264-[NF]-Lab - Networking resources for a VPC

Umi Nur F | nurfatih365@gmail.com

A. AWS service restrictions

In this lab environment, access to AWS services and service actions might be restricted to the ones that are needed to complete the lab instructions. You might encounter errors if you attempt to access other services or perform actions beyond the ones that are described in this lab.

In this lab, you will:

- Summarize the customer scenario
- Create a VPC, Internet Gateway, Route Table, Security Group, Network Access List, and EC2 instance to create a routable network within the VPC
- Familiarize yourself with the console
- Develop a solution to the customers issue found within this lab.

The lab is complete once you can successfully utilize the command ping outside the VPC.

This lab total duration is 60 minutes.

B. Scenario

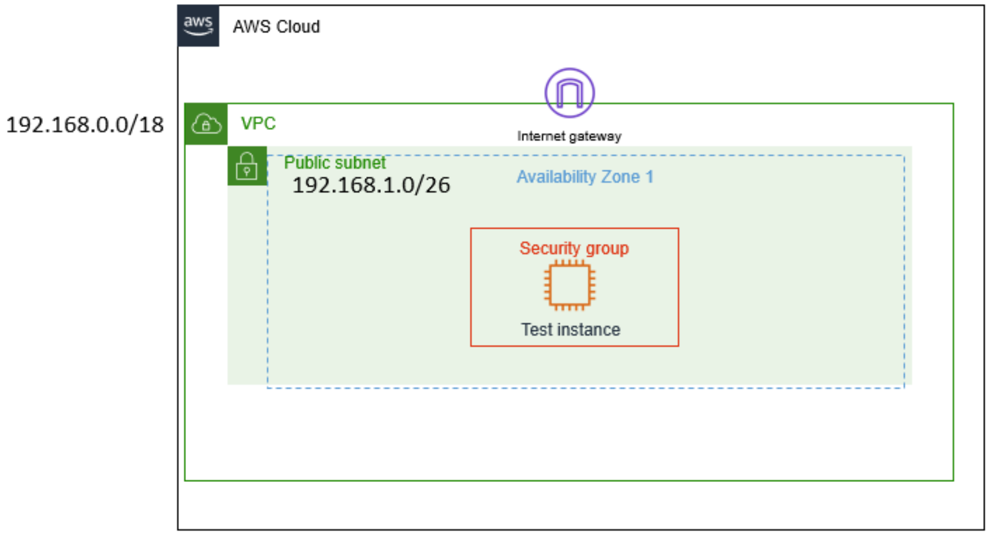
Your role is a Cloud Support Engineer at Amazon Web Services (AWS). During your shift, a customer from a startup company requests assistance regarding a networking issue within their AWS infrastructure. The email and an attachment of their architecture is below.

Email from the customer

Hello Cloud Support!

I previously reached out to you regarding help setting up my VPC. I thought I knew how to attach all the resources to make an internet connection, but I cannot even ping outside the VPC. All I need to do is ping! Can you please help me set up my VPC to where it has network connectivity and can ping? The architecture is below. Thanks!

Brock, startup owner



Customer VPC architecture

C. Accessing the AWS Management Console

1. At the top of these instructions, choose Start Lab to launch your lab. A **Start Lab** panel opens, and it displays the lab status.

   Tip: If you need more time to complete the lab, choose the Start Lab button again to restart the timer for the environment.

2. Wait until you see the message *Lab status: ready*, then close the **Start Lab** panel by choosing the **X**.

3. At the top of these instructions, choose AWS. This opens the AWS Management Console in a new browser tab. The system will automatically log you in.

   Tip: If a new browser tab does not open, a banner or icon is usually at the top of your browser with a message that your browser is preventing the site from opening pop-up windows. Choose the banner or icon and then choose **Allow pop ups**.

4. Arrange the AWS Management Console tab so that it displays alongside these instructions. Ideally, you will be able to see both browser tabs at the same time so that you can follow the lab steps more easily.

Task 1: Investigate the customer's needs

Recall

Recall protocols which can be directly used with AWS's Security Group (SG) and Network Access Control Lists (NACLs). A VPC needs an Internet Gateway (IGW) in order for the VPC to reach the internet, which has the route as 0.0.0.0/0. These routes go on what is called a Route Table, which are associated to subnets so they know where they belong. As mentioned in previous labs, you will follow the order of the navigation console to build this VPC, and a troubleshooting method to build a fully functioning VPC. When building a VPC from scratch, it is easier to work from the top and move down to the bottom since you do not have an instance yet. Think of this as building a sandwich; the VPC is the bun, and the resources are everything in between.

For task 1, you will investigate the customer's request and build a VPC that has network connectivity. You will complete this lab when you can successfully ping from your EC2 instance to the internet showing that the VPC has network connectivity.

In the scenario, Brock, the customer requesting assistance, has requested help in creating resources for his VPC to be routable to the internet. Keep the VPC CIDR at 192.168.0.0/18 and public subnet CIDR of 192.168.1.0/26.

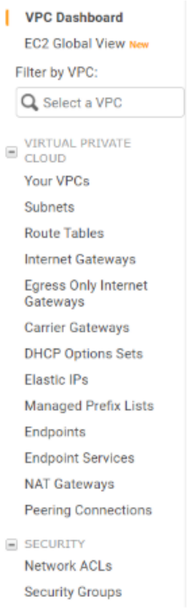


Figure: A great guide to building a VPC is to follow the left hand navigation pane, starting from "Your VPCs" and working your way down.

Before you start, let's review VPC and its components to make it network compatible.

- A **Virtual Private Cloud (VPC)** is like a data center but in the cloud. Its logically isolated from other virtual networks from which you can spin up and launch your AWS resources within minutes.
- **Private Internet Protocol (IP)** addresses are how resources within the VPC communicate with each other. An instance needs a public IP address for it to communicate outside the VPC. The VPC will need networking resources such as an Internet Gateway (IGW) and a route table in order for the instance to reach the internet.
- An **Internet Gateway (IGW)** is what makes it possible for the VPC to have internet connectivity. It has two jobs: perform network address translation (NAT) and be the target to route traffic to the internet for the VPC. An IGW's route on a route table is always 0.0.0.0/0.
- A **subnet** is a range of IP addresses within your VPC.
- A **route table** contains routes for your subnet and directs traffic using the rules defined within the route table. You associate the route table to a subnet. If an IGW was on a route table, the destination would be 0.0.0.0/0 and the target would be IGW.
- **Security groups** and **Network Access Control Lists (NACLs)** work as the firewall within your VPC. Security groups work at the instance level and are stateful, which means they block everything by default. NACLs work at the subnet level and are stateless, which means they do not block everything by default.

Steps

5. Select the **AWS** button located in the top right of the Vocareum home environment. This will open the AWS console in a new tab.
6. Once in the AWS console, click **VPC** under **Recently visited services**. If it is not there, navigate to the top left corner, and select **VPC** under **Networking and Content Delivery** in the **Services** navigation pane.

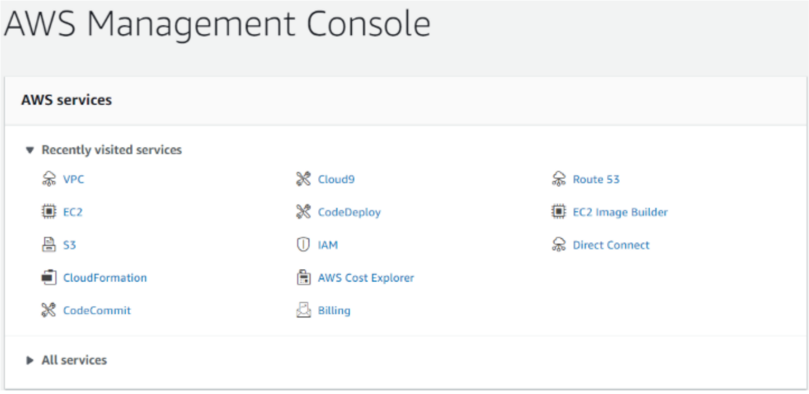
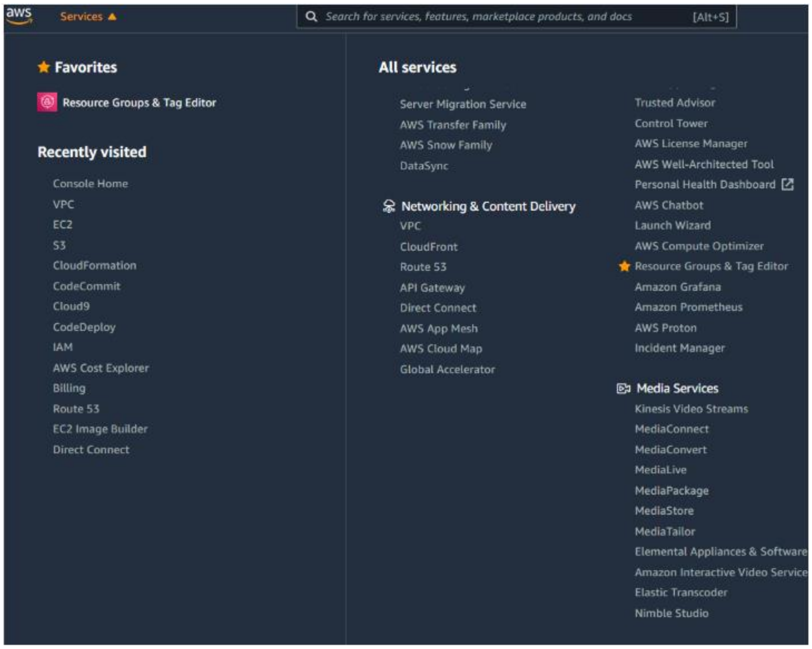


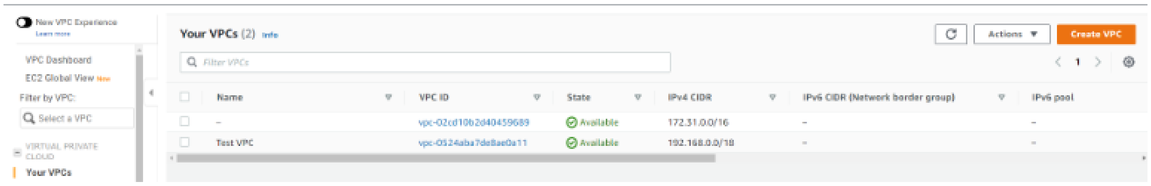
Figure: Recently visited services in the AWS console



7. Start at the top of the left navigation pane at **Your VPCs** and work your way down. Select **Your VPCs**, navigate to the top right corner, and select **Create VPC**.

   Note

   Note, you will be using a top-down theory with the top being the VPC.



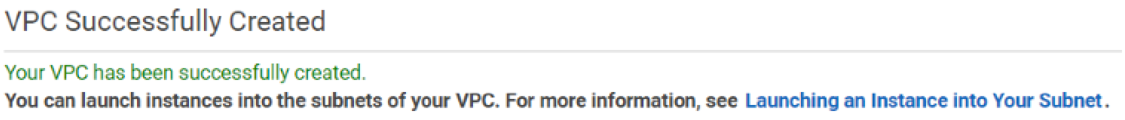
Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR (Network border group)	IPv6 pool
–	vpc-02cd10b2d40459689	Available	172.31.0.0/16	–	–
Test VPC	vpc-0524aba7de8ae0a11	Available	192.168.0.0/18	–	–

Figure: Navigate to "Your VPCs" and select Create VPC.

8. Name the VPC: Test VPC

   IPv4 CIDR block: 192.168.0.0/18

9. Leave everything else as default, and select **Create VPC**



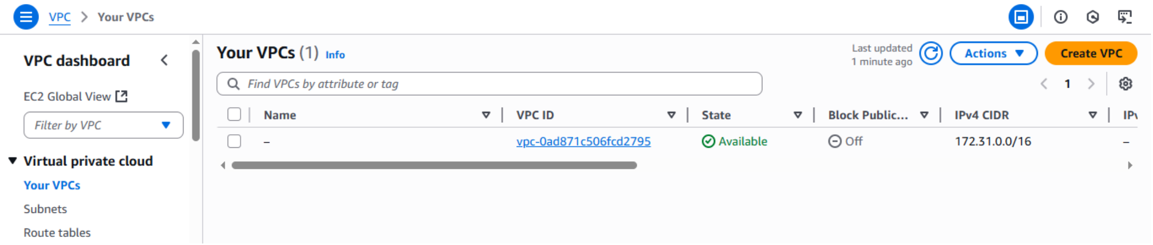
VPC Successfully Created

Your VPC has been successfully created.

You can launch instances into the subnets of your VPC. For more information, see Launching an Instance into Your Subnet.

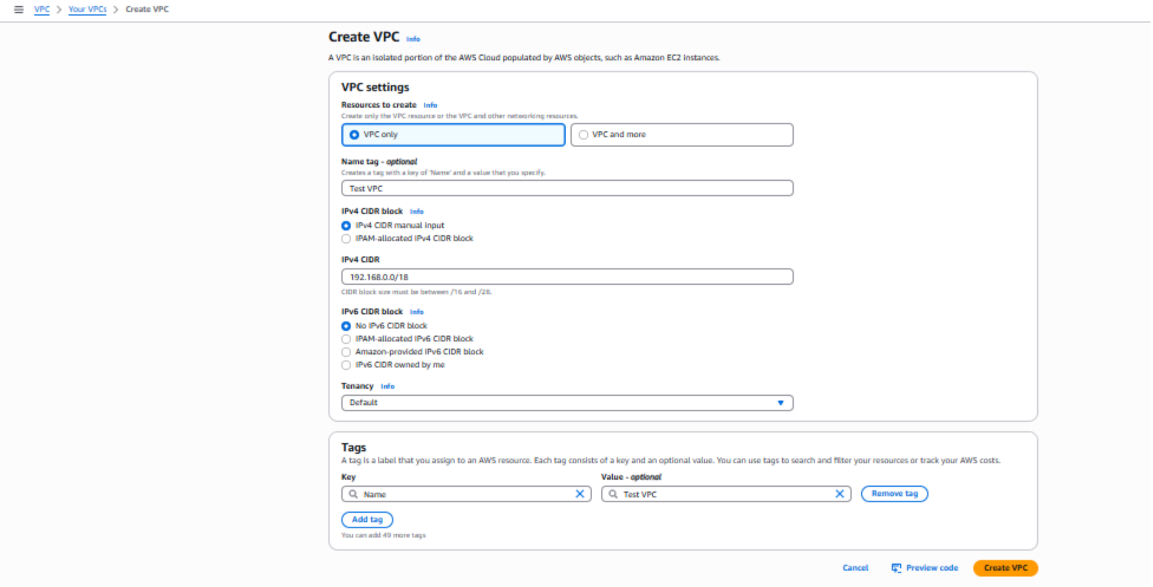
Figure: VPC settings configuration

Result:



Your VPCs (1) Info

□	Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv
□	–	vpc-0ad871c506fcd2795	✓ Available	⊖ Off	172.31.0.0/16	–



Create VPC Info

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

VPC settings

Resources to create Info

Create only the VPC resource or 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.

Test VPC

IPv4 CIDR block Info

● IPv4 CIDR manual input

○ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

192.168.0.0/18

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

Default

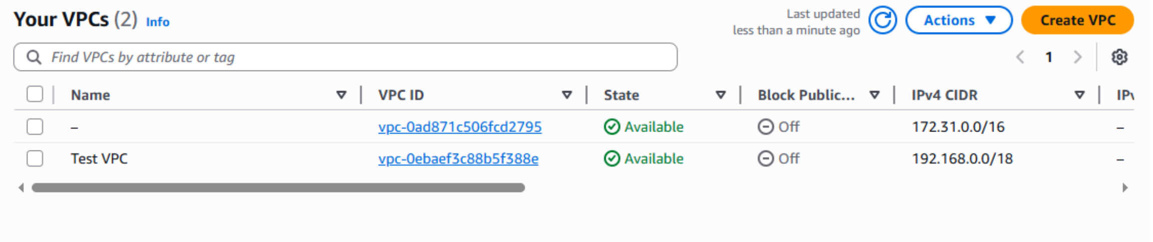
Tags

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	Test VPC

You can add 49 more tags

Cancel
Preview code
Create VPC



Last updated less than a minute ago
Actions
Create VPC
Find VPCs by attribute or tag
1

Your VPCs (2) Info

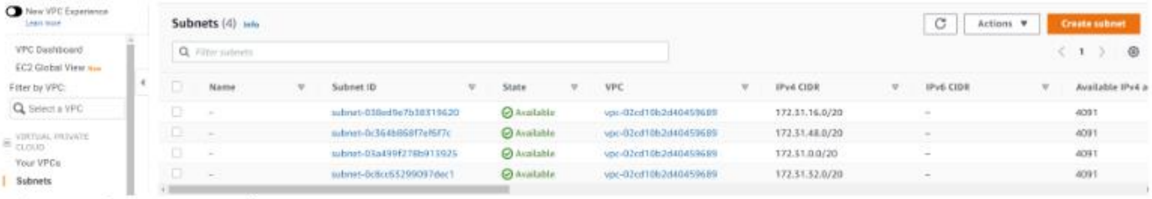
□	Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv
□	–	vpc-0ad871c506fcd2795	✓ Available	⊖ Off	172.31.0.0/16	–
□	Test VPC	vpc-0ebaef3c88b5f388e	✓ Available	⊖ Off	192.168.0.0/18	–

Creating Subnets

10. Now that the VPC is complete, look at the left navigation pane and select **Subnets**. In the top right corner, select **Create subnet**.

    Note

    Please note: Although almost anything can be created in any order, it is easier to have an approach. Having a flow or an approach will assist you in troubleshooting issues and ensure that you do not forget a resource.

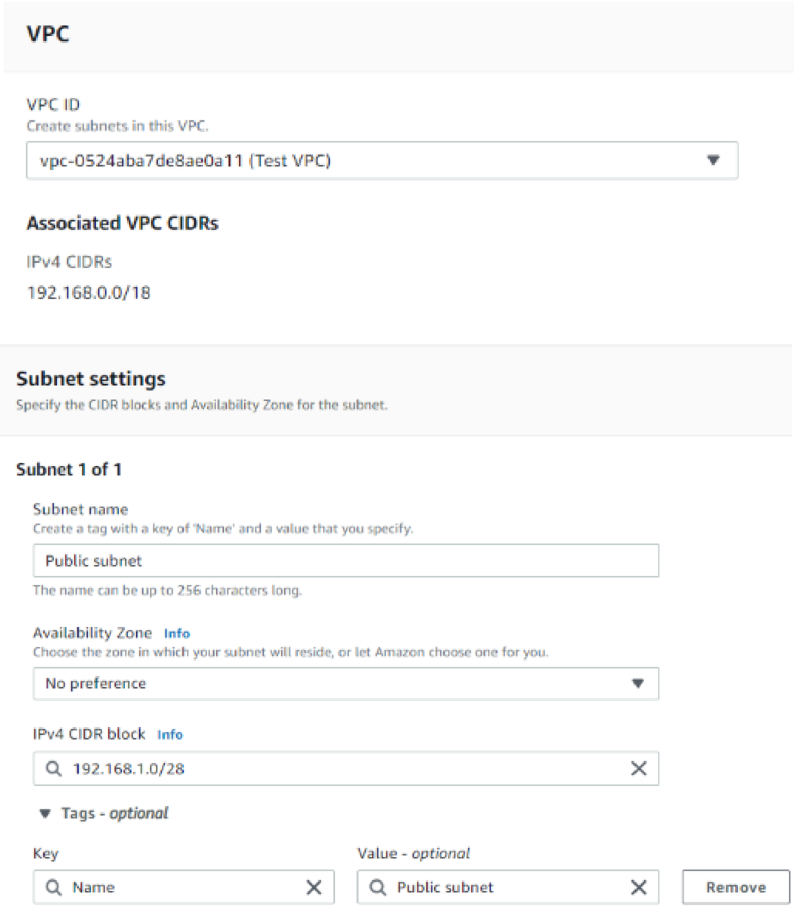


Subnets (4) Info

□	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 a
□	–	subnet-038ed9e7b38319620	✓ Available	vpc-02cd10b2d40459689	172.31.16.0/20	–	4091
□	–	subnet-0c364b868f7ef6f7c	✓ Available	vpc-02cd10b2d40459689	172.31.48.0/20	–	4091
□	–	subnet-03a499f278b913925	✓ Available	vpc-02cd10b2d40459689	172.31.0.0/20	–	4091
□	–	subnet-0c8cc65299097dec1	✓ Available	vpc-02cd10b2d40459689	172.31.32.0/20	–	4091

Figure: Select Create subnet

11. Configure like the following picture:



VPC

VPC ID
Create subnets in this VPC.
vpc-0524aba7de8ae0a11 (Test VPC) ▼

Associated VPC CIDRs

IPv4 CIDRs
192.168.0.0/18

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.
No preference ▼

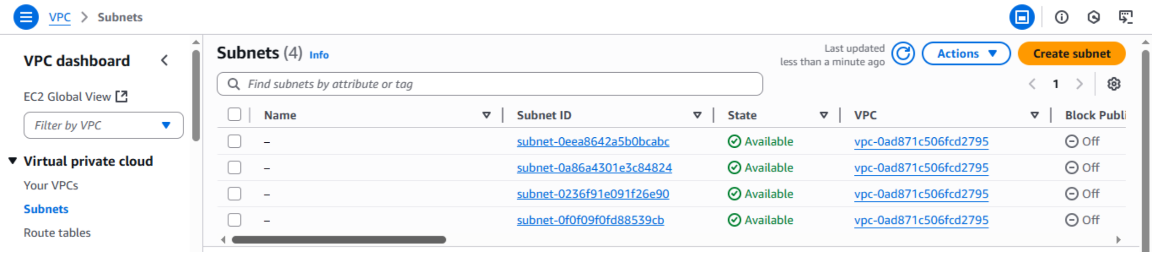
IPv4 CIDR block Info
192.168.1.0/28

▼ Tags - *optional*

Key: Name
Value - *optional*: Public subnet

Figure: Subnet configuration

Result:

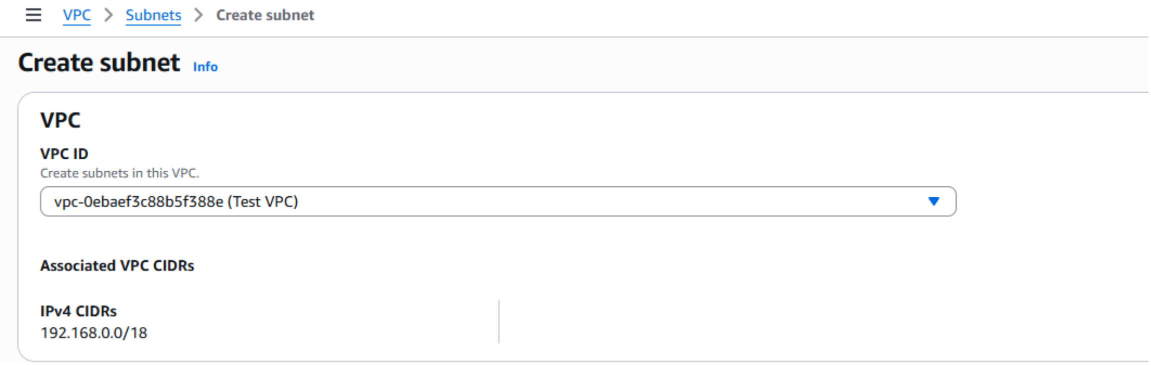


Subnets (4)

Last updated less than a minute ago

Find subnets by attribute or tag

□	Name	Subnet ID	State	VPC	Block Publi
□	–	subnet-0eea8642a5b0bcabc	✓ Available	vpc-0ad871c506fcd2795	⊖ Off
□	–	subnet-0a86a4301e3c84824	✓ Available	vpc-0ad871c506fcd2795	⊖ Off
□	–	subnet-0236f91e091f26e90	✓ Available	vpc-0ad871c506fcd2795	⊖ Off
□	–	subnet-0f0f09f0fd88539cb	✓ Available	vpc-0ad871c506fcd2795	⊖ Off



Create subnet

VPC

VPC ID

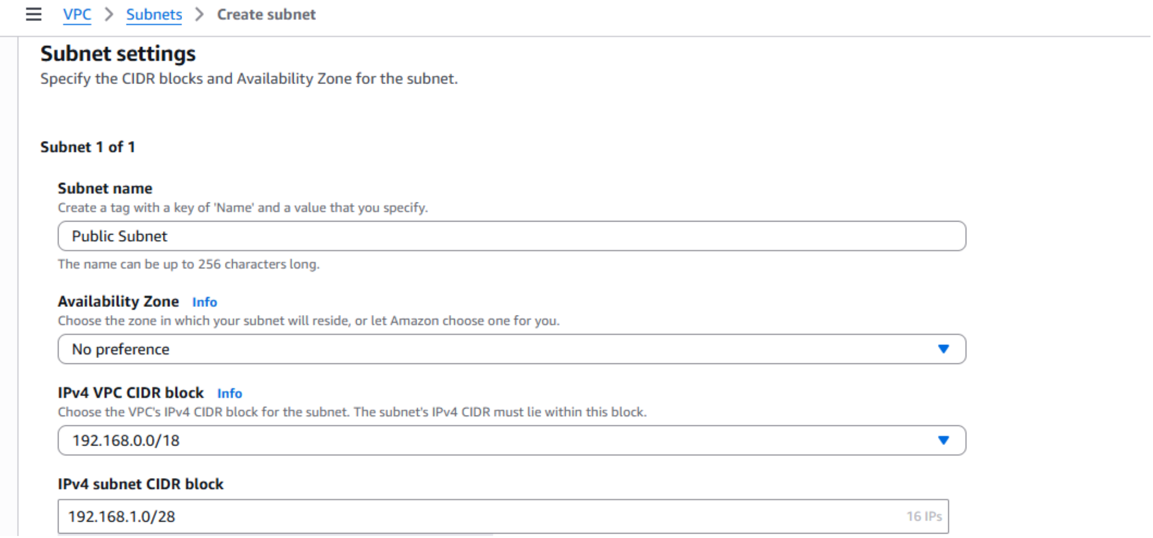
Create subnets in this VPC.

vpc-0ebaef3c88b5f388e (Test VPC)

Associated VPC CIDRs

IPv4 CIDRs

192.168.0.0/18



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

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

No preference

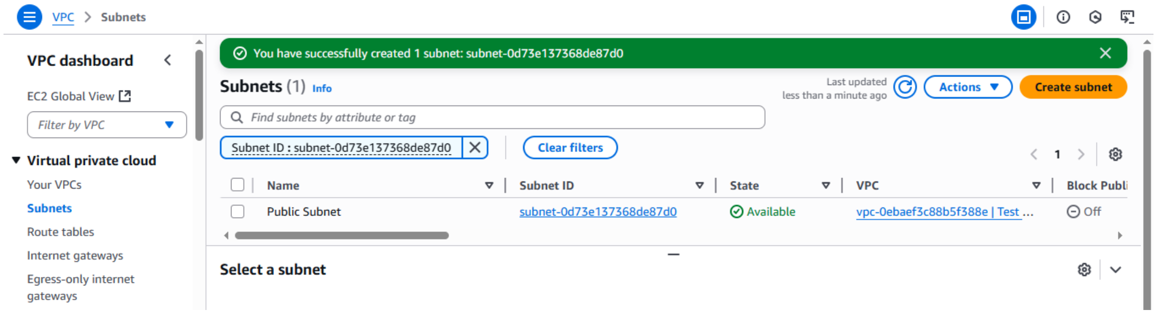
IPv4 VPC CIDR block

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

192.168.0.0/18

IPv4 subnet CIDR block

192.168.1.0/28 16 IPs



You have successfully created 1 subnet: subnet-0d73e137368de87d0

Subnets (1)

Last updated less than a minute ago

Find subnets by attribute or tag

Subnet ID : subnet-0d73e137368de87d0

□	Name	Subnet ID	State	VPC	Block Publi
□	Public Subnet	subnet-0d73e137368de87d0	✓ Available	vpc-0ebaef3c88b5f388e | Test ...	⊖ Off

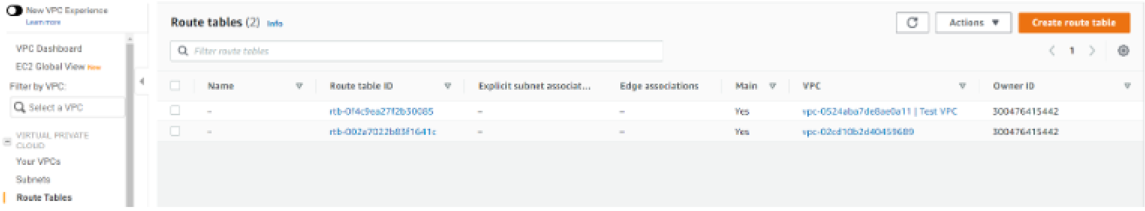
Select a subnet

Create Route Table

Recall

Recall that a route table contains the rules or routes that determine where network traffic within your subnet and VPC will go. It controls the network traffic like a router, and, just like a router, it stores IP addresses within the VPC. You associate a route table to each subnet and put the routes that you need your subnet to be able to reach. For this step, you will create the route table first, and then add the routes as you create AWS resources for the VPC.

12. Navigate to the left navigation pane, and select **Route Tables**. In the top right corner select **Create route table**.

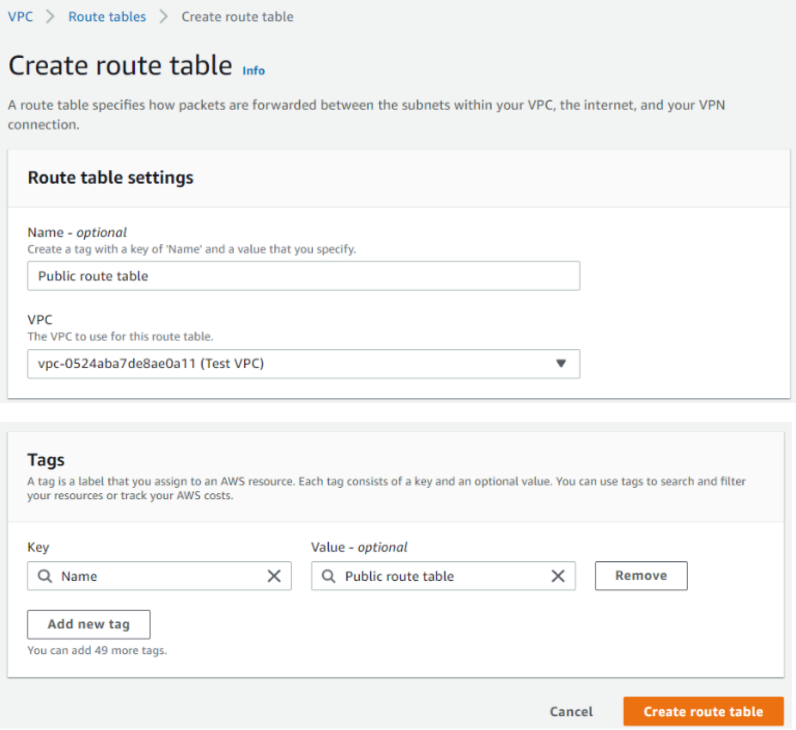


Route tables (2) Info

Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
–	rtb-0f4c9ea27f2b30085	–	–	Yes	vpc-0524aba7de8ae0a11 | Test VPC	300476415442
–	rtb-002a7022b83f1641c	–	–	Yes	vpc-02cd10b2d40459689	300476415442

Figure: Select Create route table.

13. Configure like the following picture:



Create route table

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 route table

VPC
The VPC to use for this route table.
vpc-0524aba7de8ae0a11 (Test VPC)

Tags

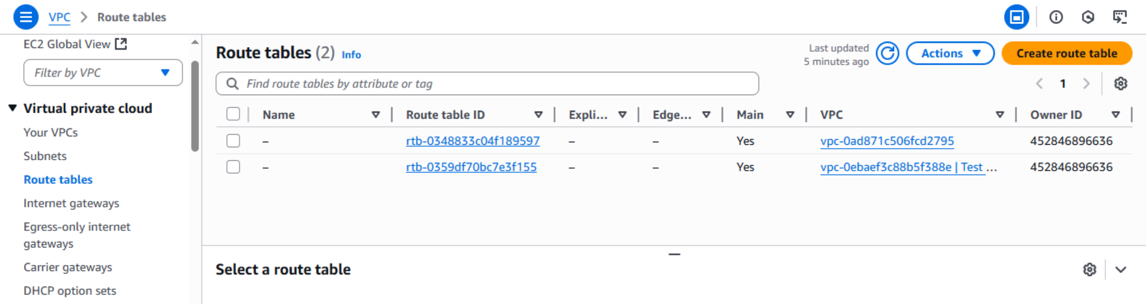
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*
Name	Public route table

You can add 49 more tags.

Figure: Route table configuration

Result:



VPC > Route tables

Route tables (2) Info

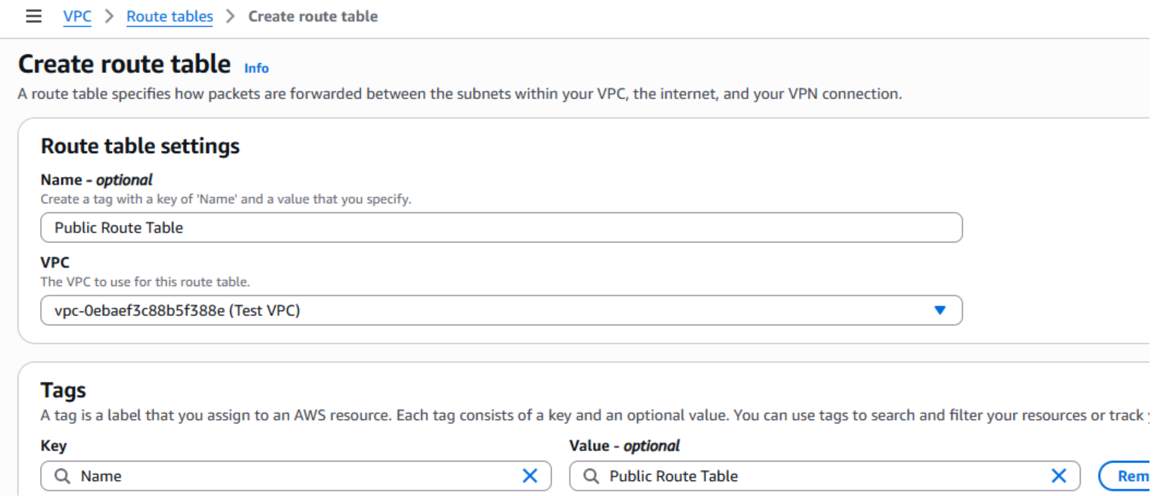
Last updated 5 minutes ago

Actions ▼ | Create route table

Find route tables by attribute or tag

☐	Name	Route table ID	Expli...	Edge...	Main	VPC	Owner ID
☐	–	rtb-0348833c04f189597	–	–	Yes	vpc-0ad871c506fcd2795	452846896636
☐	–	rtb-0359df70bc7e3f155	–	–	Yes	vpc-0ebaef3c88b5f388e | Test ...	452846896636

Select a route table



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.

Public Route Table

VPC

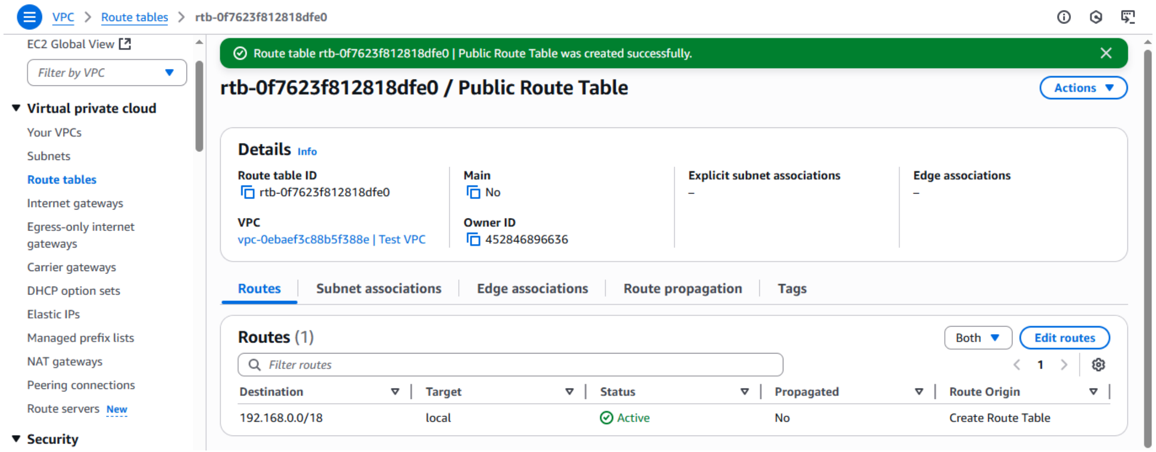
The VPC to use for this route table.

vpc-0ebaef3c88b5f388e (Test 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

Key	Value - *optional*
Name	Public Route Table



VPC > Route tables > rtb-0f7623f812818dfe0

Route table rtb-0f7623f812818dfe0 | Public Route Table was created successfully.

rtb-0f7623f812818dfe0 / Public Route Table

Details Info

Route table ID: rtb-0f7623f812818dfe0

Main: No

Explicit subnet associations: –

Edge associations: –

VPC: vpc-0ebaef3c88b5f388e | Test VPC

Owner ID: 452846896636

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (1)

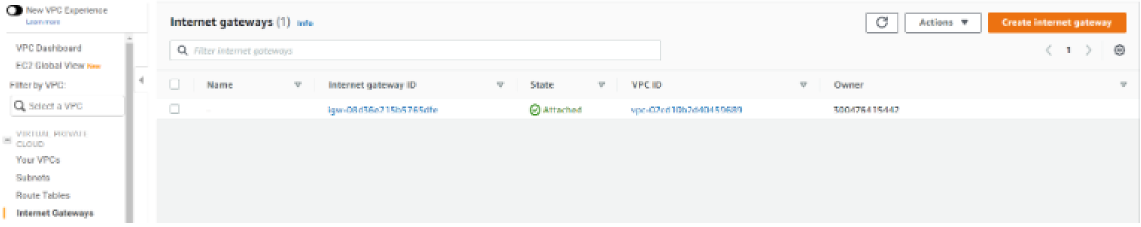
Destination	Target	Status	Propagated	Route Origin
192.168.0.0/18	local	✓ Active	No	Create Route Table

Create Internet Gateway and attach Internet Gateway

In this lab

Recall that an IGW is what allows the VPC to have internet connectivity and allows communication between resources in your VPC and the internet. The IGW is used as a target in the route table to route internet-routable traffic and to perform network address translation (NAT) for EC2 instances. NAT is a bit beyond the scope of this lab, but it is referenced in the reference section if you'd like to dive deeper.

14. From the left navigation pane, select **Internet Gateways**. Create an Internet Gateway (IGW) by selecting **Create internet gateway** at the top right corner.

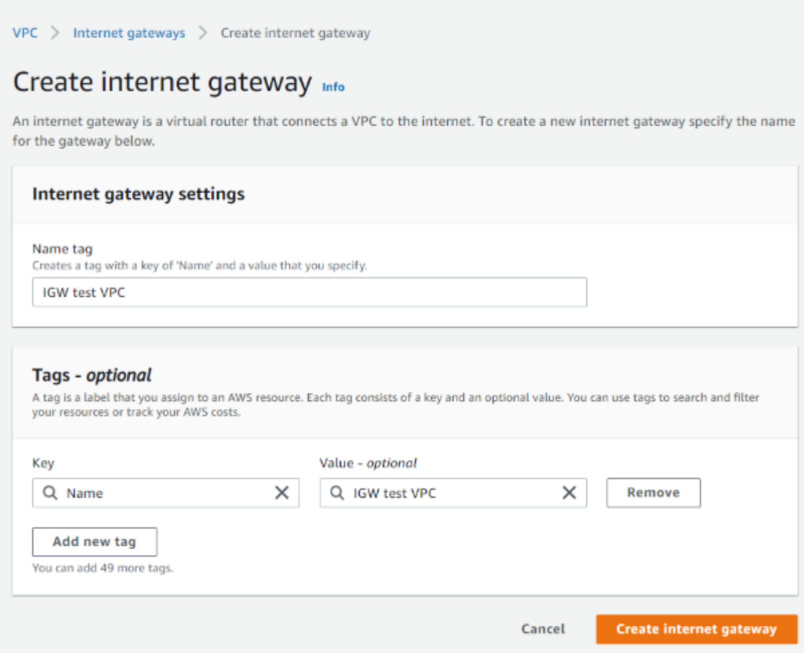


Internet gateways (1) Info

	Name	Internet gateway ID	State	VPC ID	Owner
☐	-	igw-08d36e715b5765dfe	Attached	vpc-02cd10b7d40459680	300476415442

Figure: Select Create internet gateway

15. Configure like the following picture:



VPC > Internet gateways > Create internet gateway

Create internet gateway Info

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.
IGW test VPC

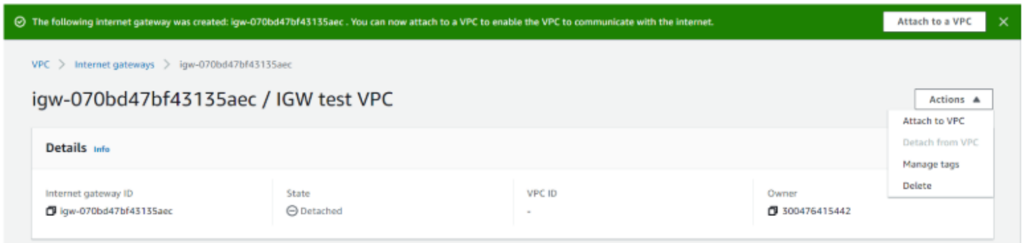
Tags - *optional*
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*
Name	IGW test VPC

You can add 49 more tags.

Figure: Internet gateway configuration

16. Once created, attach the **Internet Gateway** to the VPC by selecting **Actions** at the top right corner and clicking **Attach to VPC**.



The following internet gateway was created: igw-070bd47bf43135aec . You can now attach to a VPC to enable the VPC to communicate with the internet.

VPC > Internet gateways > igw-070bd47bf43135aec

igw-070bd47bf43135aec / IGW test VPC

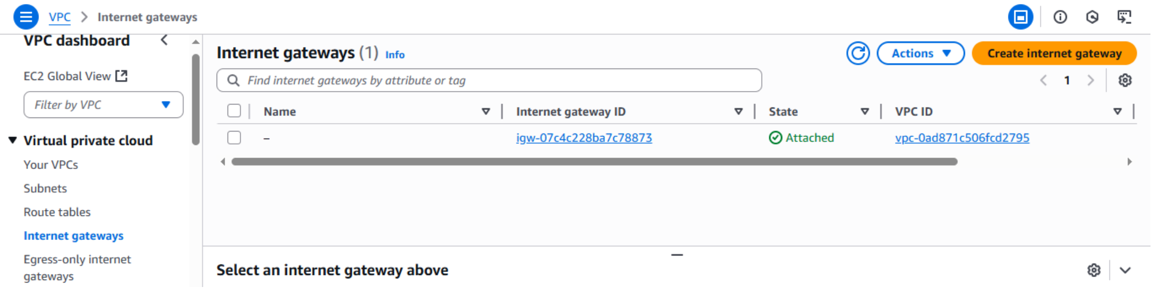
Details Info

Internet gateway ID	State	VPC ID	Owner
igw-070bd47bf43135aec	Detached	-	300476415442

Figure: Attaching the IGW that was just created.

Now your IGW is attached! You now need to add its route to the route table and associate the subnet you created to the route table.

Result:



VPC > Internet gateways

VPC dashboard

EC2 Global View

Filter by VPC

▼ Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

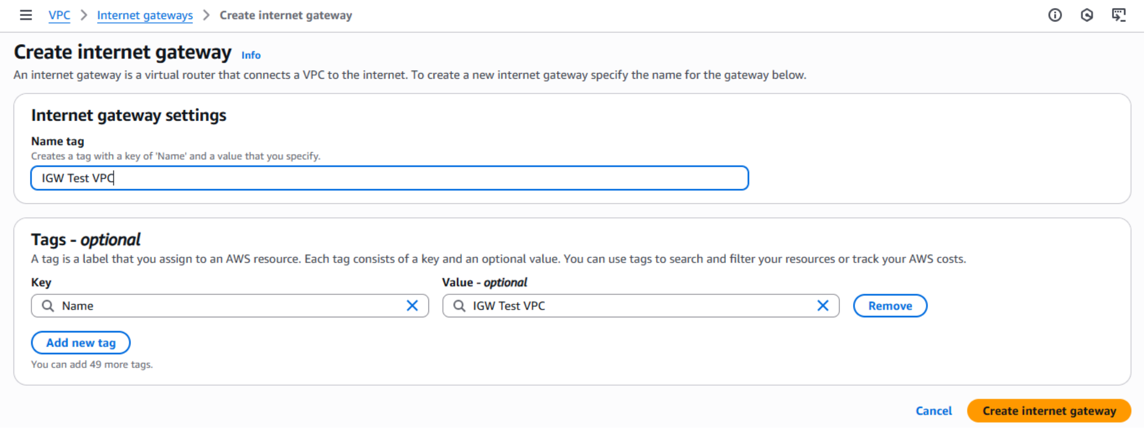
Internet gateways (1) Info

Actions ▼ | Create internet gateway

Find internet gateways by attribute or tag

□	Name	Internet gateway ID	State	VPC ID
□	–	igw-07c4c228ba7c78873	✓ Attached	vpc-0ad871c506fcd2795

Select an internet gateway above



VPC > Internet gateways > Create internet gateway

Create internet gateway Info

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.

IGW Test VPC

Tags - *optional*

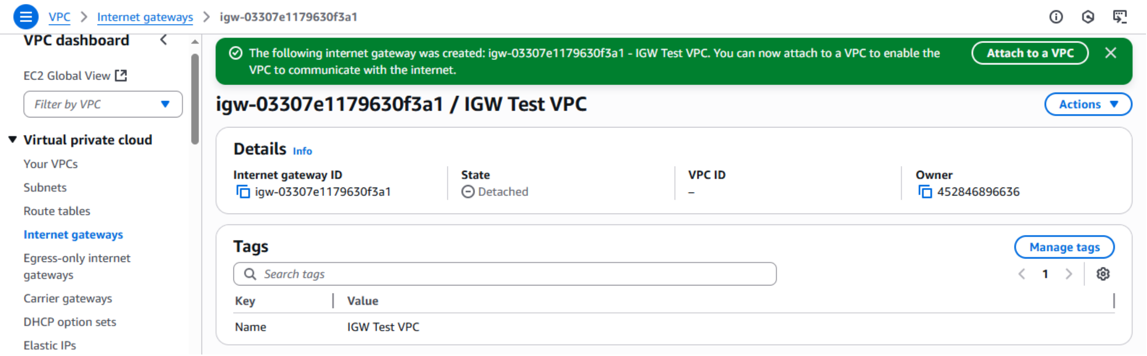
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*	
Name	IGW Test VPC	Remove

Add new tag

You can add 49 more tags.

Cancel | Create internet gateway



VPC > Internet gateways > igw-03307e1179630f3a1

VPC dashboard

EC2 Global View

Filter by VPC

▼ Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

The following internet gateway was created: igw-03307e1179630f3a1 - IGW Test VPC. You can now attach to a VPC to enable the VPC to communicate with the internet. Attach to a VPC

igw-03307e1179630f3a1 / IGW Test VPC

Actions ▼

Details Info

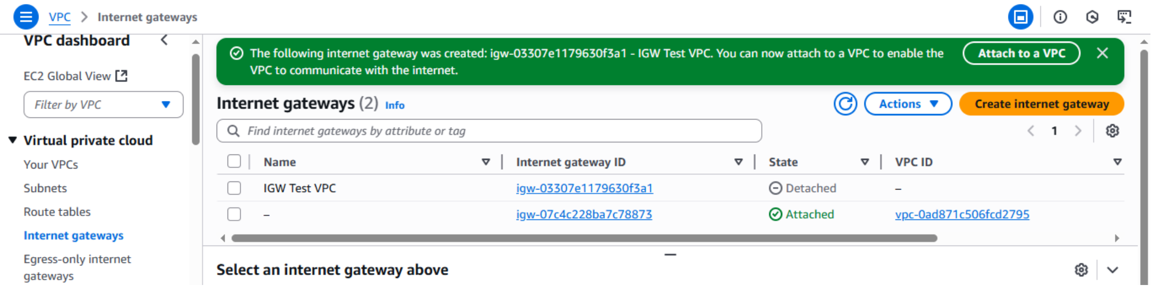
Internet gateway ID	State	VPC ID	Owner
igw-03307e1179630f3a1	Detached	–	452846896636

Tags

Manage tags

Search tags

Key	Value
Name	IGW Test VPC



VPC > Internet gateways

VPC dashboard

EC2 Global View

Filter by VPC

▼ Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

The following internet gateway was created: igw-03307e1179630f3a1 - IGW Test VPC. You can now attach to a VPC to enable the VPC to communicate with the internet. Attach to a VPC

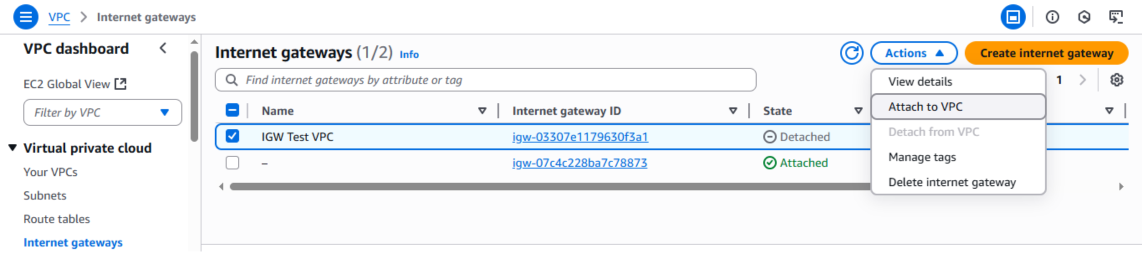
Internet gateways (2) Info

Actions ▼ | Create internet gateway

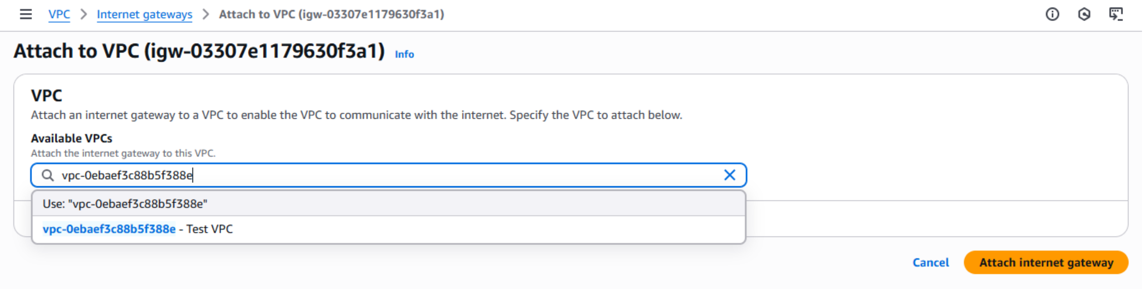
Find internet gateways by attribute or tag

□	Name	Internet gateway ID	State	VPC ID
□	IGW Test VPC	igw-03307e1179630f3a1	Detached	–
□	–	igw-07c4c228ba7c78873	✓ Attached	vpc-0ad871c506fcd2795

Select an internet gateway above



Name	Internet gateway ID	State
☑ IGW Test VPC	igw-03307e1179630f3a1	Detached
□ –	igw-07c4c228ba7c78873	Attached



VPC > Internet gateways > Attach to VPC (igw-03307e1179630f3a1)
Cancel
Attach internet gateway

Attach to VPC (igw-03307e1179630f3a1) Info

VPC

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

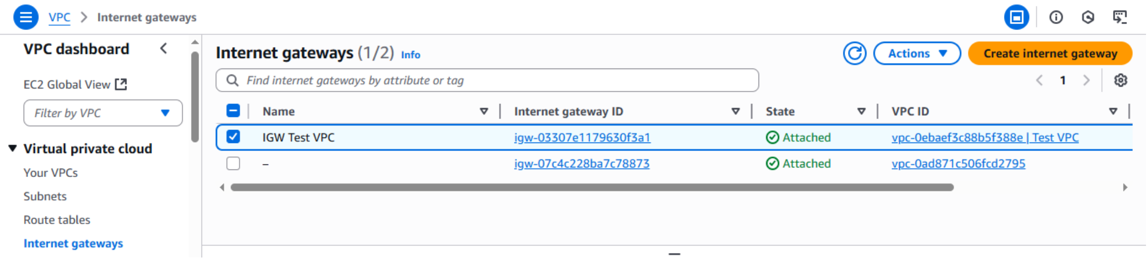
Available VPCs

Attach the internet gateway to this VPC.

vpc-0ebaef3c88b5f388e

Use: "vpc-0ebaef3c88b5f388e"

vpc-0ebaef3c88b5f388e - Test VPC



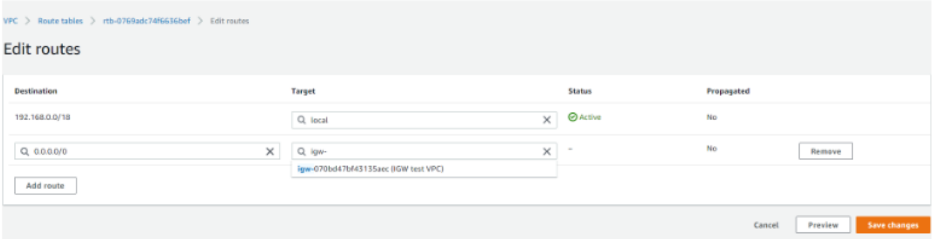
Name	Internet gateway ID	State	VPC ID
☑ IGW Test VPC	igw-03307e1179630f3a1	Attached	vpc-0ebaef3c88b5f388e | Test VPC
□ –	igw-07c4c228ba7c78873	Attached	vpc-0ad871c506fcd2795

Add route to route table and associate subnet to route table

17. Navigate to the **Route Table** section on the left navigation pane. Select **Public Route Table**, and the scroll to the bottom and select the **Routes** tab. Select the Edit routes button located in the routes box.

    On the Edit routes page, the first IP address is the local route and cannot be changed. Select **Add route**.

    - In the **Destination** section, type **0.0.0.0/0** in the search box. This is the route to the IGW. You are telling the route table that any traffic that needs internet connection will use 0.0.0.0/0 to reach the IGW so that it can reach the internet.
    - Click in the **Target** section and select **Internet Gateway** since you are targeting any traffic that needs to go to the internet to the IGW. Once you select the IGW, you will see your **TEST VPC IGW** appear. Select that IGW, navigate to the bottom right, and select **Save changes**.



VPC > Route tables > rtb-0769adc74f6636bef > Edit routes

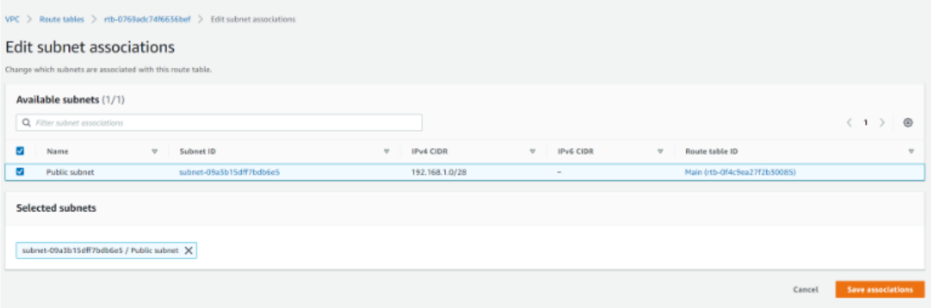
Edit routes

Destination	Target	Status	Propagated	
192.168.0.0/18	local	Active	No	
0.0.0.0/0	igw- igw-070bd47bf43135aec (IGW test VPC)	-	No	Remove

Figure: Adding the IGW in the route table (0.0.0.0/0 as the destination and IGW as the target).

Now your traffic has a route to the internet via the IGW.

18. From the Public route table dashboard, select the **Subnet associations** tab. Select the **Edit subnet associations** button.



VPC > Route tables > rtb-0769adc74f6636bef > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/1)

☑	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☑	Public subnet	subnet-09a3b15dff7bdb6e5	192.168.1.0/28	–	Main (rtb-0f4c9ea27f2b30085)

Selected subnets

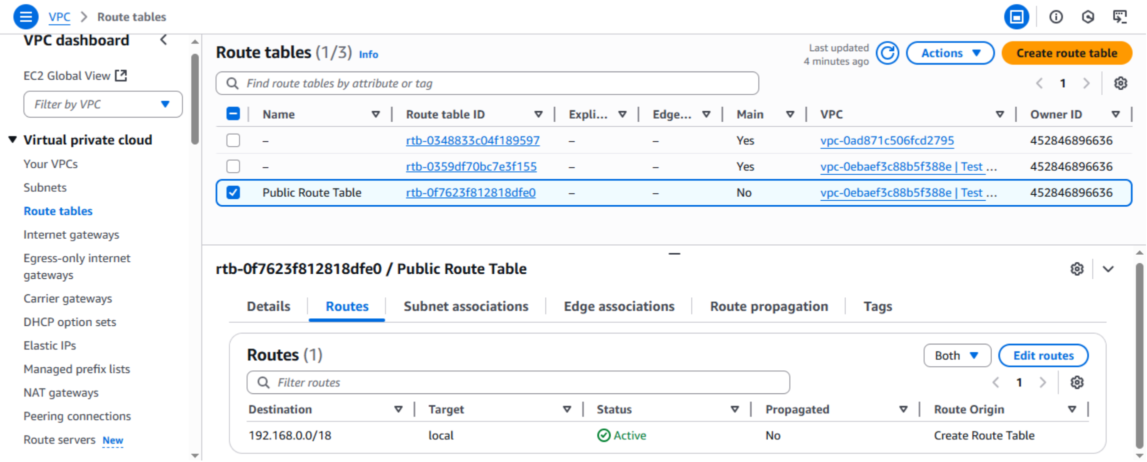
subnet-09a3b15dff7bdb6e5 / Public subnet

Figure: Associate the Public subnet and select save association.

19. Select **Save assocation**.

Note: Every route table needs to be associated to a subnet. You are now associating this route table to this subnet. As you probably noticed, the naming convention is kept the same (public route table, public subnet, etc) in order to associate the same resources together. Keep this in mind when your network and resources grow. You can have multiples of the same resources and it can get confusing to which belongs where.

Result:



VPC > Route tables

Route tables (1/3) Info

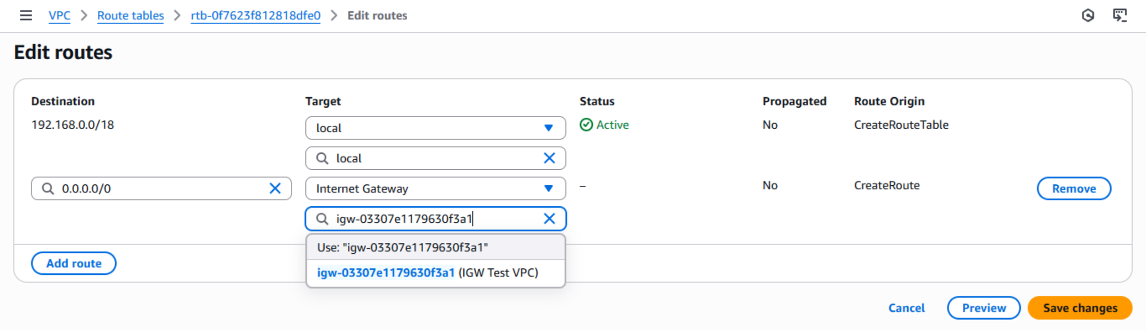
Last updated 4 minutes ago

	Name	Route table ID	Expli...	Edge...	Main	VPC	Owner ID
□	–	rtb-0348833c04f189597	–	–	Yes	vpc-0ad871c506fcd2795	452846896636
□	–	rtb-0359df70bc7e3f155	–	–	Yes	vpc-0ebaef3c88b5f388e | Test ...	452846896636
☑	Public Route Table	rtb-0f7623f812818dfe0	–	–	No	vpc-0ebaef3c88b5f388e | Test ...	452846896636

rtb-0f7623f812818dfe0 / Public Route Table

Routes (1)

Destination	Target	Status	Propagated	Route Origin
192.168.0.0/18	local	Active	No	Create Route Table

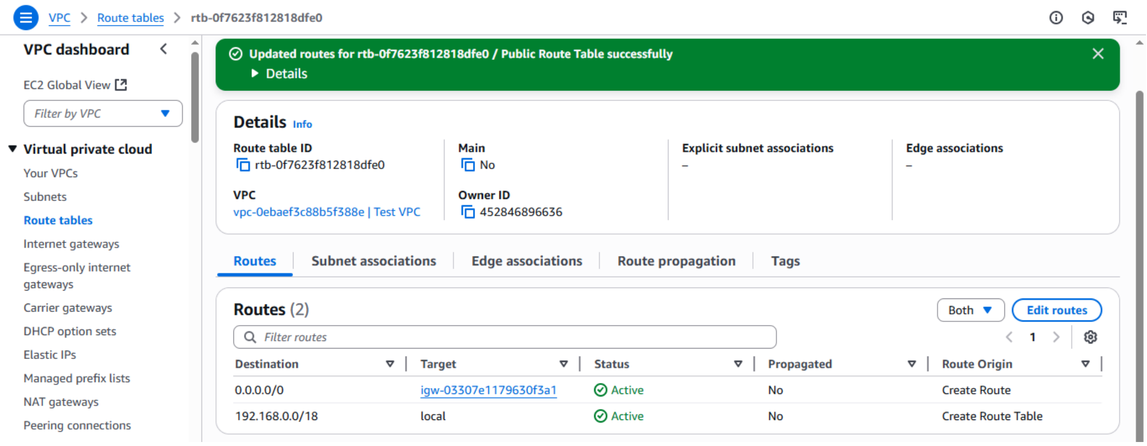


VPC > Route tables > rtb-0f7623f812818dfe0 > Edit routes

Edit routes

Destination	Target	Status	Propagated	Route Origin
192.168.0.0/18	local	Active	No	CreateRouteTable
0.0.0.0/0	Internet Gateway igw-03307e1179630f3a1	–	No	CreateRoute

Use: "igw-03307e1179630f3a1"
igw-03307e1179630f3a1 (IGW Test VPC)



VPC > Route tables > rtb-0f7623f812818dfe0

Updated routes for rtb-0f7623f812818dfe0 / Public Route Table successfully

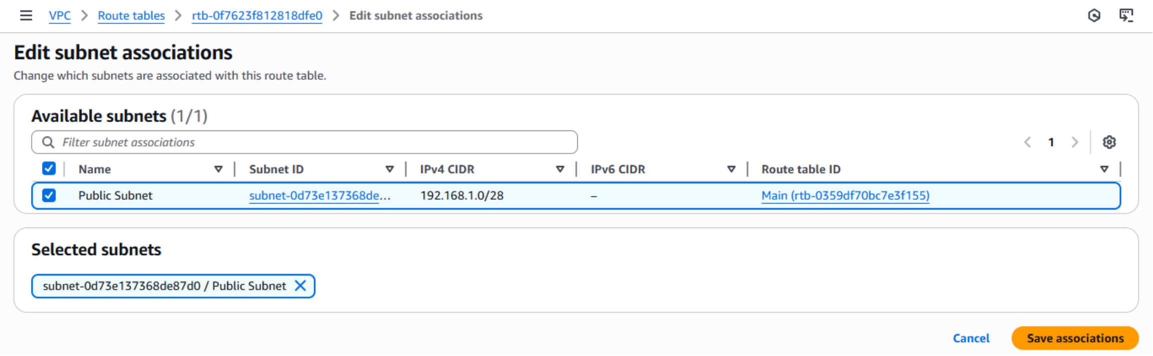
Details

Details Info

Route table ID: rtb-0f7623f812818dfe0
Main: No
Explicit subnet associations: –
Edge associations: –
VPC: vpc-0ebaef3c88b5f388e | Test VPC
Owner ID: 452846896636

Routes (2)

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-03307e1179630f3a1	Active	No	Create Route
192.168.0.0/18	local	Active	No	Create Route Table



VPC > Route tables > rtb-0f7623f812818dfe0 > Edit subnet associations

Edit subnet associations

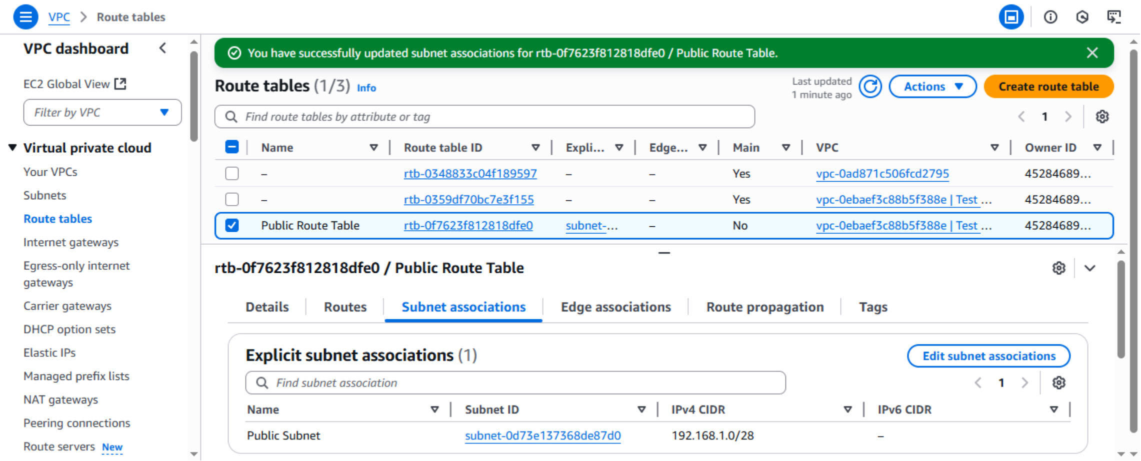
Change which subnets are associated with this route table.

Available subnets (1/1)

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
☑	Public Subnet	subnet-0d73e137368de...	192.168.1.0/28	–	Main (rtb-0359df70bc7e3f155)

Selected subnets

subnet-0d73e137368de87d0 / Public Subnet



VPC > Route tables

You have successfully updated subnet associations for rtb-0f7623f812818dfe0 / Public Route Table.

Route tables (1/3) Info

Last updated 1 minute ago

	Name	Route table ID	Expli...	Edge...	Main	VPC	Owner ID
□	–	rtb-0348833c04f189597	–	–	Yes	vpc-0ad871c506fcd2795	45284689...
□	–	rtb-0359df70bc7e3f155	–	–	Yes	vpc-0ebaef3c88b5f388e | Test ...	45284689...
☑	Public Route Table	rtb-0f7623f812818dfe0	subnet-...	–	No	vpc-0ebaef3c88b5f388e | Test ...	45284689...

rtb-0f7623f812818dfe0 / Public Route Table

Explicit subnet associations (1)

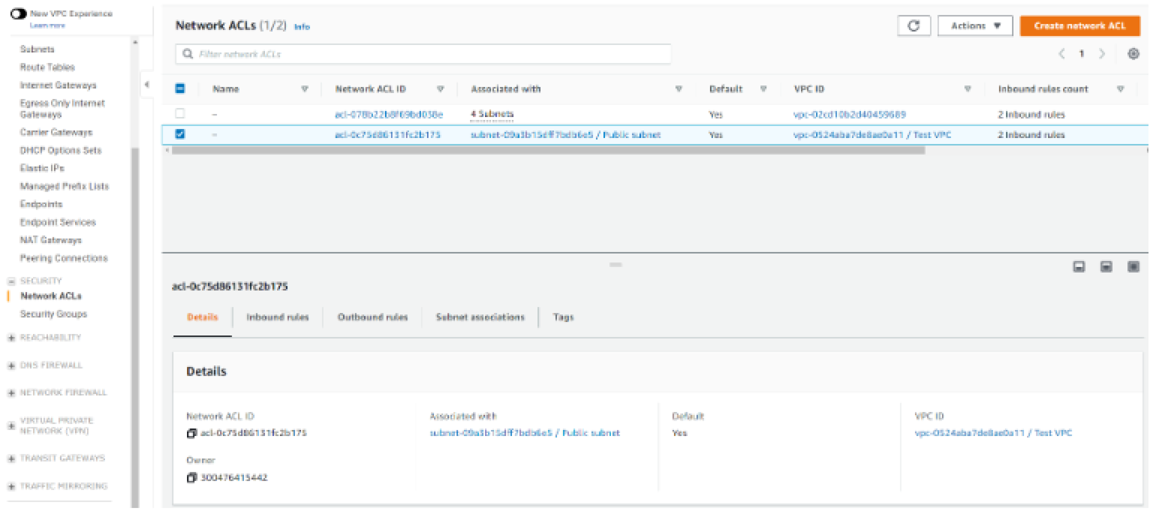
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
Public Subnet	subnet-0d73e137368de87d0	192.168.1.0/28	–

Creating a Network ACL

Recall

Recall that an NACL is a layer of security that acts like a firewall at the subnet level. The rules to set up a NACL are similar to security groups in the way that they control traffic. The following rules apply: NACLs must be associated to a subnet, NACLs are stateless, and they have the following parts: - Rule number: The lowest number rule gets evaluated first. As soon as a rule matches traffic, its applied; for example: 10 or 100. Rule 10 would get evaluated first. - Type of traffic; for example: HTTP or SSH - Protocol: You can specify all or certain types here - Port range: All or specific ones - Destination: Only applies to outbound rules - Allow or Deny specified traffic.

20. From the left navigation pane, select **Network ACLs**. Navigate to the top right corner and select **Create network ACL** to create a Network Access Control Lists (NACLs).



Network ACLs (1/2) Info

	Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count
□	–	acl-078b22b8f69bd038e	4 Subnets	Yes	vpc-02cd10b2d40459689	2 Inbound rules
☑	–	acl-0c75d86131fc2b175	subnet-09a3b15dff7bdb6e5 / Public subnet	Yes	vpc-0524aba7de8ae0a11 / Test VPC	2 Inbound rules

acl-0c75d86131fc2b175

Details | Inbound rules | Outbound rules | Subnet associations | Tags

Details

Network ACL ID	Associated with	Default	VPC ID
acl-0c75d86131fc2b175	subnet-09a3b15dff7bdb6e5 / Public subnet	Yes	vpc-0524aba7de8ae0a11 / Test VPC

Owner
300476415442

Figure: Select Create network ACL

21. On the **Create network ACL**, configure the following: - **Name**: Public Subnet NACL - **VPC**: Choose Test VPC from dropdown - Choose **Create network ACL**

22. On the **Network ACLs** option, from the list of ACLs select **Public Subnet ACL**

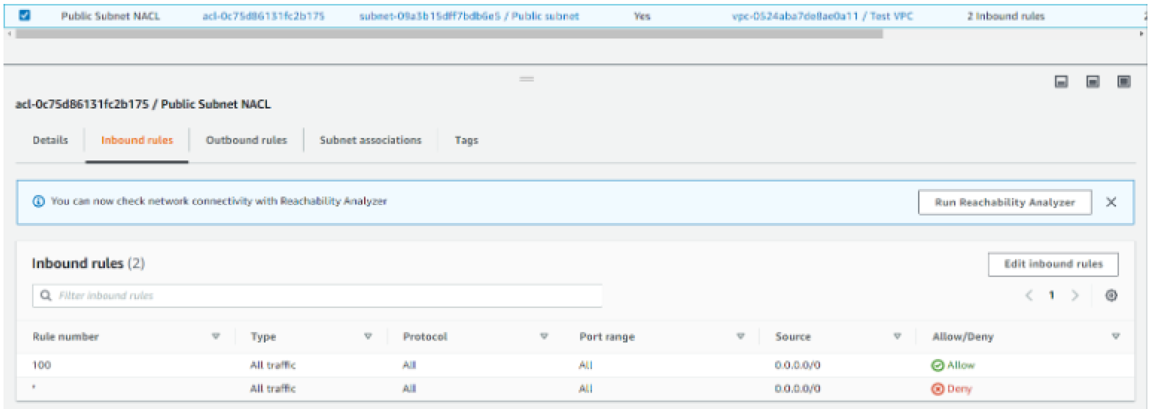
23. From the tabs below, select **Inbound rules** and then choose **Edit inbound rules**

24. On the **Edit inbound rules**, choose **Add new rule** and configure:

    - Rule number: Enter 100
    - Type: Choose **All traffic** from dropdown

25. Choose **Save changes**
26. Back on the **Network ACLs** option, ensure that **Public Subnet ACL** is selected
27. Choose **Outbound rules** and then choose _*Edit outbound rules_
28. On the **Edit outbound rules**, choose **Add new rule** and configure:
    - Rule number: Enter `100`
    - Type: Choose **All traffic** from dropdown
29. Choose **Save changes**

Inbound After creating the NACL, it will should look like the following. This indicates there is only one rule number, which is 100, that states that all traffic, all protocols, all port ranges, from any source (0.0.0.0/0) are allowed to enter (inbound) the subnet. The asterisk * indicates that anything else that does not match this rule is denied.



☑	Public Subnet NACL	acl-0c75d86131fc2b175	subnet-09a3b15dff7bdb6e5 / Public subnet	Yes	vpc-0524aba7de8ae0a11 / Test VPC	2 Inbound rules

acl-0c75d86131fc2b175 / Public Subnet NACL

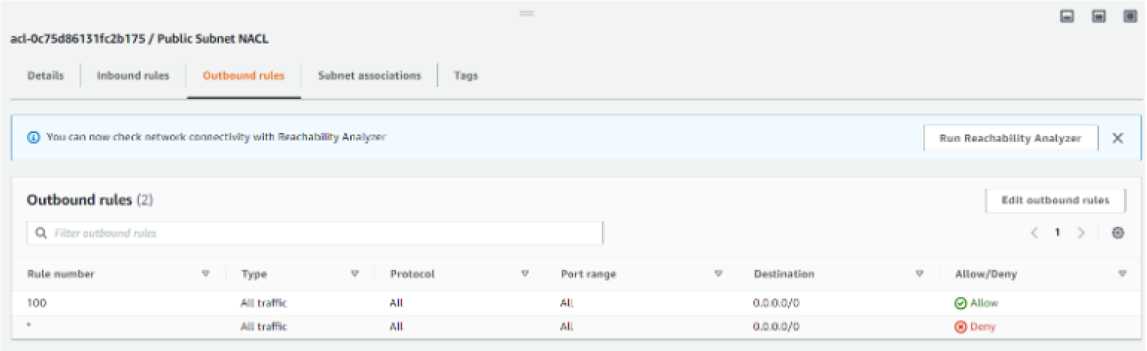
You can now check network connectivity with Reachability Analyzer

Inbound rules (2)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Figure: Default inbound rule configuration for NACL. This will allow all traffic from anywhere and deny anything else that does not match this rule at the subnet level.

Outbound What do you think this rule says?



acl-0c75d86131fc2b175 / Public Subnet NACL

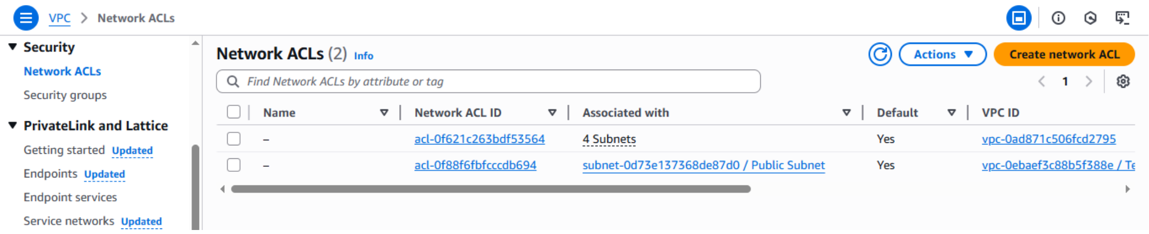
You can now check network connectivity with Reachability Analyzer

Outbound rules (2)

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Figure: Default outbound rule configuration for NACL. This will allow all traffic from anywhere and deny anything else that does not match this rule at the subnet level.

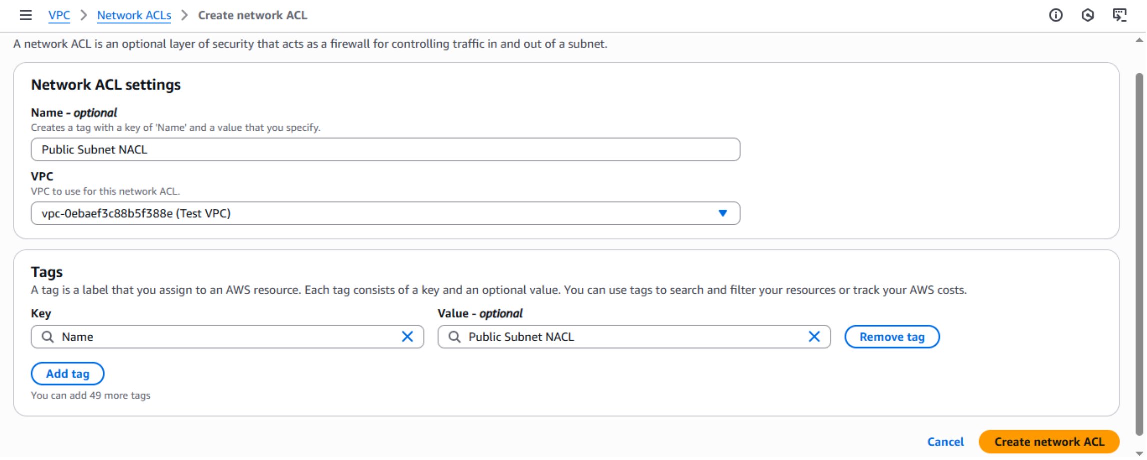
Result:



Network ACLs (2) Info

Find Network ACLs by attribute or tag

Name	Network ACL ID	Associated with	Default	VPC ID
–	acl-0f621c263bdf53564	4 Subnets	Yes	vpc-0ad871c506fcd2795
–	acl-0f88f6fbfcccdb694	subnet-0d73e137368de87d0 / Public Subnet	Yes	vpc-0ebaef3c88b5f388e / Te



A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.

Network ACL settings

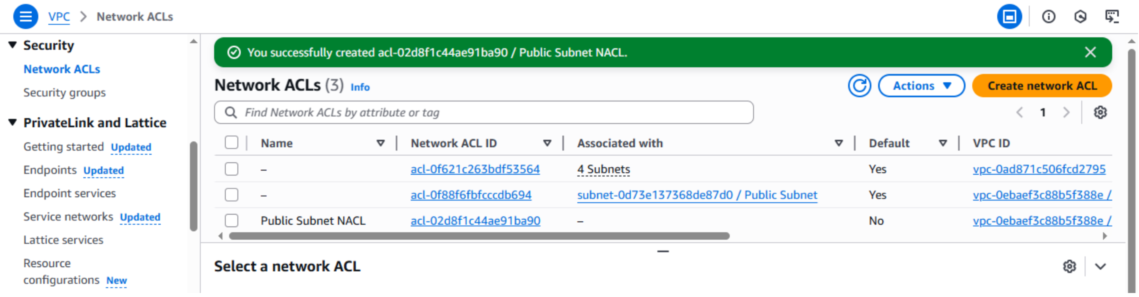
Name - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
Public Subnet NACL

VPC
VPC to use for this network ACL.
vpc-0ebaef3c88b5f388e (Test 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 NACL

You can add 49 more tags



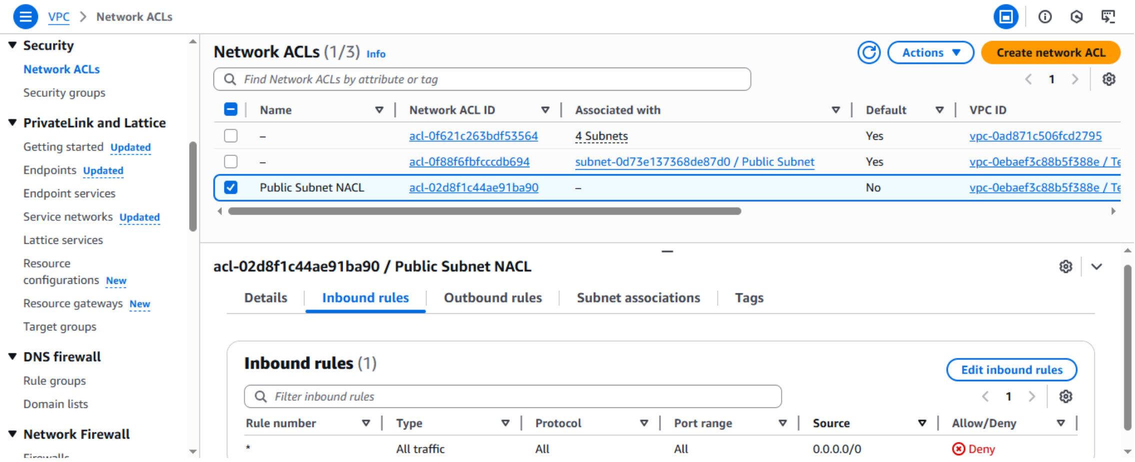
You successfully created acl-02d8f1c44ae91ba90 / Public Subnet NACL.

Network ACLs (3) Info

Find Network ACLs by attribute or tag

Name	Network ACL ID	Associated with	Default	VPC ID
–	acl-0f621c263bdf53564	4 Subnets	Yes	vpc-0ad871c506fcd2795
–	acl-0f88f6fbfcccdb694	subnet-0d73e137368de87d0 / Public Subnet	Yes	vpc-0ebaef3c88b5f388e /
Public Subnet NACL	acl-02d8f1c44ae91ba90	–	No	vpc-0ebaef3c88b5f388e /

Select a network ACL



Network ACLs (1/3) Info

Find Network ACLs by attribute or tag

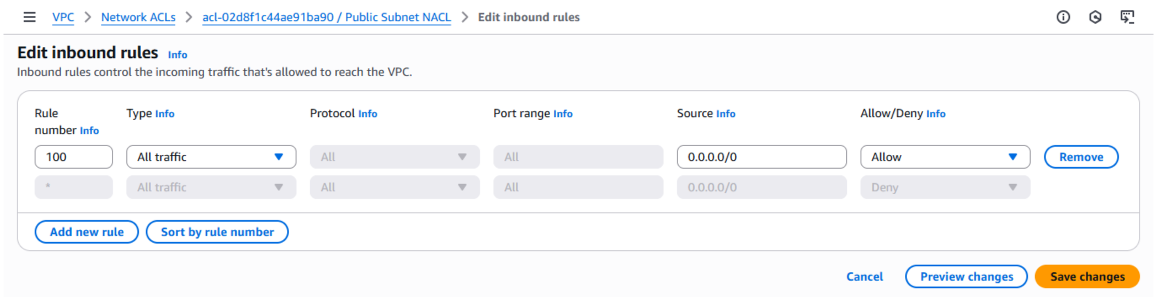
	Name	Network ACL ID	Associated with	Default	VPC ID
□	–	acl-0f621c263bdf53564	4 Subnets	Yes	vpc-0ad871c506fcd2795
□	–	acl-0f88f6fbfcccdb694	subnet-0d73e137368de87d0 / Public Subnet	Yes	vpc-0ebaef3c88b5f388e / Te
☑	Public Subnet NACL	acl-02d8f1c44ae91ba90	–	No	vpc-0ebaef3c88b5f388e / Te

acl-02d8f1c44ae91ba90 / Public Subnet NACL

Inbound rules (1)

Filter inbound rules

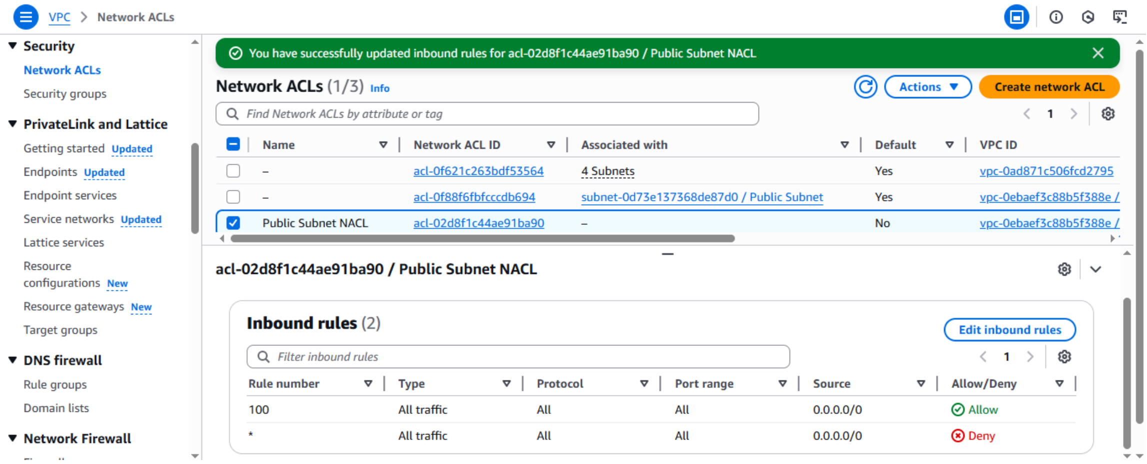
Rule number	Type	Protocol	Port range	Source	Allow/Deny
*	All traffic	All	All	0.0.0.0/0	⊗ Deny


VPC > Network ACLs > acl-02d8f1c44ae91ba90 / Public Subnet NACL > Edit inbound rules

Edit inbound rules Info

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

Rule number Info	Type Info	Protocol Info	Port range Info	Source Info	Allow/Deny Info	
100	All traffic	All	All	0.0.0.0/0	Allow	Remove
*	All traffic	All	All	0.0.0.0/0	Deny	


VPC > Network ACLs

You have successfully updated inbound rules for acl-02d8f1c44ae91ba90 / Public Subnet NACL

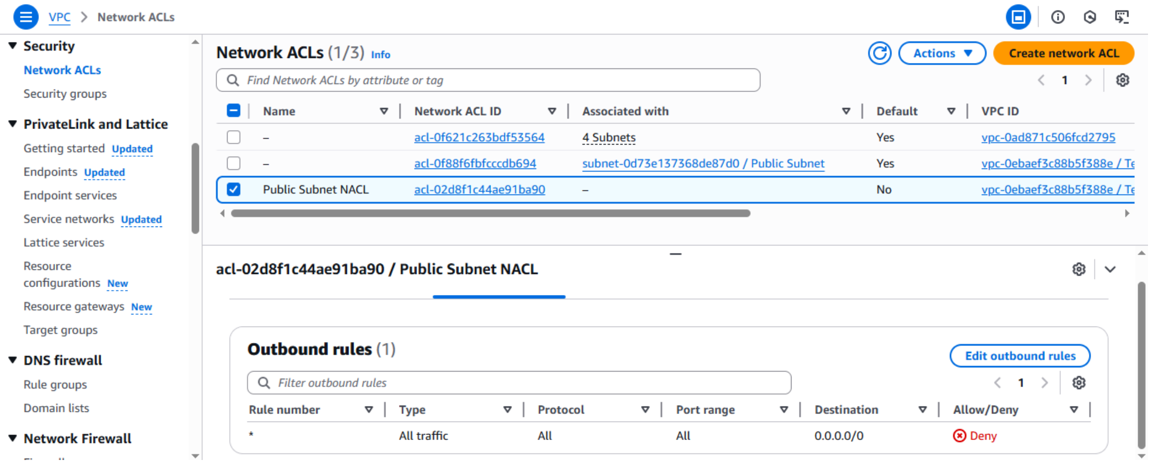
Network ACLs (1/3) Info

	Name	Network ACL ID	Associated with	Default	VPC ID
□	–	acl-0f621c263bdf53564	4 Subnets	Yes	vpc-0ad871c506fcd2795
□	–	acl-0f88f6fbfcccdb694	subnet-0d73e137368de87d0 / Public Subnet	Yes	vpc-0ebaef3c88b5f388e /
☑	Public Subnet NACL	acl-02d8f1c44ae91ba90	–	No	vpc-0ebaef3c88b5f388e /

acl-02d8f1c44ae91ba90 / Public Subnet NACL

Inbound rules (2)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	✓ Allow
*	All traffic	All	All	0.0.0.0/0	⊗ Deny


VPC > Network ACLs

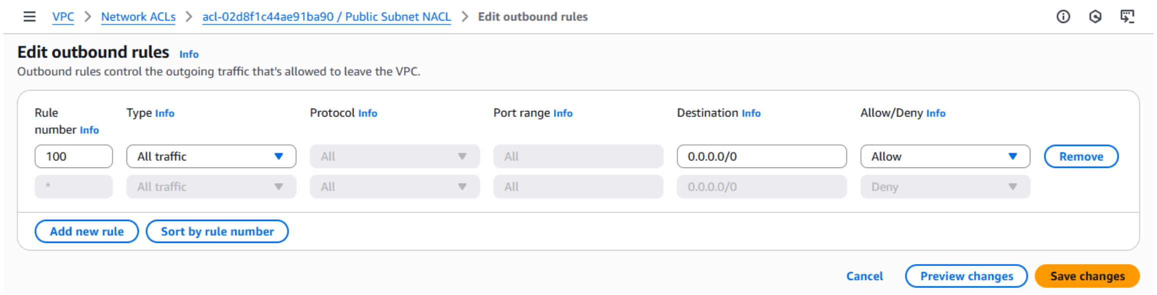
Network ACLs (1/3) Info

	Name	Network ACL ID	Associated with	Default	VPC ID
□	–	acl-0f621c263bdf53564	4 Subnets	Yes	vpc-0ad871c506fcd2795
□	–	acl-0f88f6fbfcccdb694	subnet-0d73e137368de87d0 / Public Subnet	Yes	vpc-0ebaef3c88b5f388e / Te
☑	Public Subnet NACL	acl-02d8f1c44ae91ba90	–	No	vpc-0ebaef3c88b5f388e / Te

acl-02d8f1c44ae91ba90 / Public Subnet NACL

Outbound rules (1)

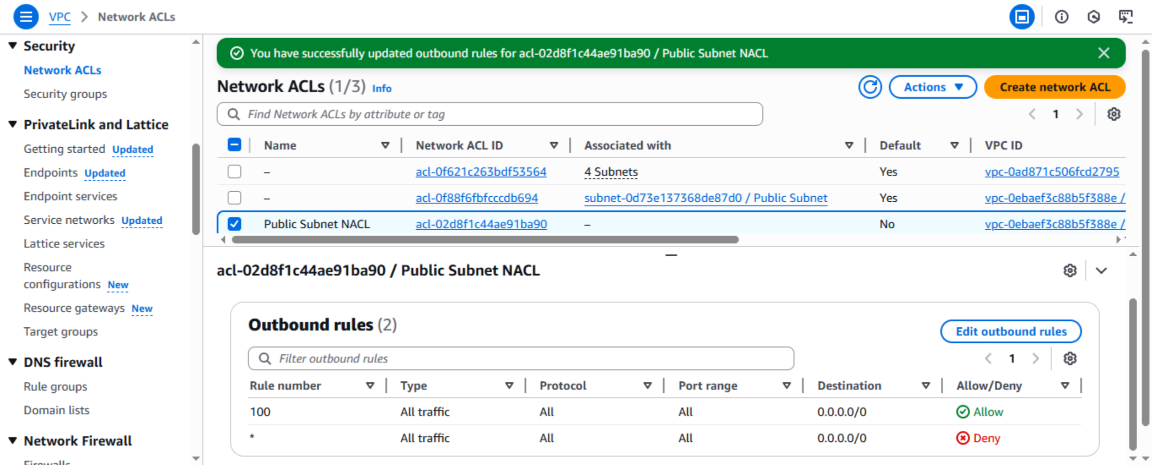
Rule number	Type	Protocol	Port range	Destination	Allow/Deny
*	All traffic	All	All	0.0.0.0/0	⊗ Deny


VPC > Network ACLs > acl-02d8f1c44ae91ba90 / Public Subnet NACL > Edit outbound rules

Edit outbound rules Info

Outbound rules control the outgoing traffic that's allowed to leave the VPC.

Rule number Info	Type Info	Protocol Info	Port range Info	Destination Info	Allow/Deny Info	
100	All traffic	All	All	0.0.0.0/0	Allow	Remove
*	All traffic	All	All	0.0.0.0/0	Deny	



You have successfully updated outbound rules for acl-02d8f1c44ae91ba90 / Public Subnet NACL

Network ACLs (1/3) Info

Find Network ACLs by attribute or tag

	Name	Network ACL ID	Associated with	Default	VPC ID
□	–	acl-0f621c263bdf53564	4 Subnets	Yes	vpc-0ad871c506fcd2795
□	–	acl-0f88f6fbfcccdb694	subnet-0d73e137368de87d0 / Public Subnet	Yes	vpc-0ebaef3c88b5f388e /
☑	Public Subnet NACL	acl-02d8f1c44ae91ba90	–	No	vpc-0ebaef3c88b5f388e /

acl-02d8f1c44ae91ba90 / Public Subnet NACL

Outbound rules (2)

Filter outbound rules

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	✓ Allow
*	All traffic	All	All	0.0.0.0/0	⊗ Deny

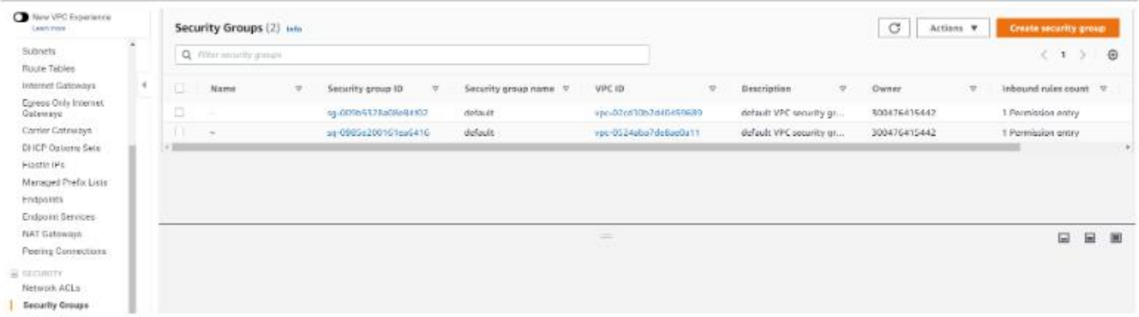
Creating a Security Group

Recall

Recall that a security group is a virtual firewall at the instance level that controls inbound and outbound traffic. Just like a NACL, security groups control traffic; however, security groups cannot deny traffic. Security groups are stateful; you must allow traffic through the security group as it blocks everything by default, and it must be associated to an instance. A security group has the following parts for both inbound and outbound rules:

- Inbound Source: It can be an IP or a specific resource
- Outbound Destination: Can by an IP such as anywhere (0.0.0.0/0)
- Protocol: Example UDP or TCP
- Port range: All or specific range
- Description: You can input a description

30. From the left navigation pane, select **Security Groups**. Navigate to the top right corner and select **Create security group** to create a security group.



Security Groups (2) Info

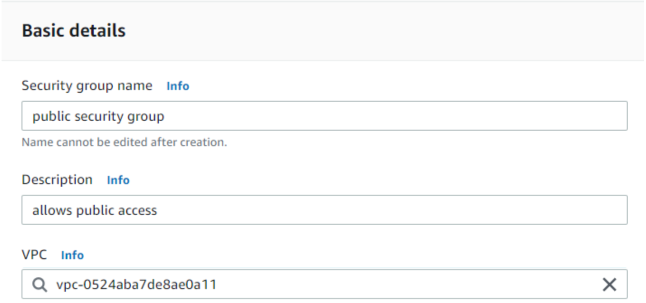
Filter security groups

	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count
□	–	sg-009b5178a08e84f02	default	vpc-02cd10b7dd0459689	default VPC security gr...	300476415442	1 Permission entry
□	–	sg-0985e200161ea6416	default	vpc-0524aba7de8ae0a11	default VPC security gr...	300476415442	1 Permission entry

Figure: Select Create security group

Configure like the following image of the Basic details page:

Note: In the VPC portion, remove the current VPC, and select **Test VPC**.



Basic details

Security group name Info

public security group

Name cannot be edited after creation.

Description Info

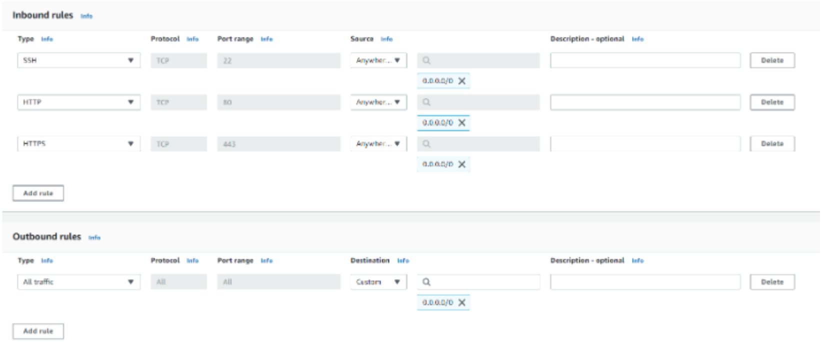
allows public access

VPC Info

vpc-0524aba7de8ae0a11

Figure: Configure the Basic details page

The completed security group is shown below. This indicates that for **Inbound rules** you are allowing SSH, HTTP, and HTTPS types of traffic, each of which has its own protocols and port range. The source from which this traffic reaches your instance can be originating from anywhere. For **Outbound rules**, you are allowing all traffic from outside your instance.



Inbound rules Info

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

Add rule

Outbound rules Info

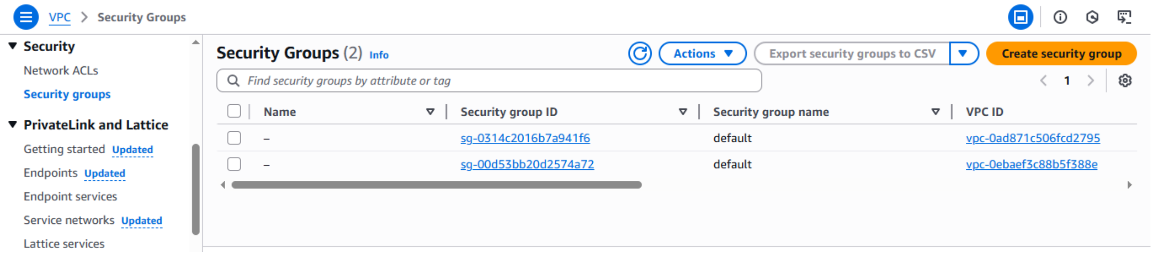
Type Info	Protocol Info	Port range Info	Destination Info		Description - optional Info	
All traffic	All	All	Custom	0.0.0.0/0		Delete

Add rule

Figure: Configuration details for inbound and outbound rules for the security group

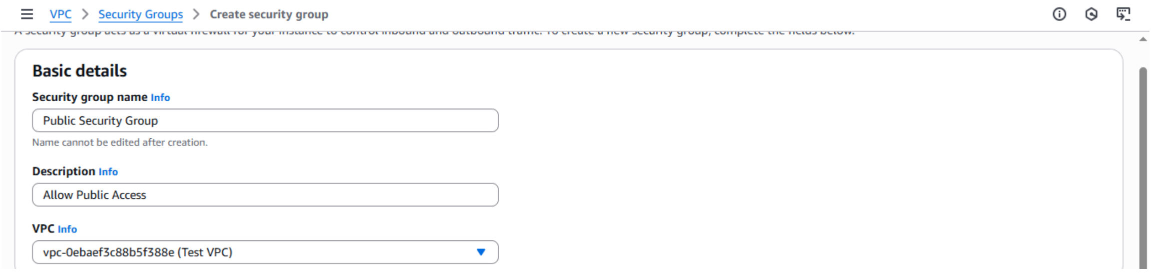
You now have a functional VPC. The next task is to launch an EC2 instance to ensure that everything works.

Result:



Security Groups (2) Info

	Name	Security group ID	Security group name	VPC ID
□	–	sg-0314c2016b7a941f6	default	vpc-0ad871c506fcd2795
□	–	sg-00d53bb20d2574a72	default	vpc-0ebaef3c88b5f388e



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.

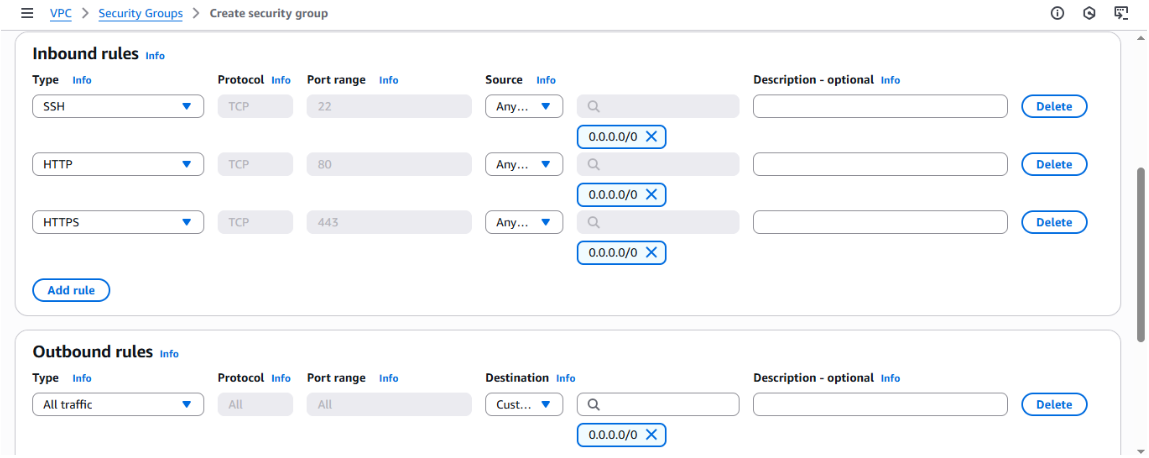
Basic details

Security group name Info: Public Security Group

Name cannot be edited after creation.

Description Info: Allow Public Access

VPC Info: vpc-0ebaef3c88b5f388e (Test VPC)

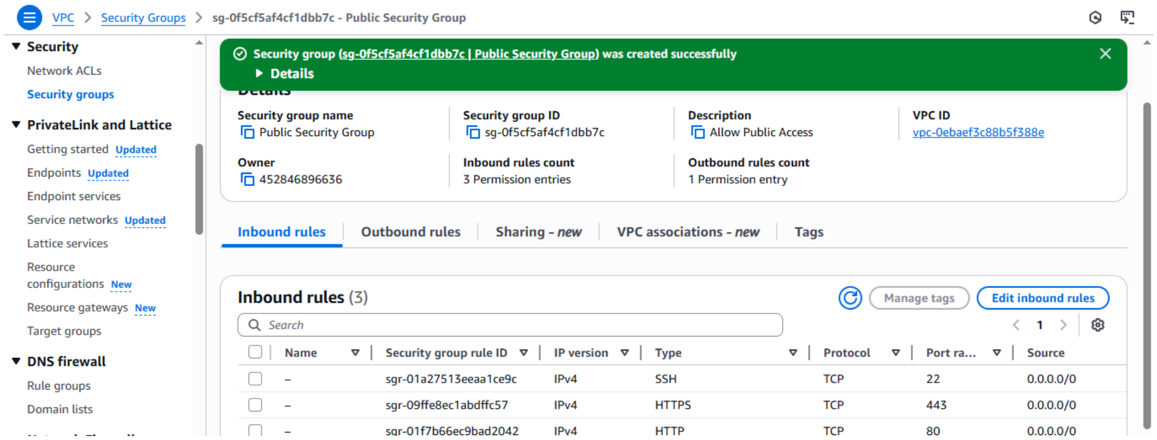


Inbound rules Info

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

Outbound rules Info

Type Info	Protocol Info	Port range Info	Destination Info		Description - optional Info	
All traffic	All	All	Cust...	0.0.0.0/0		Delete



Security group (sg-0f5cf5af4cf1dbb7c | Public Security Group) was created successfully

▶ Details

Security group name: Public Security Group

Security group ID: sg-0f5cf5af4cf1dbb7c

Description: Allow Public Access

VPC ID: vpc-0ebaef3c88b5f388e

Owner: 452846896636

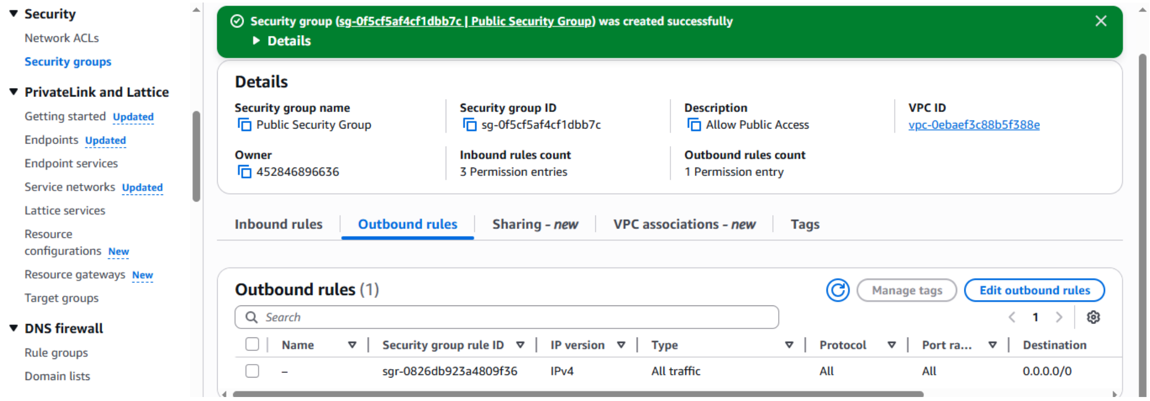
Inbound rules count: 3 Permission entries

Outbound rules count: 1 Permission entry

Inbound rules | Outbound rules | Sharing - new | VPC associations - new | Tags

Inbound rules (3)

□	Name	Security group rule ID	IP version	Type	Protocol	Port ra...	Source
□	–	sgr-01a27513eeaa1ce9c	IPv4	SSH	TCP	22	0.0.0.0/0
□	–	sgr-09ffe8ec1abdffc57	IPv4	HTTPS	TCP	443	0.0.0.0/0
□	–	sgr-01f7b66ec9bad2042	IPv4	HTTP	TCP	80	0.0.0.0/0



Security group (sg-0f5cf5af4cf1dbb7c | Public Security Group) was created successfully

▶ Details

Details

Security group name: Public Security Group

Security group ID: sg-0f5cf5af4cf1dbb7c

Description: Allow Public Access

VPC ID: vpc-0ebaef3c88b5f388e

Owner: 452846896636

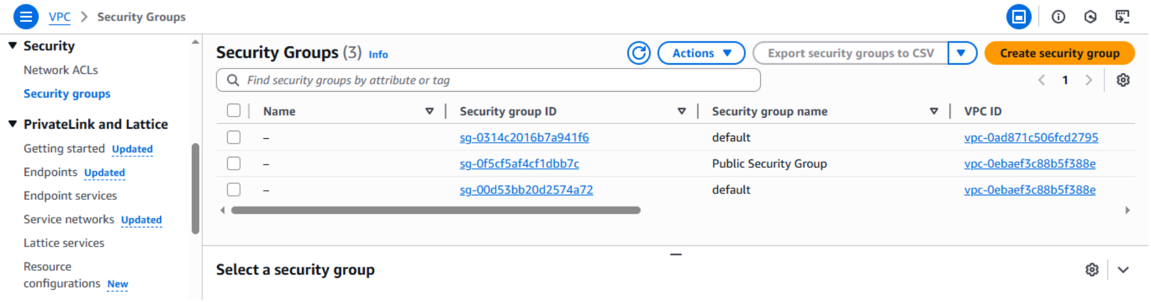
Inbound rules count: 3 Permission entries

Outbound rules count: 1 Permission entry

Inbound rules | Outbound rules | Sharing - new | VPC associations - new | Tags

Outbound rules (1)

□	Name	Security group rule ID	IP version	Type	Protocol	Port ra...	Destination
□	–	sgr-0826db923a4809f36	IPv4	All traffic	All	All	0.0.0.0/0



Security Groups (3) Info

Name	Security group ID	Security group name	VPC ID
–	sg-0314c2016b7a941f6	default	vpc-0ad871c506fcd2795
–	sg-0f5cf5af4cf1dbb7c	Public Security Group	vpc-0ebaef3c88b5f388e
–	sg-00d53bb20d2574a72	default	vpc-0ebaef3c88b5f388e

Select a security group

Task 2: Launch EC2 instance and SSH into instance

In task 2, you will launch an EC2 instance within your Public subnet and test connectivity by running the command **ping**. This will validate that your infrastructure is correct, such as security groups and network ACLs, to ensure that they are not blocking any traffic from your instance to the internet and vice versa. This will validate that you have a route to the IGW via the route table and that the IGW is attached.

31. On the AWS Management Console, in the **Search** bar, enter and choose EC2 to go to the **EC2 Management Console**.
32. In the left navigation pane, choose **Instances**.
33. Choose **Launch instances** and configure the following options:

- In the **Name and tags** section, leave the Name blank.
- In the **Application and OS Images (Amazon Machine Image)** section, configure the following options:
  - **Quick Start:** Choose **Amazon Linux**.
  - **Amazon Machine Image (AMI):** Choose **Amazon Linux 2023 AMI**.
- In the **Instance type** section, choose **t3.micro**.
- In the **Key pair (login)** section, choose **vockey**.

34. In the **Network settings** section, choose Edit and configure the following options:

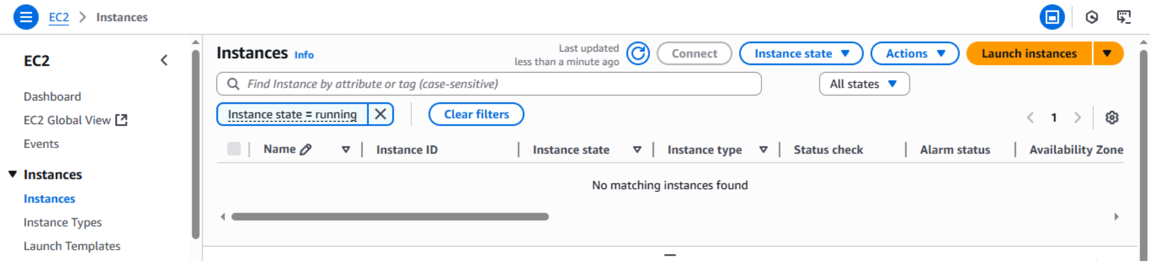
- **VPC -** ***required***: Choose **Test VPC**.
- **Subnet:** Choose **Public Subnet**.
- **Auto-assign public IP:** Choose **Enable**.
- **Firewall (security groups):** Choose **Select existing security group**.
  - Choose **public security group**.

35. Choose **Launch instance**.

36. To display the launched instance, choose **View all instances**.

The EC2 instance named **Bastion Server** is initially in a *Pending* state. The **Instance state** then changes to *Running* to indicate that the instance has finished booting.

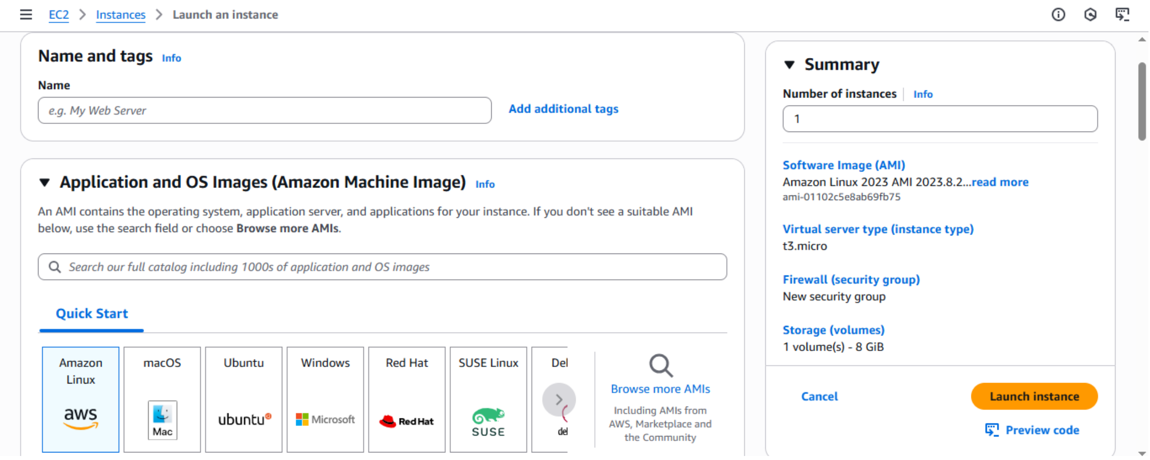
Result:



Instance state = running

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone

No matching instances found



Name and tags

Name: *e.g. My Web Server*

Application and OS Images (Amazon Machine Image)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose **Browse more AMIs**.

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

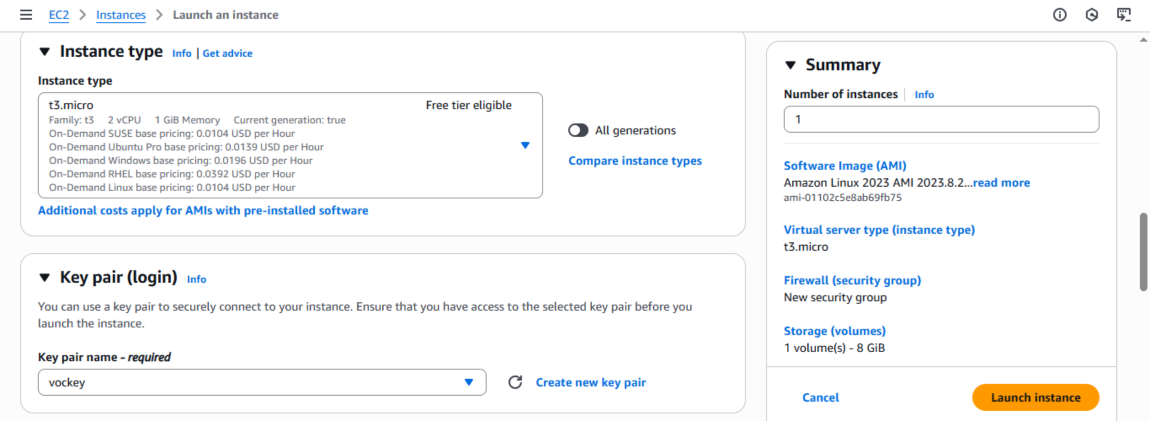
Number of instances: 1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.8.2...read more
ami-01102c5e8ab69fb75

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

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



Instance type

Instance type: t3.micro — Free tier eligible
Family: t3 2 vCPU 1 GiB Memory Current generation: true
On-Demand SUSE base pricing: 0.0104 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0139 USD per Hour
On-Demand Windows base pricing: 0.0196 USD per Hour
On-Demand RHEL base pricing: 0.0392 USD per Hour
On-Demand Linux base pricing: 0.0104 USD per Hour

Key pair (login)

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

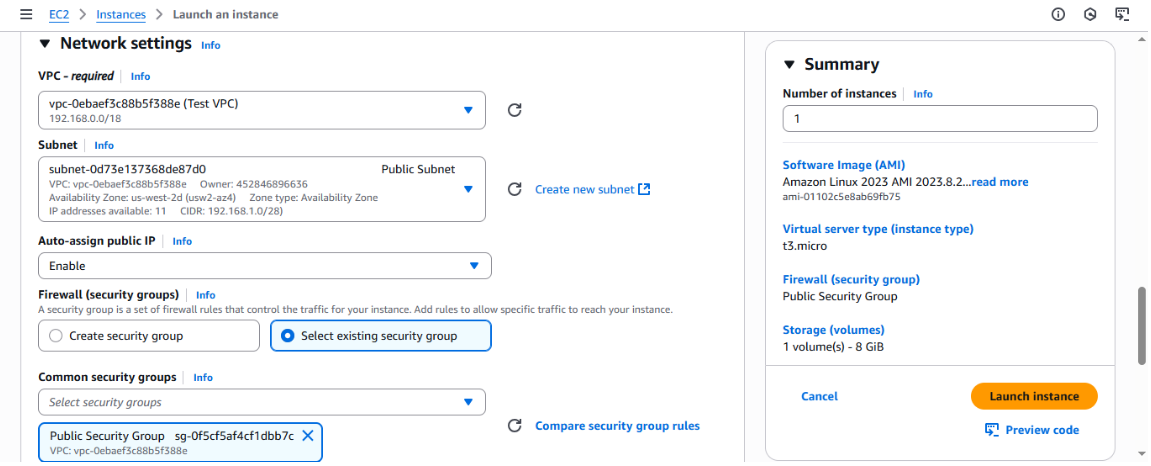
Number of instances: 1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.8.2...read more
ami-01102c5e8ab69fb75

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

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



EC2 > Instances > Launch an instance

Network settings Info

VPC - *required* | Info

vpc-0ebaef3c88b5f388e (Test VPC)
192.168.0.0/18

Subnet | Info

subnet-0d73e137368de87d0 Public Subnet
VPC: vpc-0ebaef3c88b5f388e Owner: 452846896636
Availability Zone: us-west-2d (usw2-az4) Zone type: Availability Zone
IP addresses available: 11 CIDR: 192.168.1.0/28)

Create new subnet

Auto-assign public IP | Info

Enable

Firewall (security groups) | Info

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

○ Create security group ● Select existing security group

Common security groups | Info

Select security groups

Public Security Group sg-0f5cf5af4cf1dbb7c
VPC: vpc-0ebaef3c88b5f388e

Compare security group rules

Summary

Number of instances | Info

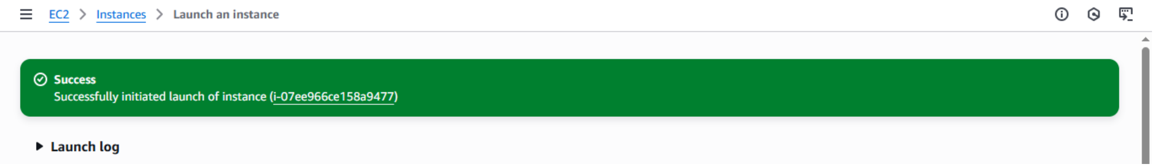
1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.8.2...read more
ami-01102c5e8ab69fb75

Virtual server type (instance type)
t3.micro

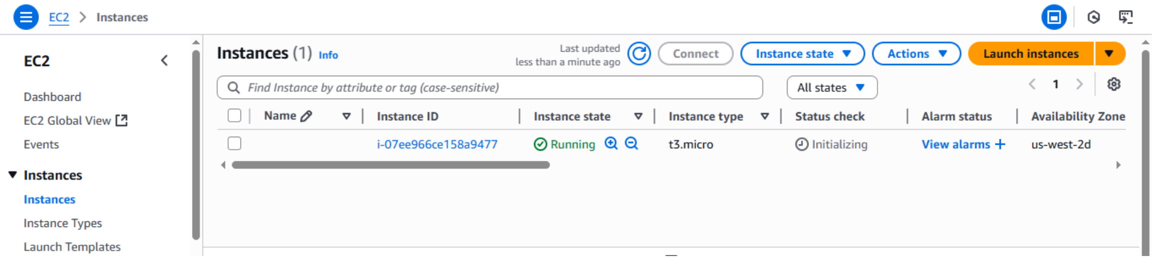
Firewall (security group)
Public Security Group

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



EC2 > Instances > Launch an instance

Success
Successfully initiated launch of instance (i-07ee966ce158a9477)



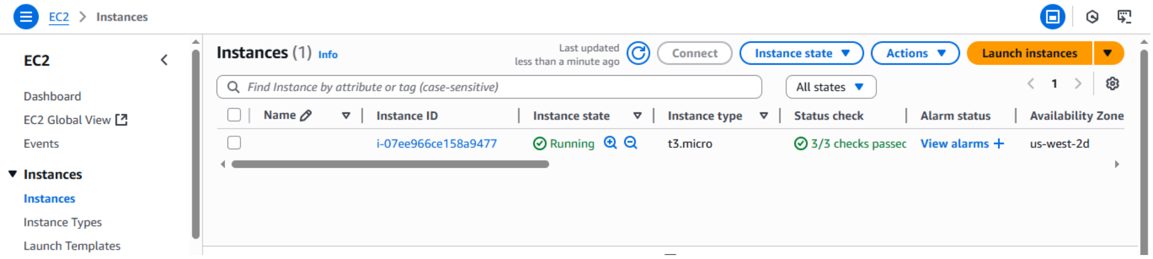
EC2 > Instances

Instances (1) Info

Last updated less than a minute ago

Find Instance by attribute or tag (case-sensitive)

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
□		i-07ee966ce158a9477	✓ Running	t3.micro	Initializing	View alarms +	us-west-2d



EC2 > Instances

Instances (1) Info

Last updated less than a minute ago

Find Instance by attribute or tag (case-sensitive)

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
□		i-07ee966ce158a9477	✓ Running	t3.micro	✓ 3/3 checks passec	View alarms +	us-west-2d

Use SSH to connect to an Amazon Linux EC2 instance

Ways to connect Amazon Linux EC2

The following instructions vary slightly depending on whether you are using Windows or Mac/Linux.

Windows Users: Using SSH to Connect

These instructions are specifically for Windows users. If you are using macOS or Linux, skip to the next section.

37. Select the Details drop-down menu above these instructions you are currently reading, and then select Show. A Credentials window will be presented.
38. Select the **Download PPK** button and save the **labsuser.ppk** file. *Typically your browser will save it to the Downloads directory.*
39. Make a note of the **PublicIP** address.
40. Then exit the Details panel by selecting the **X**.
41. Download **PuTTY** to SSH into the Amazon EC2 instance. If you do not have PuTTY installed on your computer.
42. Open **putty.exe**
43. Configure your PuTTY session

macOS and Linux Users

These instructions are specifically for Mac/Linux users. If you are a Windows user, skip ahead to the next task.

45. Select the Details drop-down menu above these instructions you are currently reading, and then select Show. A Credentials window will be presented.
46. Select the **Download PEM** button and save the **labsuser.pem** file.
47. Make a note of **PublicIP**, the IPV4 server's address you have to connect to.
48. Then exit the Details panel by selecting the **X**.
49. Open a terminal window, and change directory `cd` to the directory where the *labsuser.pem* file was downloaded. For example, if the *labuser.pem* file was saved to your Downloads directory, run this command:

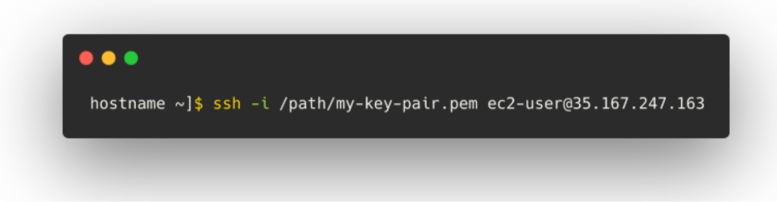
    ```
    cd ~/Downloads
    ```

50. Change the permissions on the key to be read-only, by running this command:

    ```
    chmod 400 labsuser.pem
    ```

51. Run the below command *(replace **<public-ip>** with the server's address you copied earlier)*:

```
ssh -i labsuser.pem ec2-user@<public-ip>
```



```
hostname ~]$ ssh -i /path/my-key-pair.pem ec2-user@35.167.247.163
```

Figure: SSH using a terminal for Mac.

52. Type `yes` when prompted to allow the first connection to this remote SSH server. Because you are using a key pair for authentication, you will not be prompted for a password.

Task 3: Use ping to test internet connectivity

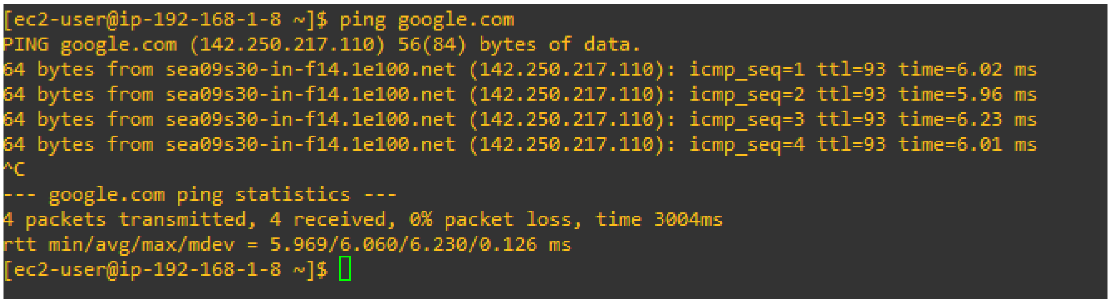
53. Run the following command to test internet connectivity:

```
ping google.com
```

After a few seconds, exit ping by holding **CTRL+C** on Windows or **CMD+C** on Mac to exit.

You should get the following result:

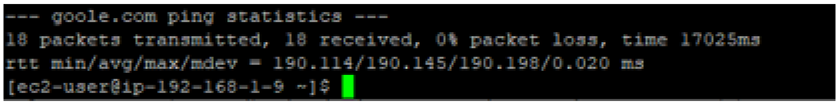
Successful ping:



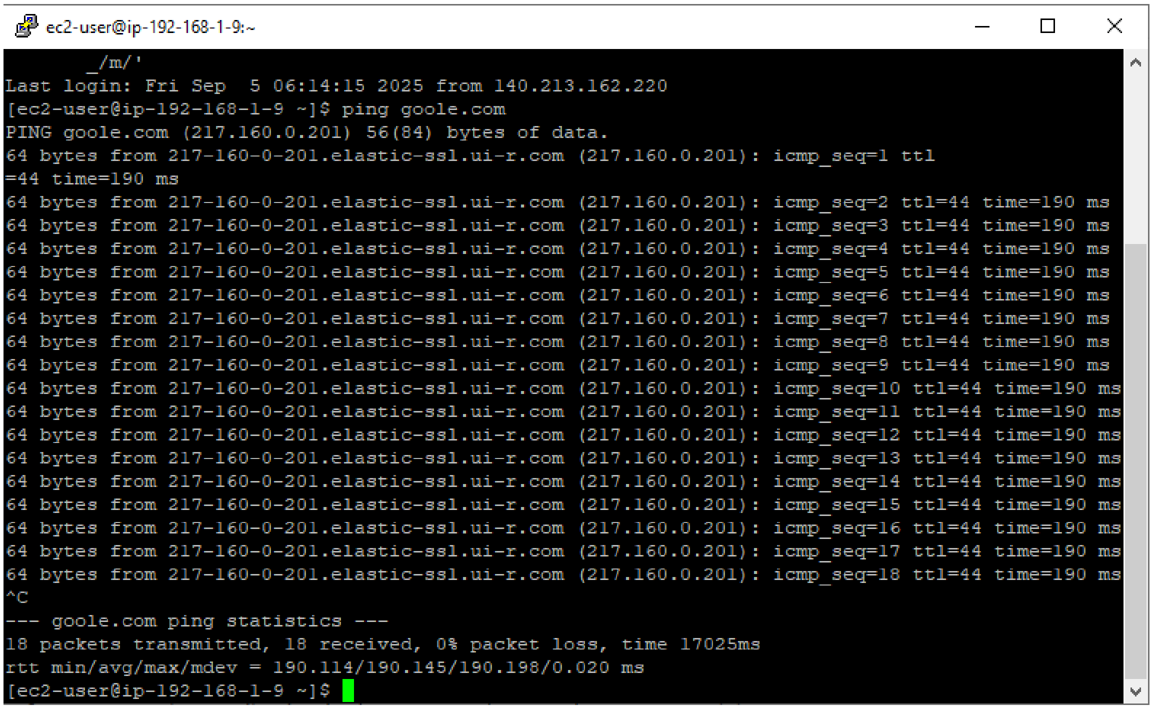
```
[ec2-user@ip-192-168-1-8 ~]$ ping google.com
PING google.com (142.250.217.110) 56(84) bytes of data.
64 bytes from sea09s30-in-f14.1e100.net (142.250.217.110): icmp_seq=1 ttl=93 time=6.02 ms
64 bytes from sea09s30-in-f14.1e100.net (142.250.217.110): icmp_seq=2 ttl=93 time=5.96 ms
64 bytes from sea09s30-in-f14.1e100.net (142.250.217.110): icmp_seq=3 ttl=93 time=6.23 ms
64 bytes from sea09s30-in-f14.1e100.net (142.250.217.110): icmp_seq=4 ttl=93 time=6.01 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 5.969/6.060/6.230/0.126 ms
[ec2-user@ip-192-168-1-8 ~]$
```

Run ping to test connectivity. The above results are saying you have replies from google.com and have 0% packet loss.

If you are getting replies back, that means that you have connectivity.



```
--- goole.com ping statistics ---
18 packets transmitted, 18 received, 0% packet loss, time 17025ms
rtt min/avg/max/mdev = 190.114/190.145/190.198/0.020 ms
[ec2-user@ip-192-168-1-9 ~]$
```



```
       _/m/'
Last login: Fri Sep  5 06:14:15 2025 from 140.213.162.220
[ec2-user@ip-192-168-1-9 ~]$ ping goole.com
PING goole.com (217.160.0.201) 56(84) bytes of data.
64 bytes from 217-160-0-201.elastic-ssl.ui-r.com (217.160.0.201): icmp_seq=1 ttl
=44 time=190 ms
64 bytes from 217-160-0-201.elastic-ssl.ui-r.com (217.160.0.201): icmp_seq=2 ttl=44 time=190 ms
64 bytes from 217-160-0-201.elastic-ssl.ui-r.com (217.160.0.201): icmp_seq=3 ttl=44 time=190 ms
64 bytes from 217-160-0-201.elastic-ssl.ui-r.com (217.160.0.201): icmp_seq=4 ttl=44 time=190 ms
64 bytes from 217-160-0-201.elastic-ssl.ui-r.com (217.160.0.201): icmp_seq=5 ttl=44 time=190 ms
64 bytes from 217-160-0-201.elastic-ssl.ui-r.com (217.160.0.201): icmp_seq=6 ttl=44 time=190 ms
64 bytes from 217-160-0-201.elastic-ssl.ui-r.com (217.160.0.201): icmp_seq=7 ttl=44 time=190 ms
64 bytes from 217-160-0-201.elastic-ssl.ui-r.com (217.160.0.201): icmp_seq=8 ttl=44 time=190 ms
64 bytes from 217-160-0-201.elastic-ssl.ui-r.com (217.160.0.201): icmp_seq=9 ttl=44 time=190 ms
64 bytes from 217-160-0-201.elastic-ssl.ui-r.com (217.160.0.201): icmp_seq=10 ttl=44 time=190 ms
64 bytes from 217-160-0-201.elastic-ssl.ui-r.com (217.160.0.201): icmp_seq=11 ttl=44 time=190 ms
64 bytes from 217-160-0-201.elastic-ssl.ui-r.com (217.160.0.201): icmp_seq=12 ttl=44 time=190 ms
64 bytes from 217-160-0-201.elastic-ssl.ui-r.com (217.160.0.201): icmp_seq=13 ttl=44 time=190 ms
64 bytes from 217-160-0-201.elastic-ssl.ui-r.com (217.160.0.201): icmp_seq=14 ttl=44 time=190 ms
64 bytes from 217-160-0-201.elastic-ssl.ui-r.com (217.160.0.201): icmp_seq=15 ttl=44 time=190 ms
64 bytes from 217-160-0-201.elastic-ssl.ui-r.com (217.160.0.201): icmp_seq=16 ttl=44 time=190 ms
64 bytes from 217-160-0-201.elastic-ssl.ui-r.com (217.160.0.201): icmp_seq=17 ttl=44 time=190 ms
64 bytes from 217-160-0-201.elastic-ssl.ui-r.com (217.160.0.201): icmp_seq=18 ttl=44 time=190 ms
^C
--- goole.com ping statistics ---
18 packets transmitted, 18 received, 0% packet loss, time 17025ms
rtt min/avg/max/mdev = 190.114/190.145/190.198/0.020 ms
[ec2-user@ip-192-168-1-9 ~]$ 
```

Lab Complete

Congratulations! You have completed the lab.

54. Choose **End Lab** at the top of this page, and then select **Yes** to confirm that you want to end the lab.

    A panel indicates that *You may close this message box now. Lab resources are terminating...*

55. Choose the **X** in the upper-right corner to close the **End Lab** panel.