

Number of instances Info: 1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.4.2...read more
ami-0b20a6f09484773af

Virtual server type (instance type)
t2.micro

Firewall (security group)
MyWebServerSG

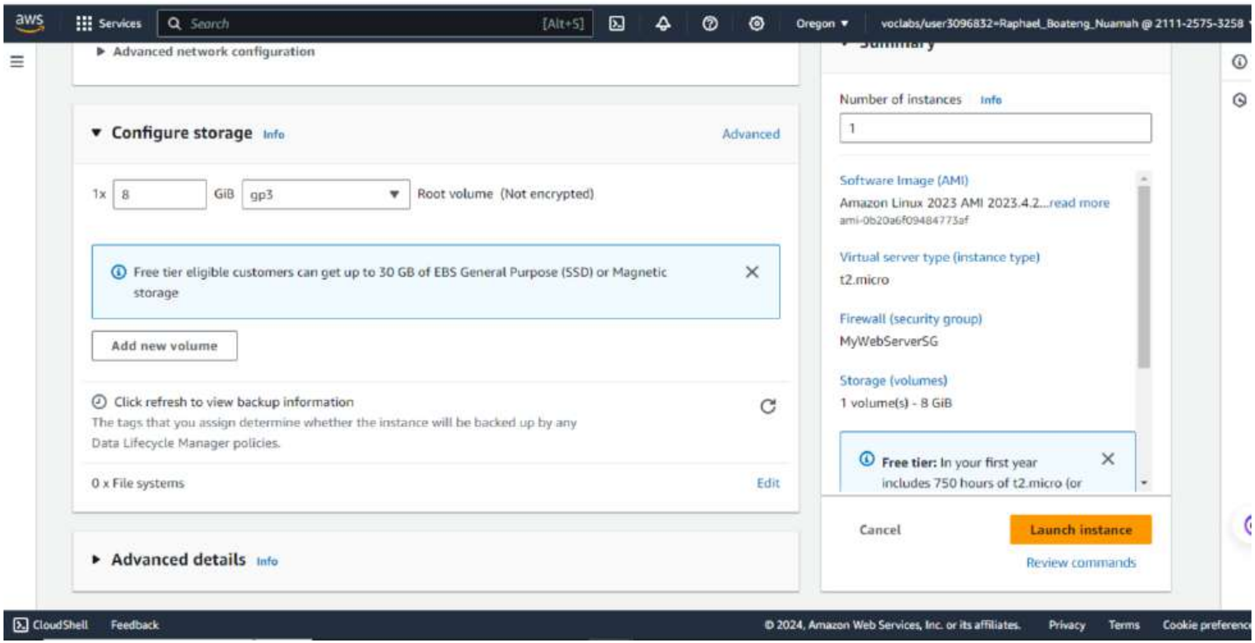
Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or

Cancel

Launch instance

Review commands



aws
Services
Search
[Alt+S]
Oregon ▼
voclabs/user3096832=Raphael_Boateng_Nuamah @ 2111-2575-3258
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferenc

▶ Advanced network configuration

▼ Configure storage Info Advanced

1x 8 GiB gp3 ▼ Root volume (Not encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage ✕

Add new volume

Click refresh to view backup information
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems Edit

▶ Advanced details Info

Summary

Number of instances Info
1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.4.2...read more
ami-0b20a6f09484773af

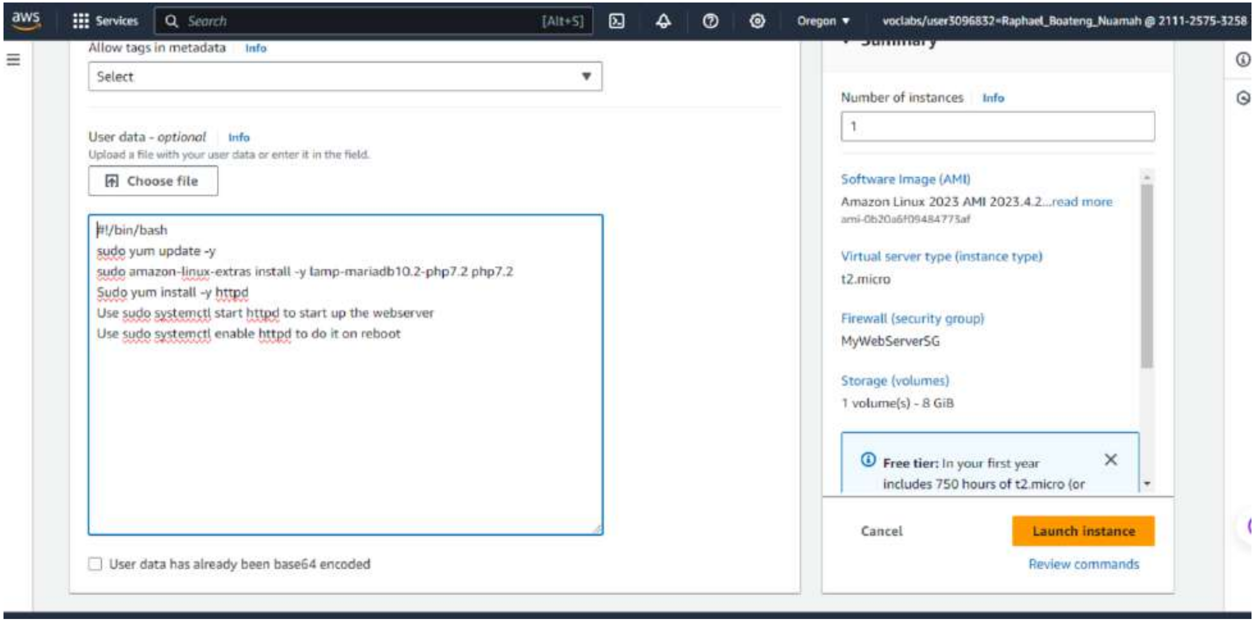
Virtual server type (instance type)
t2.micro

Firewall (security group)
MyWebServerSG

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or ✕

Cancel Launch instance
Review commands



Allow tags in metadata Info
Select ▼

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
Use sudo systemctl start httpd to start up the webserver
Use sudo systemctl enable httpd to do it on reboot
```

□ User data has already been base64 encoded

Summary

Number of instances Info
1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.4.2...read more
ami-0b20a6f09484773af

Virtual server type (instance type)
t2.micro

Firewall (security group)
MyWebServerSG

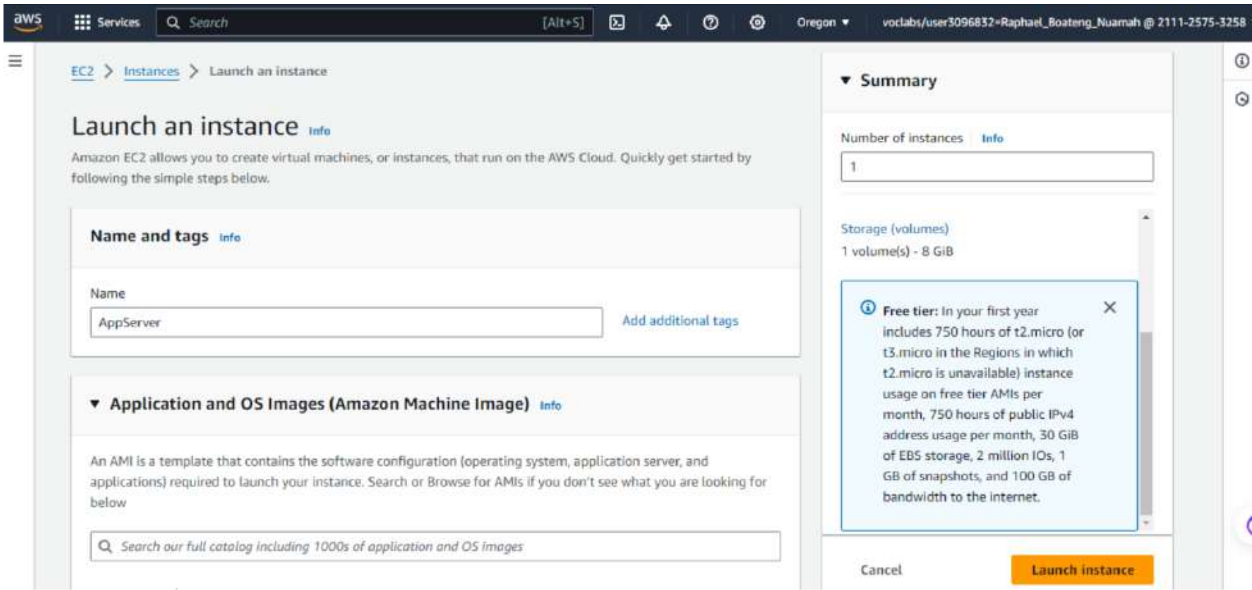
Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or ✕

Cancel Launch instance
Review commands

Create App Server

- EC2 instance
  - Amazon linux 2 ami
  - T2.micro
  - Use your vpc and private subnet
  - Type into user data
    - #!/bin/bash
    - sudo yum install -y mariadb-server
    - Sudo service mariadb start
  - Use Security Group for App Server made in VPC Setup


aws
Services
Search
[Alt+S]
Oregon ▾
voclabs/user3096832=Raphael_Boateng_Nuamah @ 2111-2575-3258
EC2 > Instances > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name: AppServer

▾ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

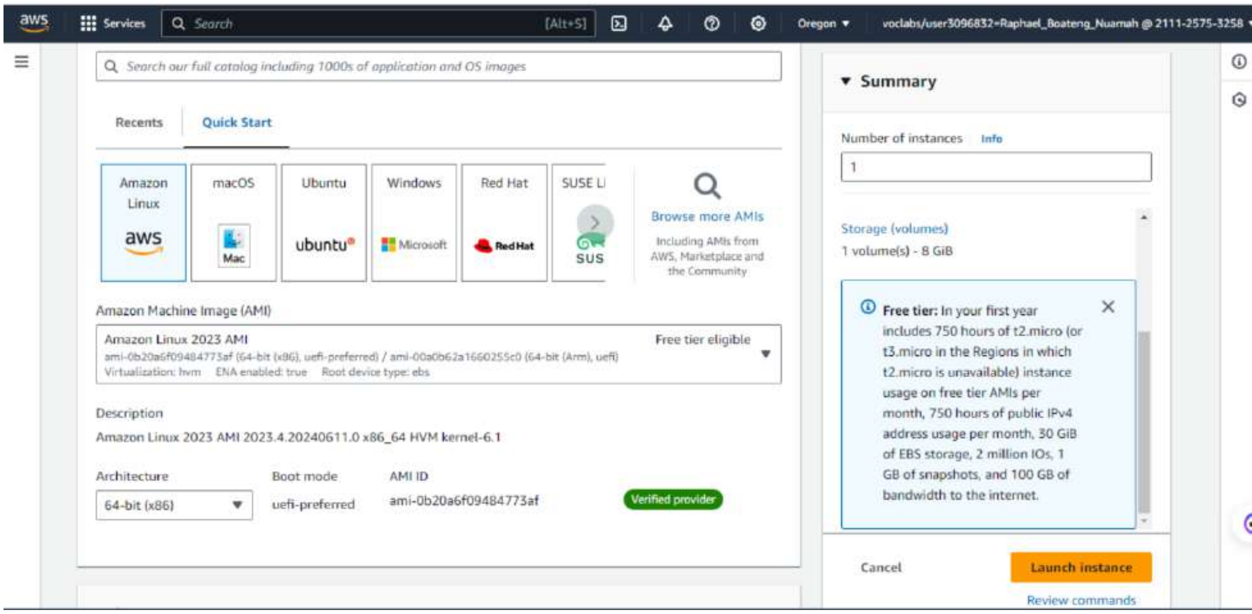
Search our full catalog including 1000s of application and OS images

▾ Summary

Number of instances Info: 1

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 t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.


aws
Services
Search
[Alt+S]
Oregon ▾
voclabs/user3096832=Raphael_Boateng_Nuamah @ 2111-2575-3258
Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Amazon Linux
aws
macOS
Mac
Ubuntu
ubuntu
Windows
Microsoft
Red Hat
Red Hat
SUSE Li
SUS
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI — Free tier eligible
ami-0b20a6f09484773af (64-bit (x86), uefi-preferred) / ami-00a0b62a1660255c0 (64-bit (Arm), uefi)
Virtualization: hvm   ENA enabled: true   Root device type: ebs

Description
Amazon Linux 2023 AMI 2023.4.20240611.0 x86_64 HVM kernel-6.1

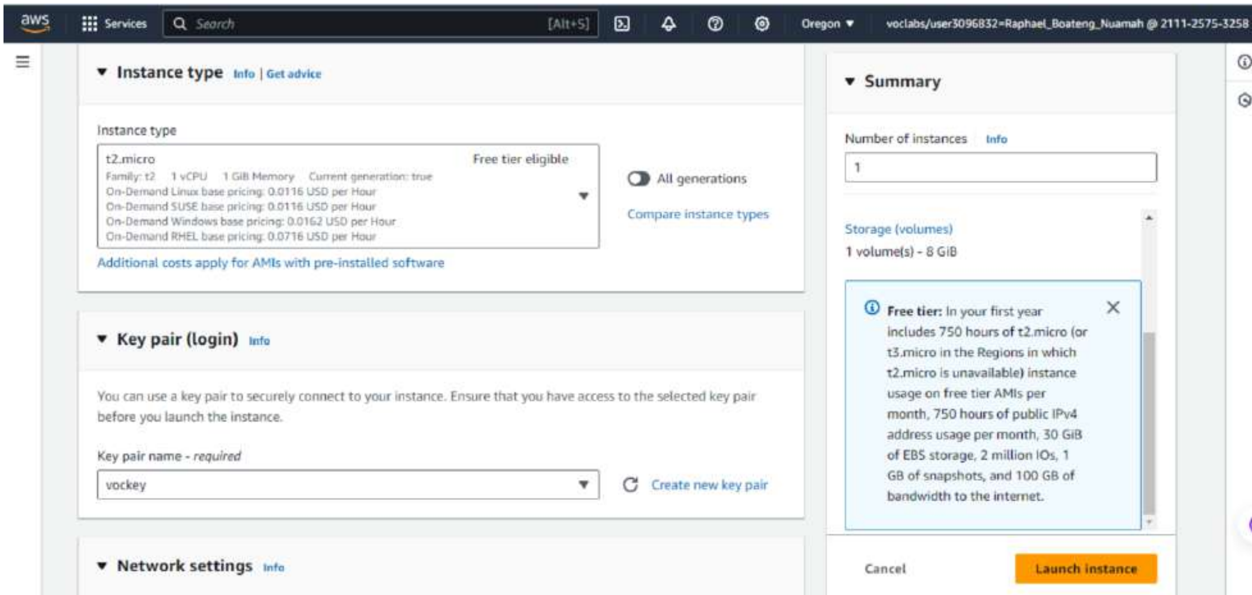
Architecture	Boot mode	AMI ID	
64-bit (x86) ▾	uefi-preferred	ami-0b20a6f09484773af	Verified provider

▾ Summary

Number of instances Info: 1

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 t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.



▼ 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

Additional costs apply for AMIs with pre-installed software

▼ 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

▼ Network settings Info

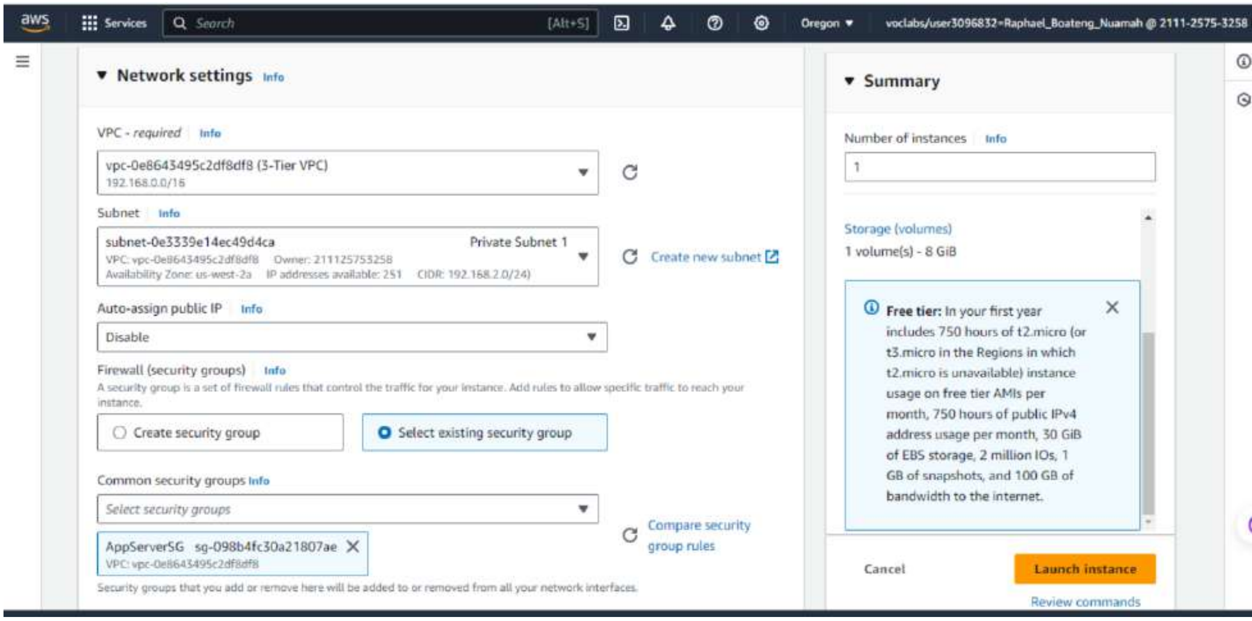
▼ Summary

Number of instances Info

1

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 t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.



▼ Network settings Info

VPC - *required* Info

vpc-0e8643495c2df8df8 (3-Tier VPC)
192.168.0.0/16

Subnet Info

subnet-0e3339e14ec49d4ca Private Subnet 1
VPC: vpc-0e8643495c2df8df8 Owner: 211125753258
Availability Zone: us-west-2a IP addresses available: 251 CIDR: 192.168.2.0/24)

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

AppServerSG sg-098b4fc30a21807ae
VPC: vpc-0e8643495c2df8df8

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

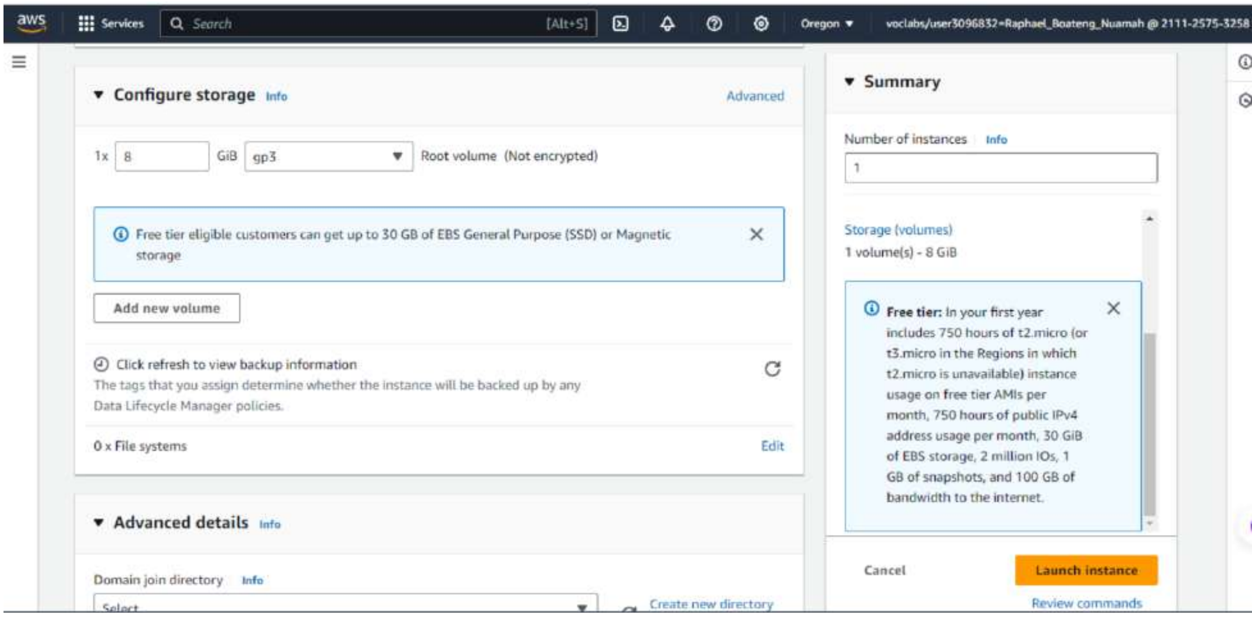
▼ Summary

Number of instances Info

1

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 t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.



▾ Configure storage Info — Advanced

1x 8 GiB gp3 ▾ Root volume (Not encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Add new volume

Click refresh to view backup information
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems — Edit

▾ Advanced details Info

Domain join directory Info
Select ▾ — Create new directory

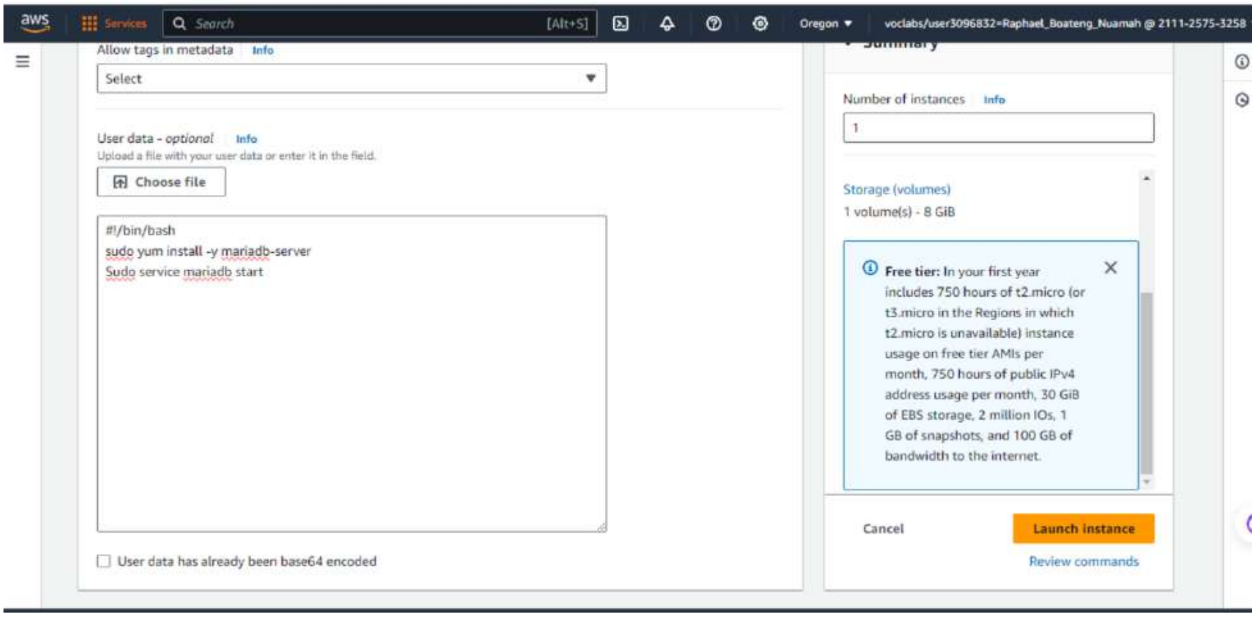
▾ Summary

Number of instances Info
1

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 t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel — Launch instance
Review commands



Allow tags in metadata Info
Select ▾

User data - *optional* Info
Upload a file with your user data or enter it in the field.
Choose file

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

□ User data has already been base64 encoded

Summary

Number of instances Info
1

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 t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

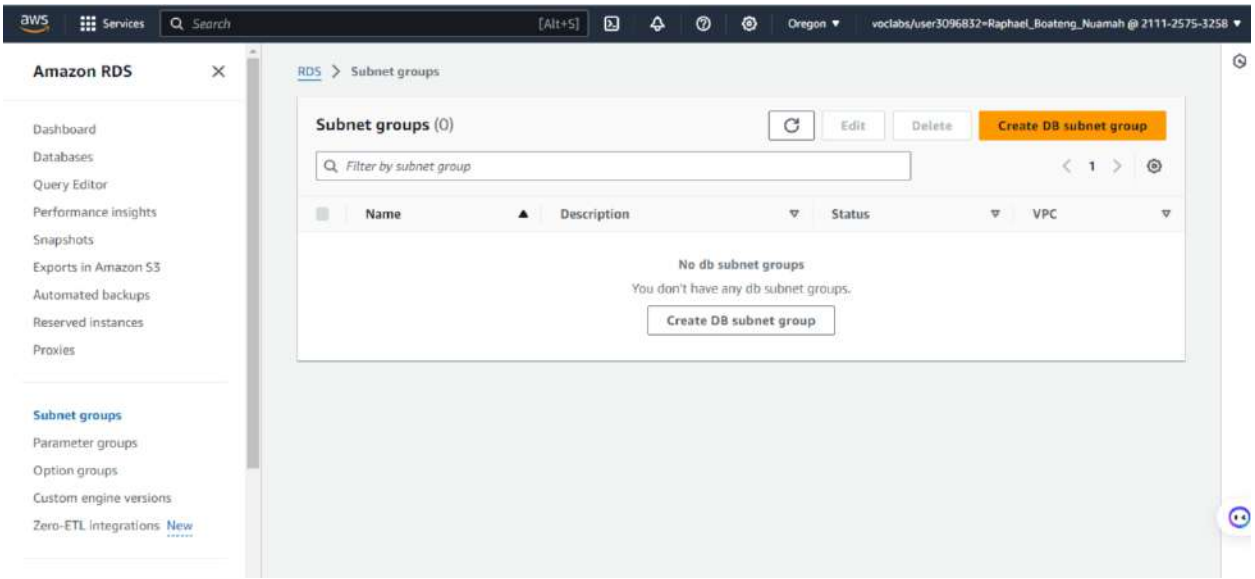
Cancel — Launch instance
Review commands

Create DB instance

- Create a subnet group
- Make a database instance
  - Standard create
  - mariadb
  - Free Tier
  - Disable automated backups
  - Disable encryption
  - User = root
  - Password = Re:Start!9
  - Initial database = mydb

Create a Database

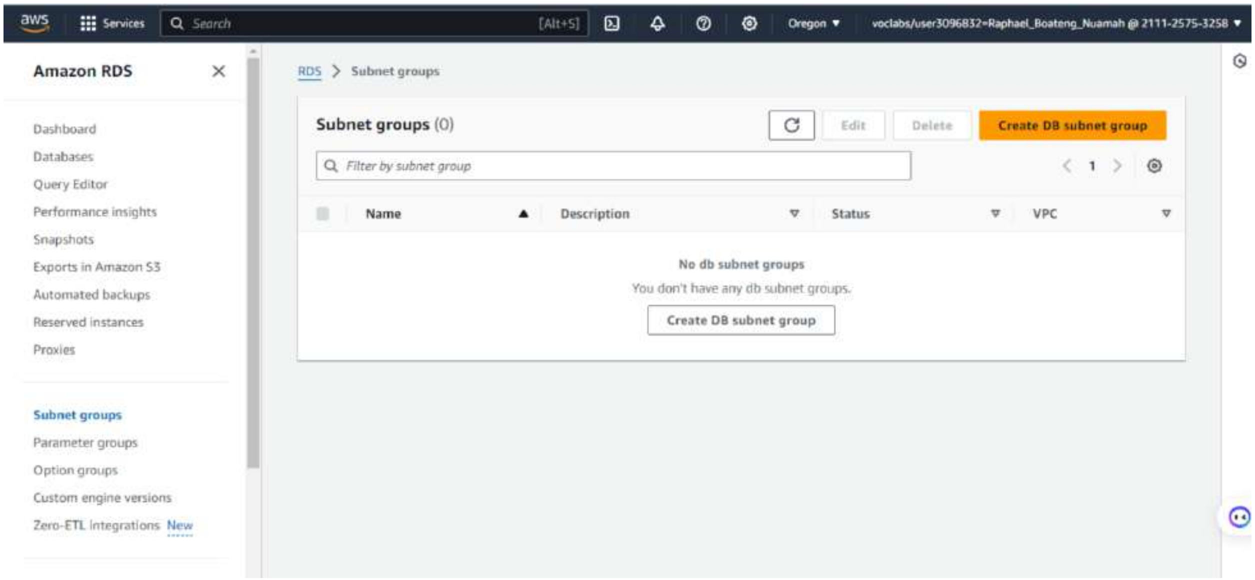
- Create a DB subnet group by first heading to the Amazon RDS service page on the AWS management console
- Click on Subnet Groups on the left hand side and the click on “Create DB subnet group”



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

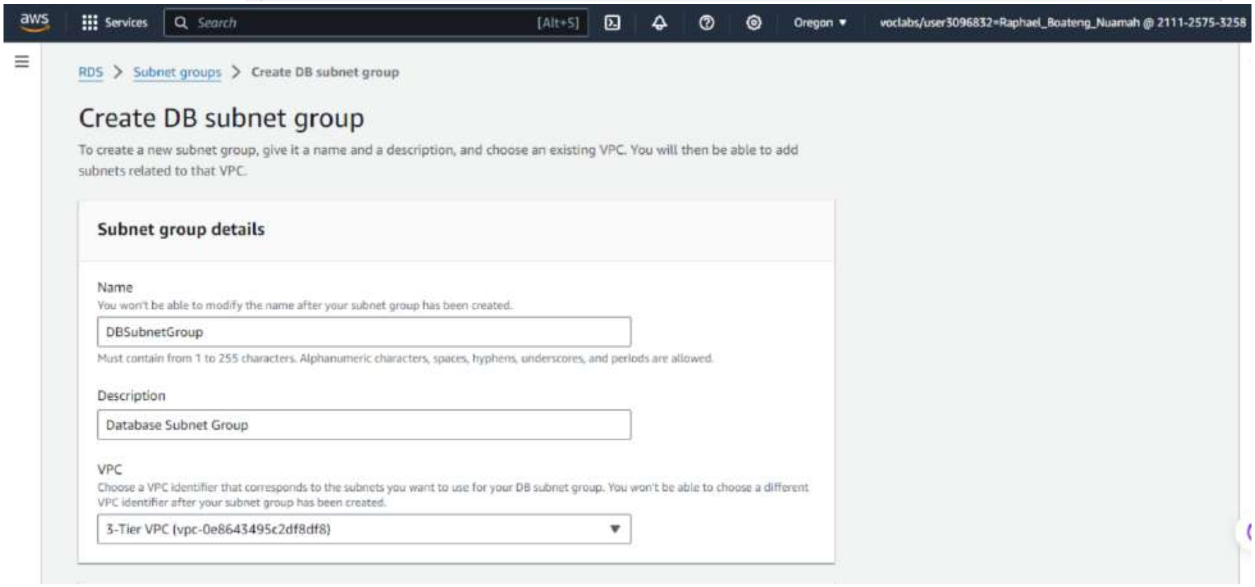


Subnet groups (0)

No db subnet groups

You don't have any db subnet groups.

Create DB subnet group


aws
Services
Search
[Alt+S]
Oregon ▼
voclabs/user3096832=Raphael_Boateng_Nuamah @ 2111-2575-3258
RDS > Subnet groups > Create DB subnet group

Create DB subnet group

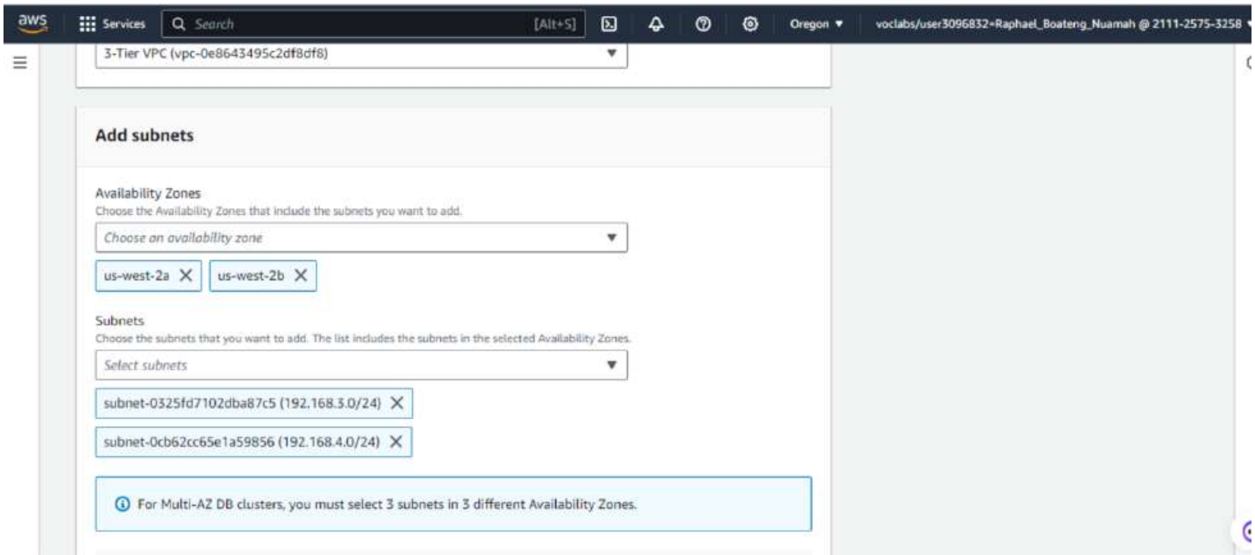
To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.

Subnet group details

Name
You won't be able to modify the name after your subnet group has been created.
DBSubnetGroup
Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

Description
Database Subnet Group

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.
3-Tier VPC (vpc-0e8643495c2df8df8)



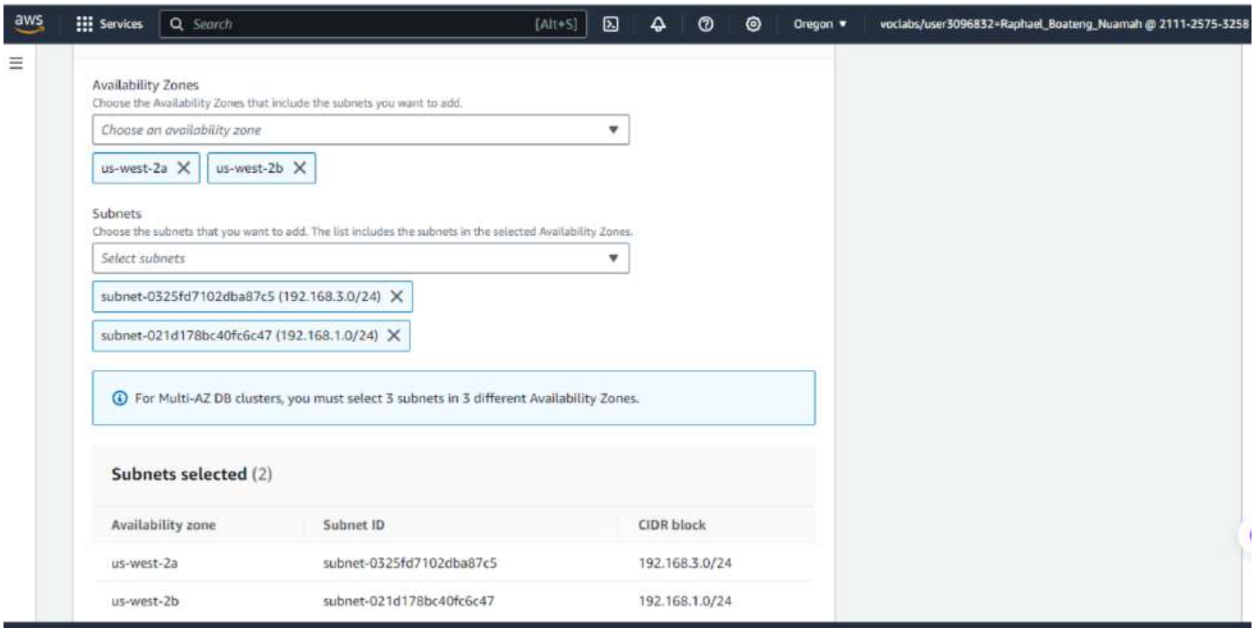
3-Tier VPC (vpc-0e8643495c2df8df8)

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-0325fd7102dba87c5 (192.168.3.0/24)
subnet-0cb62cc65e1a59856 (192.168.4.0/24)

For Multi-AZ DB clusters, you must select 3 subnets in 3 different Availability Zones.



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-0325fd7102dba87c5 (192.168.3.0/24) ✕

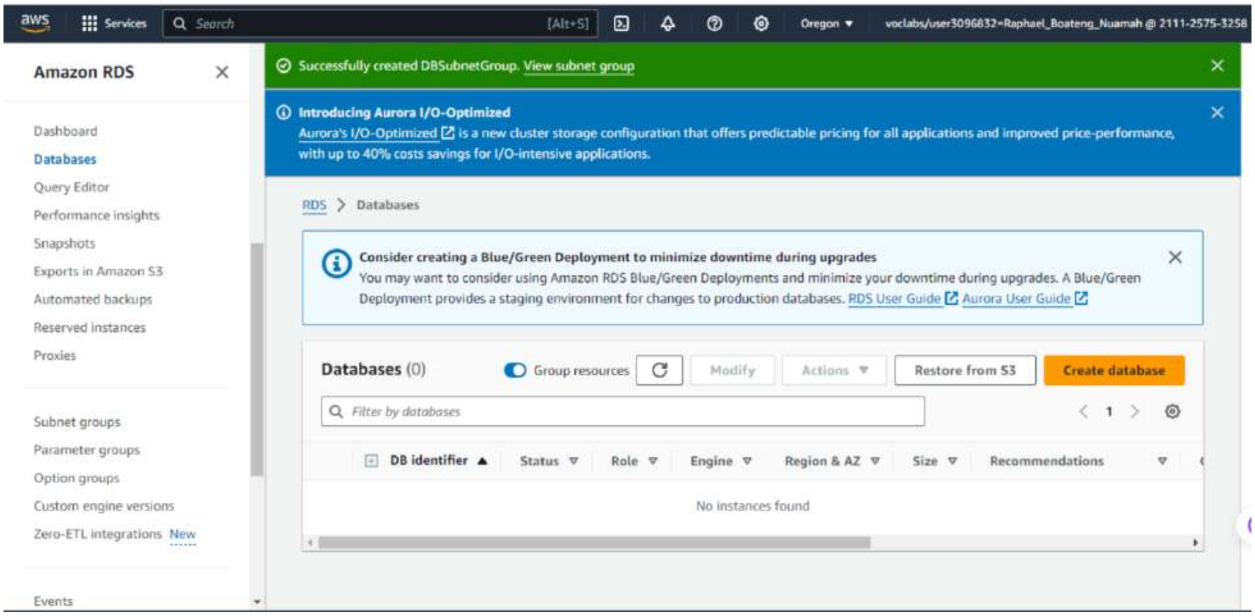
subnet-021d178bc40fc6c47 (192.168.1.0/24) ✕

For Multi-AZ DB clusters, you must select 3 subnets in 3 different Availability Zones.

Subnets selected (2)

Availability zone	Subnet ID	CIDR block
us-west-2a	subnet-0325fd7102dba87c5	192.168.3.0/24
us-west-2b	subnet-021d178bc40fc6c47	192.168.1.0/24

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



Successfully created DBSubnetGroup. View subnet group

Introducing Aurora I/O-Optimized
Aurora's I/O-Optimized is a new cluster storage configuration that offers predictable pricing for all applications and improved price-performance, with up to 40% costs savings for I/O-intensive applications.

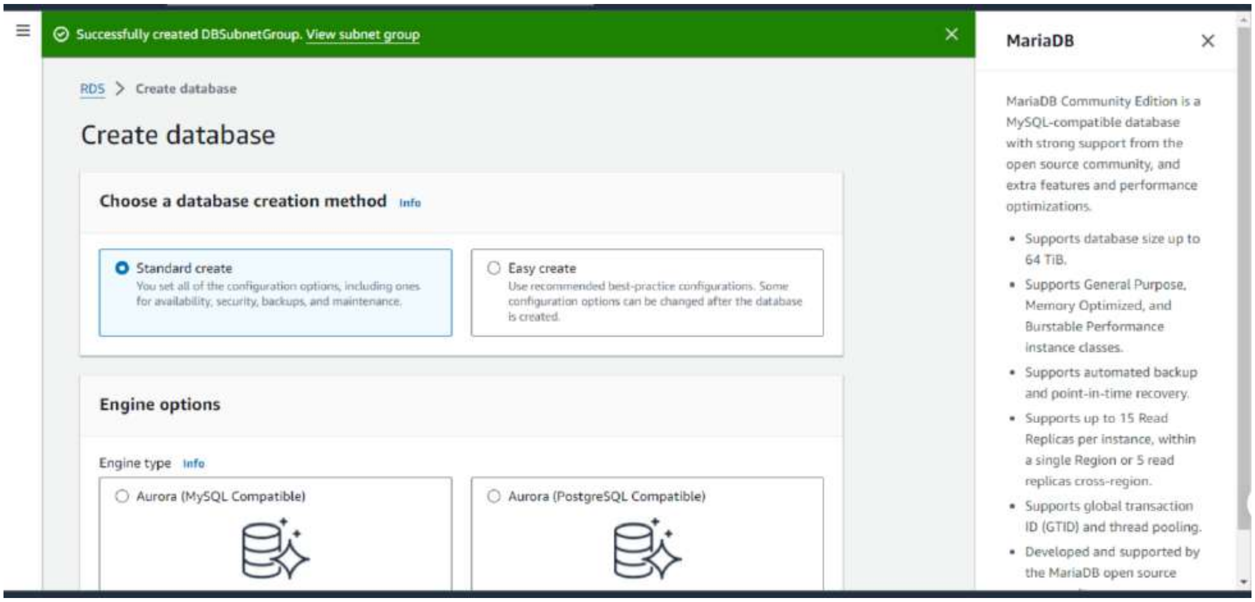
Consider creating a Blue/Green Deployment to minimize downtime during upgrades
You may want to consider using Amazon RDS Blue/Green Deployments and minimize your downtime during upgrades. A Blue/Green Deployment provides a staging environment for changes to production databases. RDS User Guide Aurora User Guide

Databases (0)

DB identifier ▲	Status ▾	Role ▾	Engine ▾	Region & AZ ▾	Size ▾	Recommendations ▾

No instances found

- Click on Standard create and MariaDB for the engine type


Successfully created DBSubnetGroup. View subnet group

RDS > Create database

Create database

Choose a database creation method Info

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

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

Engine options

Engine type Info

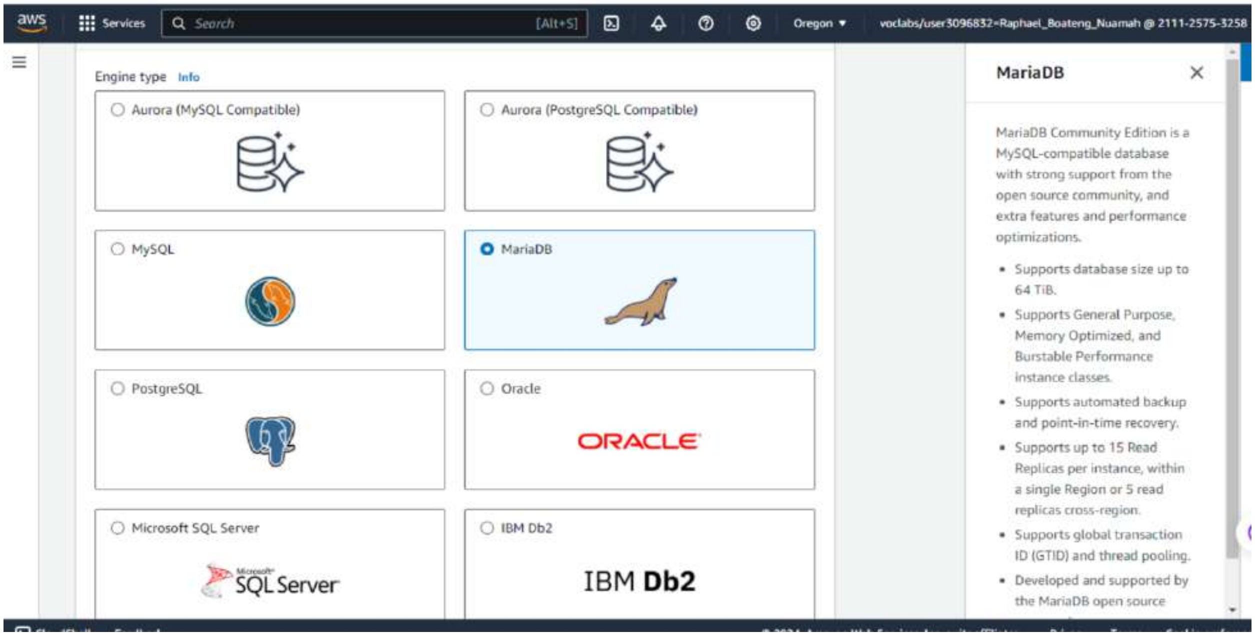
○ Aurora (MySQL Compatible)

○ Aurora (PostgreSQL Compatible)

MariaDB

MariaDB Community Edition is a MySQL-compatible database with strong support from the open source community, and extra features and performance optimizations.

- Supports database size up to 64 TiB.
- Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
- Supports automated backup and point-in-time recovery.
- Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.
- Supports global transaction ID (GTID) and thread pooling.
- Developed and supported by the MariaDB open source



Engine type Info

○ Aurora (MySQL Compatible)

○ Aurora (PostgreSQL Compatible)

○ MySQL

● MariaDB

○ PostgreSQL

○ Oracle

○ Microsoft SQL Server

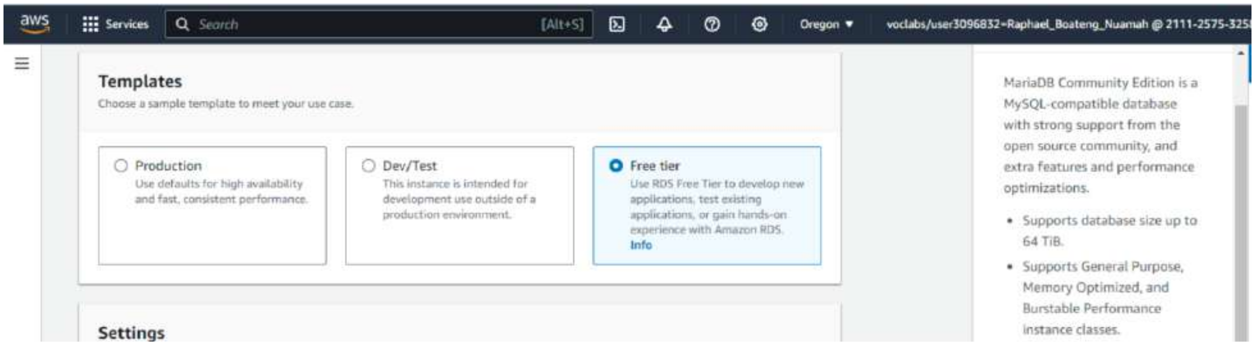
○ IBM Db2

MariaDB

MariaDB Community Edition is a MySQL-compatible database with strong support from the open source community, and extra features and performance optimizations.

- Supports database size up to 64 TiB.
- Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
- Supports automated backup and point-in-time recovery.
- Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.
- Supports global transaction ID (GTID) and thread pooling.
- Developed and supported by the MariaDB open source

- Make sure you click on Free tier here



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

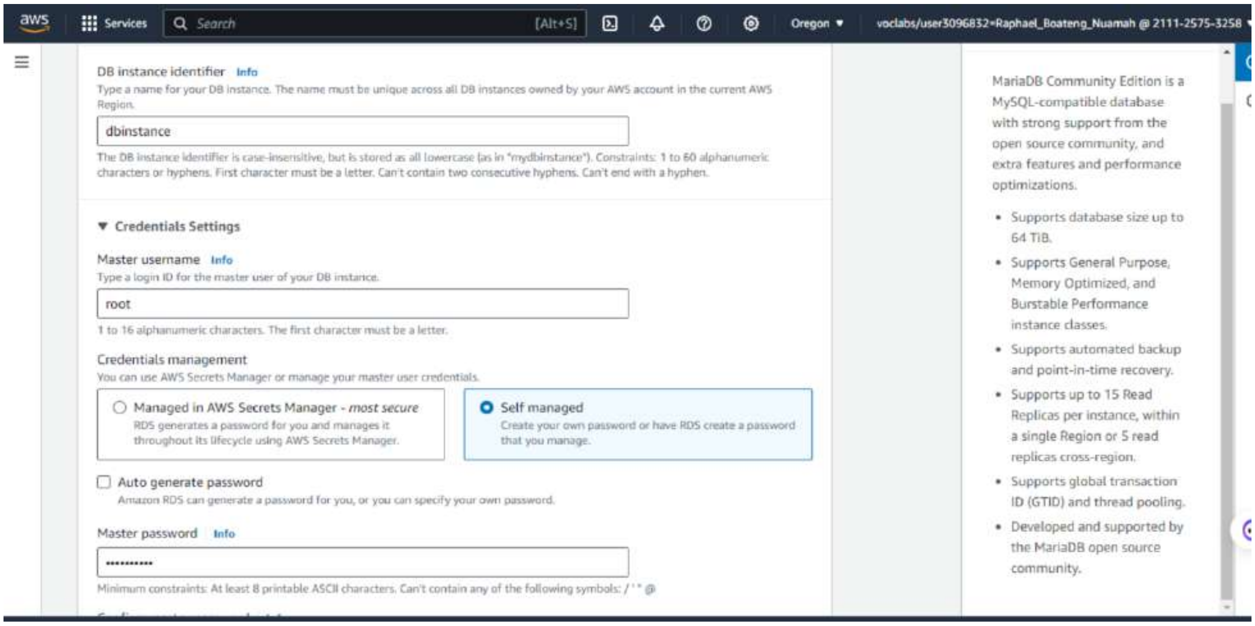
Settings

MariaDB Community Edition is a MySQL-compatible database with strong support from the open source community, and extra features and performance optimizations.

- Supports database size up to 64 TiB.
- Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.

- 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



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. The first character must be a letter.

Credentials management
You can use AWS Secrets Manager or manage your master user credentials.

○ Managed in AWS Secrets Manager - *most secure*
RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.

● Self managed
Create your own password or have RDS create a password that you manage.

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

Master password Info

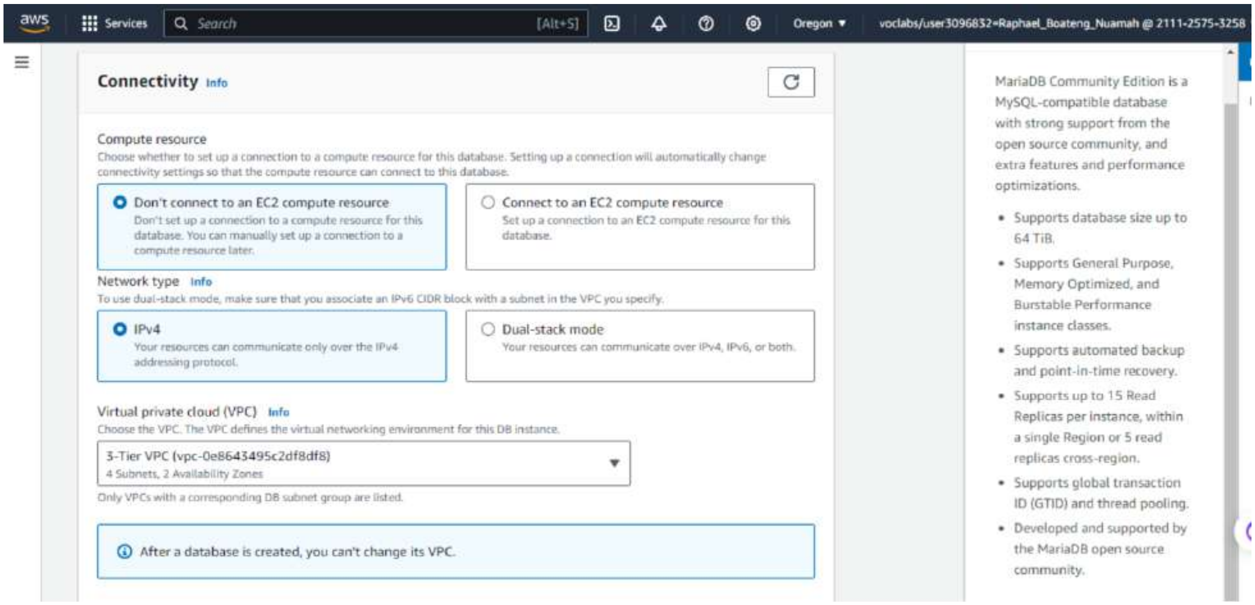
••••••••••

Minimum constraints: At least 8 printable ASCII characters. Can't contain any of the following symbols: / ' " @

MariaDB Community Edition is a MySQL-compatible database with strong support from the open source community, and extra features and performance optimizations.

- Supports database size up to 64 TiB.
- Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
- Supports automated backup and point-in-time recovery.
- Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.
- Supports global transaction ID (GTID) and thread pooling.
- Developed and supported by the MariaDB open source community.

- 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 Info

Compute resource

Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

● Don't connect to an EC2 compute resource
Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

○ Connect to an EC2 compute resource
Set up a connection to an EC2 compute resource for this database.

Network type Info

To use dual-stack mode, make sure that you associate an IPv6 CIDR block with a subnet in the VPC you specify.

● IPv4
Your resources can communicate only over the IPv4 addressing protocol.

○ Dual-stack mode
Your resources can communicate over IPv4, IPv6, or both.

Virtual private cloud (VPC) Info

Choose the VPC. The VPC defines the virtual networking environment for this DB instance.

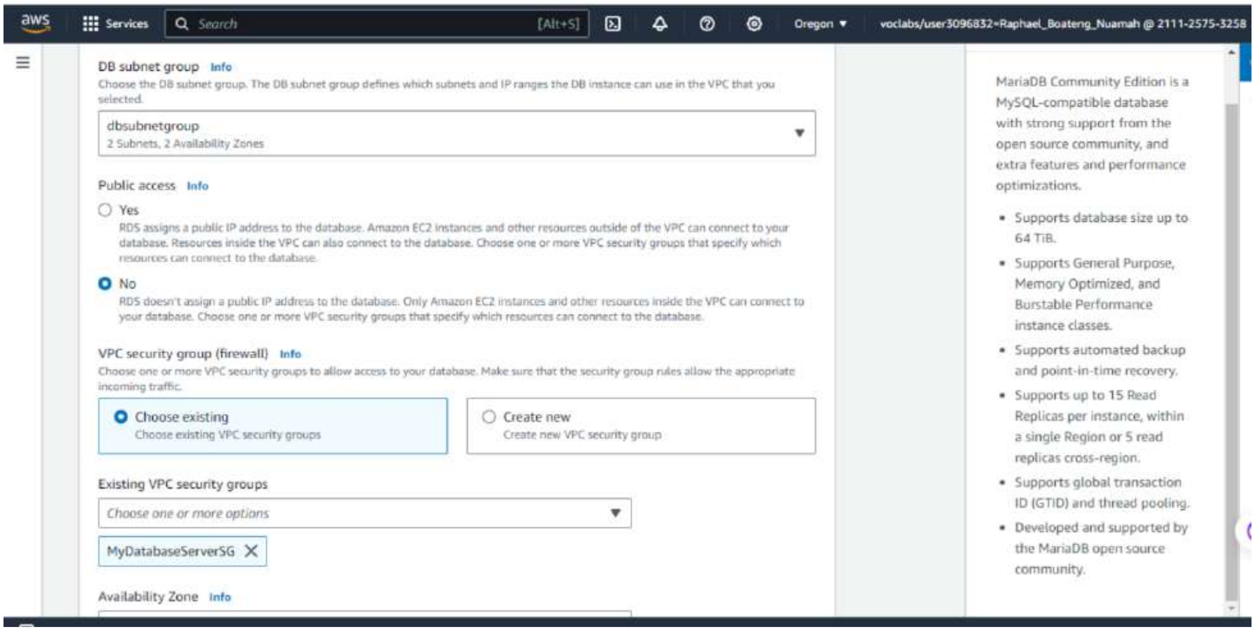
3-Tier VPC (vpc-0e8643495c2df8df8) ▼
4 Subnets, 2 Availability Zones

Only VPCs with a corresponding DB subnet group are listed.

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

MariaDB Community Edition is a MySQL-compatible database with strong support from the open source community, and extra features and performance optimizations.

- Supports database size up to 64 TiB.
- Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
- Supports automated backup and point-in-time recovery.
- Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.
- Supports global transaction ID (GTID) and thread pooling.
- Developed and supported by the MariaDB open source community.



DB subnet group Info

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

dbsubnetgroup ▼
2 Subnets, 2 Availability Zones

Public access Info

○ Yes
RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.

● No
RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database.

VPC security group (firewall) Info

Choose one or more VPC security groups to allow access to your database. Make sure 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

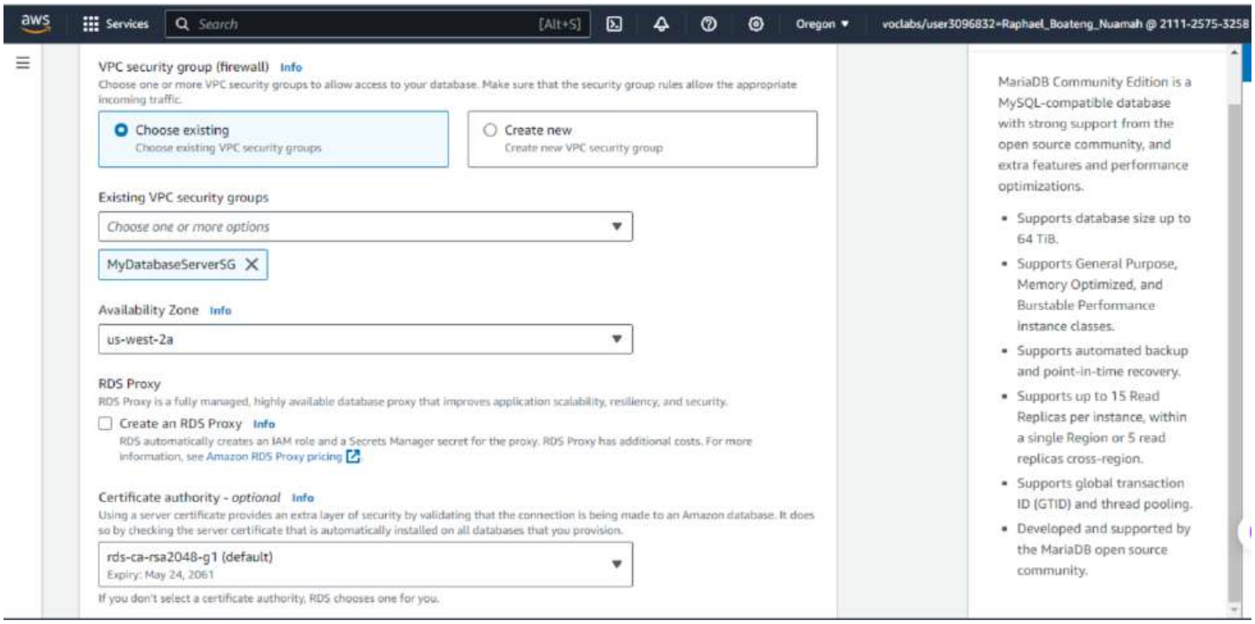
Choose one or more options ▼

MyDatabaseServerSG ✕

Availability Zone Info

MariaDB Community Edition is a MySQL-compatible database with strong support from the open source community, and extra features and performance optimizations.

- Supports database size up to 64 TiB.
- Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
- Supports automated backup and point-in-time recovery.
- Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.
- Supports global transaction ID (GTID) and thread pooling.
- Developed and supported by the MariaDB open source community.



VPC security group (firewall) Info

Choose one or more VPC security groups to allow access to your database. Make sure 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 one or more options ▾

MyDatabaseServerSG ✕

Availability Zone Info

us-west-2a ▾

RDS Proxy

RDS Proxy is a fully managed, highly available database proxy that improves application scalability, resiliency, and security.

□ Create an RDS Proxy Info
RDS automatically creates an IAM role and a Secrets Manager secret for the proxy. RDS Proxy has additional costs. For more information, see Amazon RDS Proxy pricing

Certificate authority - *optional* Info

Using a server certificate provides an extra layer of security by validating that the connection is being made to an Amazon database. It does so by checking the server certificate that is automatically installed on all databases that you provision.

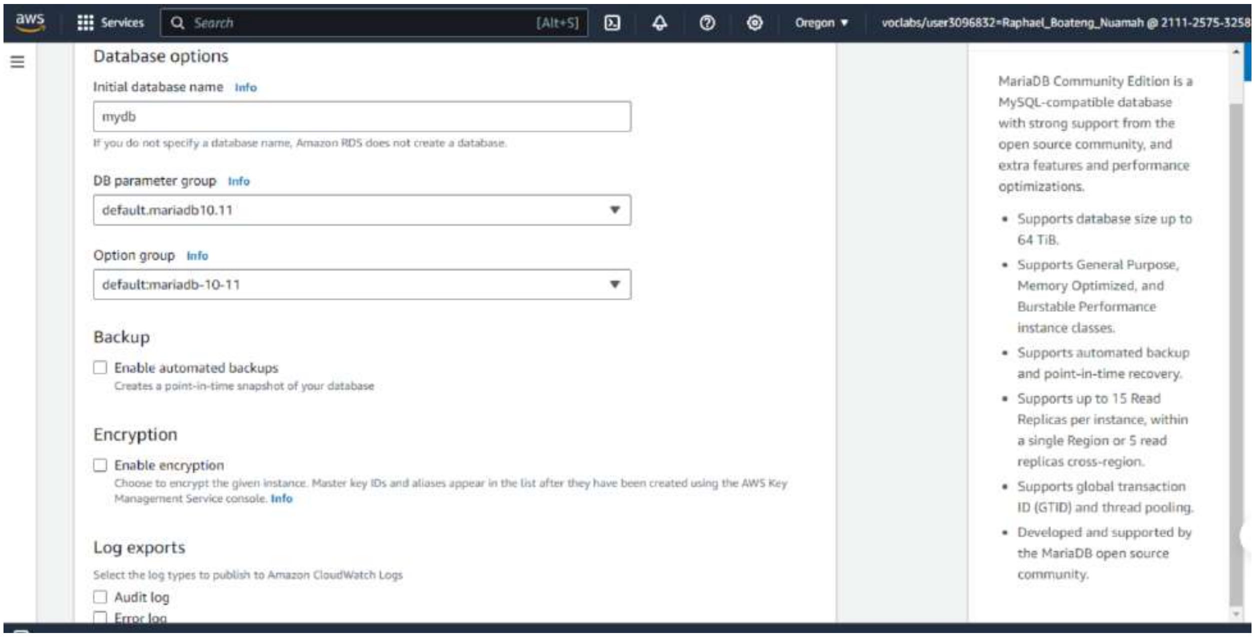
rds-ca-rsa2048-g1 (default) ▾
Expiry: May 24, 2061

If you don't select a certificate authority, RDS chooses one for you.

MariaDB Community Edition is a MySQL-compatible database with strong support from the open source community, and extra features and performance optimizations.

- Supports database size up to 64 TiB.
- Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
- Supports automated backup and point-in-time recovery.
- Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.
- Supports global transaction ID (GTID) and thread pooling.
- Developed and supported by the MariaDB open source community.

- 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



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.mariadb10.11 ▾

Option group Info

default:mariadb-10-11 ▾

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

Log exports

Select the log types to publish to Amazon CloudWatch Logs

□ Audit log

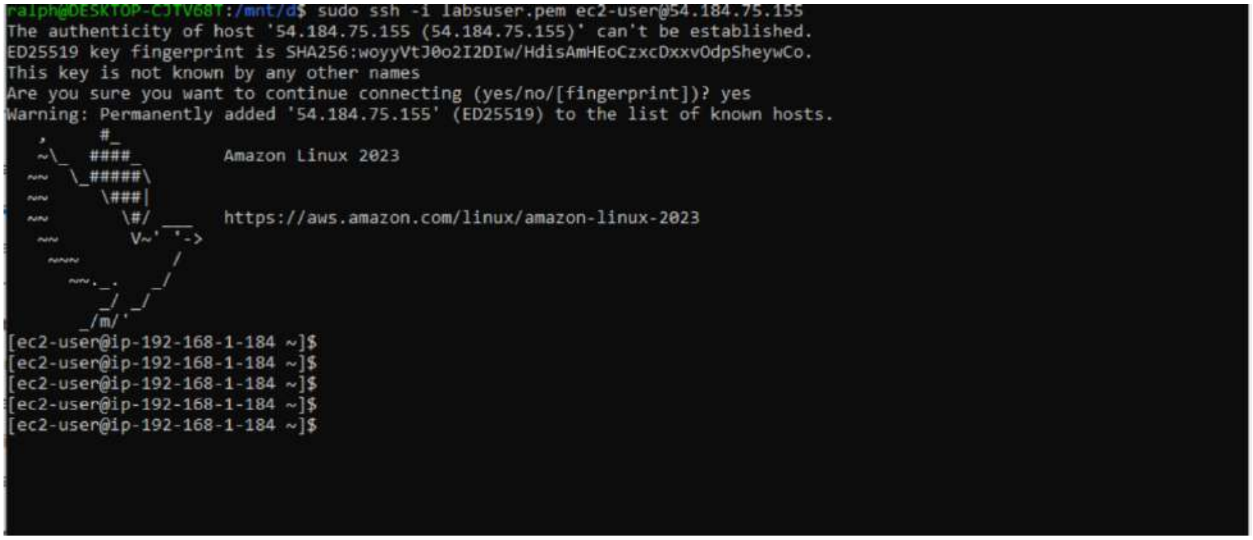
□ Error log

MariaDB Community Edition is a MySQL-compatible database with strong support from the open source community, and extra features and performance optimizations.

- Supports database size up to 64 TiB.
- Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
- Supports automated backup and point-in-time recovery.
- Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.
- Supports global transaction ID (GTID) and thread pooling.
- Developed and supported by the MariaDB open source community.

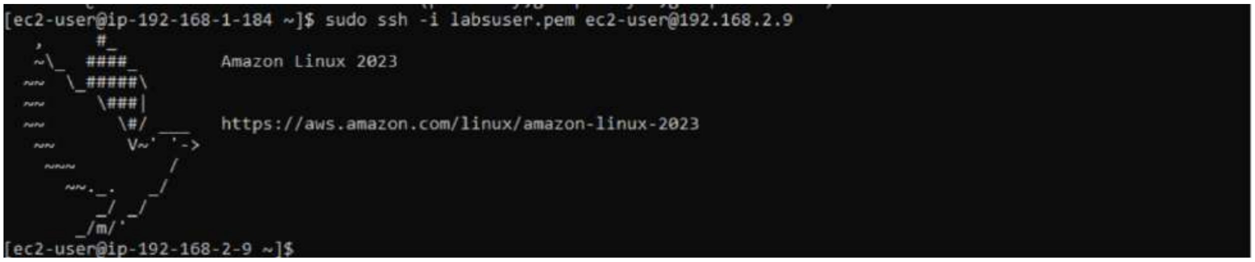
- Change file permissions for the file we just downloaded to our bastion host by typing
  - chmod 400 labsuser.pem
- Then ssh into our app server by typing
  - ssh -i my-key-pair.pem ec2-user@app-server-private-ip
  - Replace my-key-pair with the name of your key

    - Replace app-server-private-ip with your app server’s private ip address



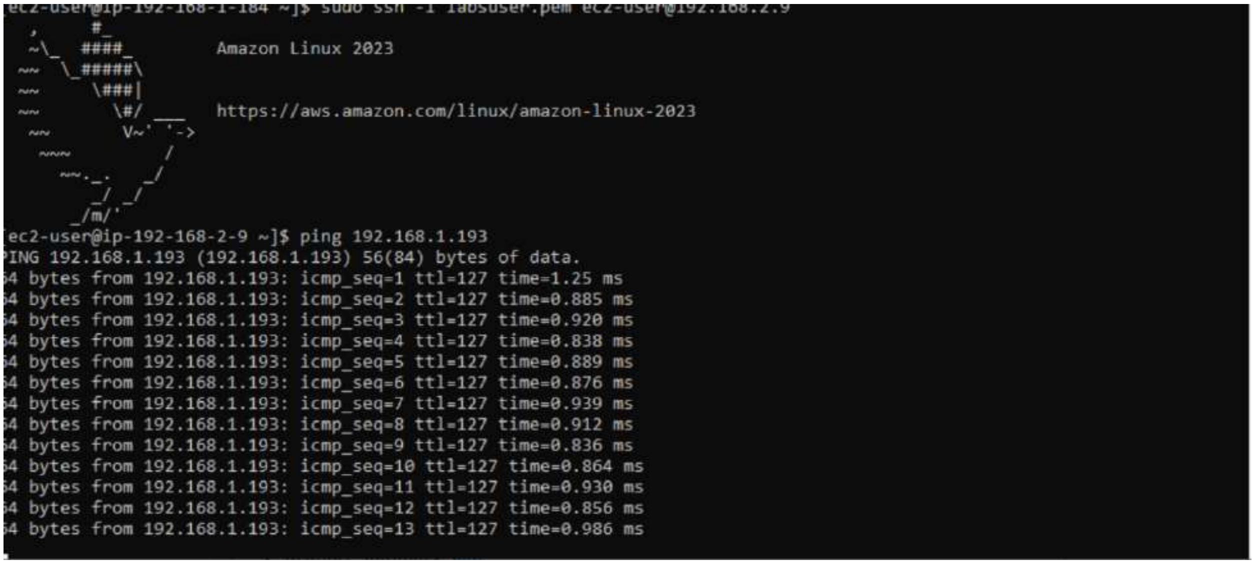
```
ralph@DESKTOP-CJTV68T:/mnt/d$ sudo ssh -i labsuser.pem ec2-user@54.184.75.155
The authenticity of host '54.184.75.155 (54.184.75.155)' can't be established.
ED25519 key fingerprint is SHA256:woyyVtJ0o2I2DIw/HdisAmHEoCzxcDxxvOdpSheywCo.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '54.184.75.155' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-192-168-1-184 ~]$
[ec2-user@ip-192-168-1-184 ~]$
[ec2-user@ip-192-168-1-184 ~]$
[ec2-user@ip-192-168-1-184 ~]$
[ec2-user@ip-192-168-1-184 ~]$
```

- 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



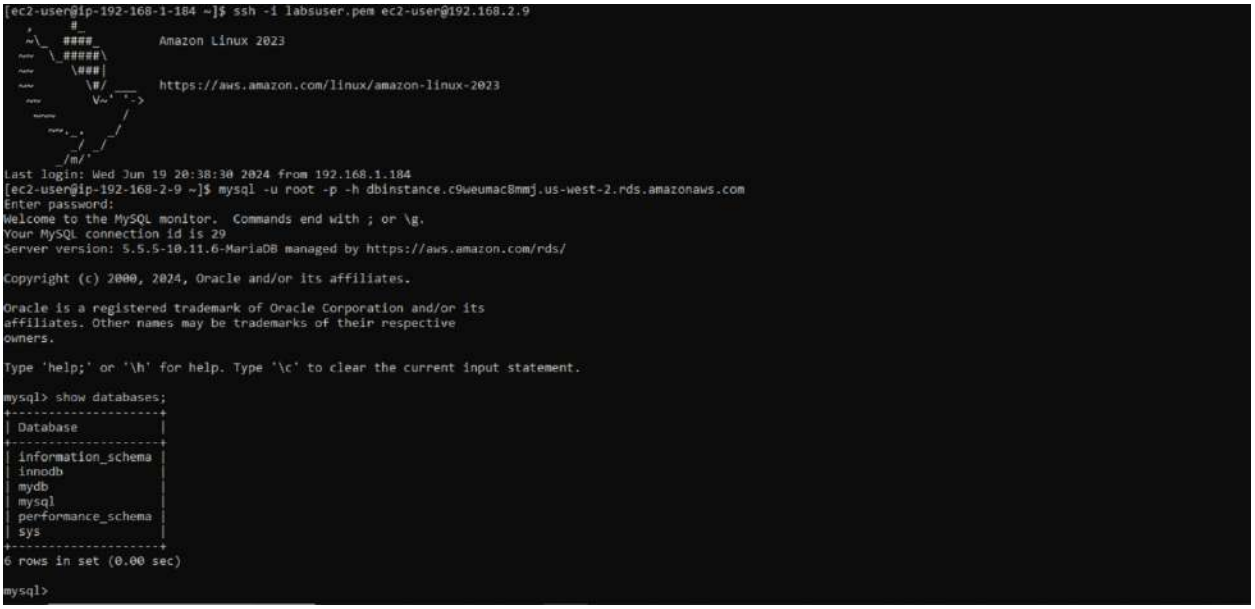
```
[ec2-user@ip-192-168-1-184 ~]$ sudo ssh -i labsuser.pem ec2-user@192.168.2.9
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-192-168-2-9 ~]$
```

- Ping the private ip address of your web server to and see if it connect



```
ec2-user@ip-192-168-1-184 ~]$ sudo ssh -i labsuser.pem ec2-user@192.168.2.9
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-192-168-2-9 ~]$ ping 192.168.1.193
ING 192.168.1.193 (192.168.1.193) 56(84) bytes of data.
4 bytes from 192.168.1.193: icmp_seq=1 ttl=127 time=1.25 ms
4 bytes from 192.168.1.193: icmp_seq=2 ttl=127 time=0.885 ms
4 bytes from 192.168.1.193: icmp_seq=3 ttl=127 time=0.920 ms
4 bytes from 192.168.1.193: icmp_seq=4 ttl=127 time=0.838 ms
4 bytes from 192.168.1.193: icmp_seq=5 ttl=127 time=0.889 ms
4 bytes from 192.168.1.193: icmp_seq=6 ttl=127 time=0.876 ms
4 bytes from 192.168.1.193: icmp_seq=7 ttl=127 time=0.939 ms
4 bytes from 192.168.1.193: icmp_seq=8 ttl=127 time=0.912 ms
4 bytes from 192.168.1.193: icmp_seq=9 ttl=127 time=0.836 ms
4 bytes from 192.168.1.193: icmp_seq=10 ttl=127 time=0.864 ms
4 bytes from 192.168.1.193: icmp_seq=11 ttl=127 time=0.930 ms
4 bytes from 192.168.1.193: icmp_seq=12 ttl=127 time=0.856 ms
4 bytes from 192.168.1.193: icmp_seq=13 ttl=127 time=0.986 ms
```

- 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-192-168-1-184 ~]$ ssh -i labsuser.pem ec2-user@192.168.2.9
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Wed Jun 19 20:38:30 2024 from 192.168.1.184
[ec2-user@ip-192-168-2-9 ~]$ mysql -u root -p -h dbinstance.c9weumac8mmj.us-west-2.rds.amazonaws.com
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 29
Server version: 5.5.5-10.11.6-MariaDB managed by https://aws.amazon.com/rds/

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| innodb             |
| mydb               |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
6 rows in set (0.00 sec)

mysql>
```

1. VPC Setup:
   - Create a VPC with 4 subnets (1 public, 3 private) across 2 Availability Zones (AZs).
   - Enable public IP addresses for instances in the public subnet.
   - Set up Internet and NAT Gateways for connectivity.

2. Instance Deployment:
   - Launch instances:

- Bastion Host (Amazon Linux 2, T2.micro) in public subnet for SSH access.
- Web Server (Amazon Linux 2, T2.micro) in public subnet with LAMP stack.
- App Server (Amazon Linux 2, T2.micro) in private subnet with MariaDB installed via User Data.

3. Database Setup:
   - Create a MySQL or MariaDB RDS instance:
     - Configure root user with 'Re:Start!9' password and initial database setup.

4. Networking and Security:
   - Configure security groups for Bastion Host, Web Server, App Server, and Database to control traffic.
   - Define route tables for public and private subnets, attaching Internet and NAT Gateways.

5. Connectivity and Testing:
   - Upload SSH keys to Bastion Host for secure access.
   - Verify connectivity by SSHing into instances via Bastion Host.
   - Test web server functionality and database connectivity from the App Server.

This summary outlines the foundational steps required to deploy and connect a three-tier architecture on AWS, emphasizing networking, instance deployment, security setup, and connectivity testing. Adjust configurations based on specific project requirements and AWS guidelines for optimal performance and security.