Introduction to Amazon Virtual Private Cloud (VPC)

Lab overview

This lab introduces you to Amazon Virtual Private Cloud (Amazon VPC). In this lab you use the Amazon VPC wizard to create a VPC, attach an Internet gateway, add a subnet and then define routing for the VPC so that traffic can flow between the subnet and the Internet gateway.

Objectives

By the end of this lab, you should be able to do the following:

- Create an Amazon VPC Using the VPC Wizard
- Explore the basic components of a VPC including:
    - Public and private subnets
    - Route tables and routes
    - NAT gateways
    - Network ACLs

Start lab

1. To launch the lab, at the top of the page, choose **Start Lab**.

Caution: You must wait for the provisioned AWS services to be ready before you can continue.

2. To open the lab, choose **Open Console** .

You are automatically signed in to the AWS Management Console in a new web browser tab.

Warning: Do not change the **Region** unless instructed.

Services used in this lab

Amazon Virtual Private Cloud (VPC)

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications.

Task 1: Create an Amazon VPC

In this task you create an Amazon VPC using the *VPC wizard*. The wizard automatically creates a VPC based upon parameters you specify. Using the VPC Wizard is much simpler than manually creating each component of the VPC.

Here is an overview of the VPC you create:

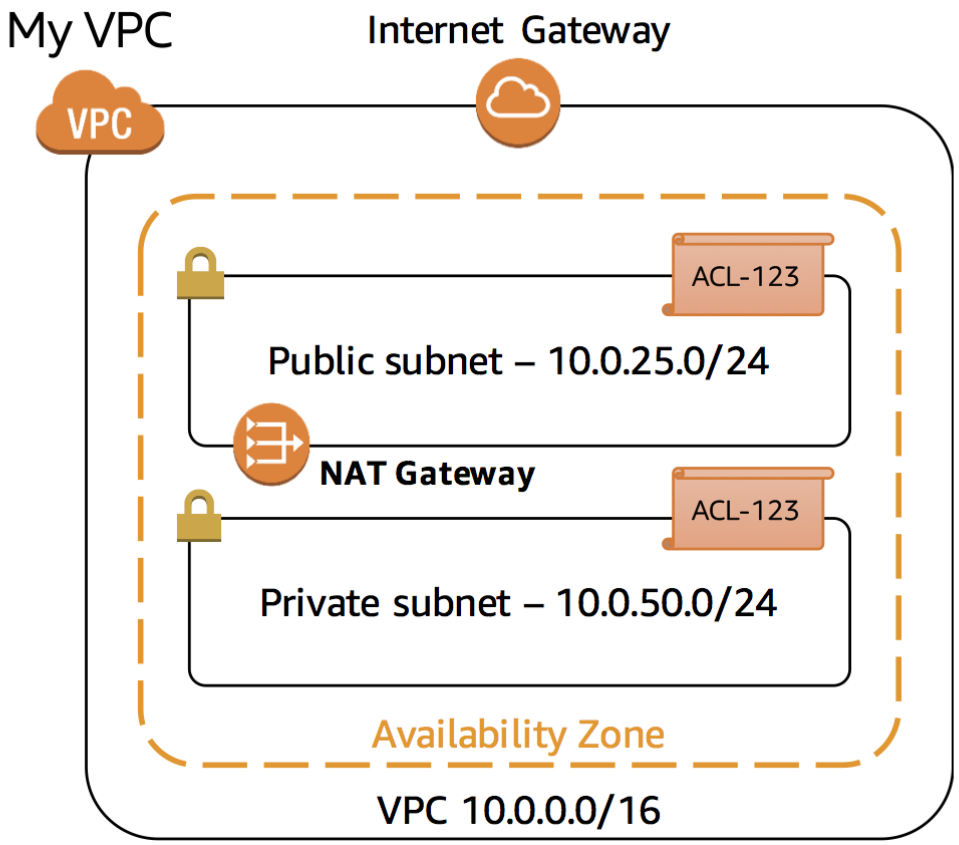
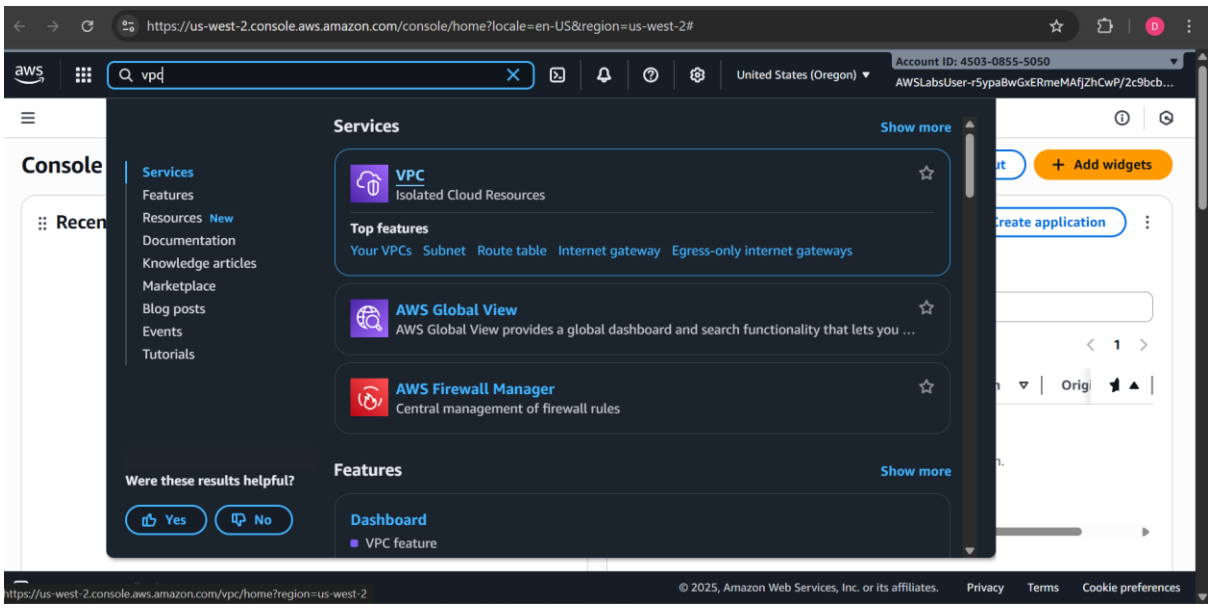


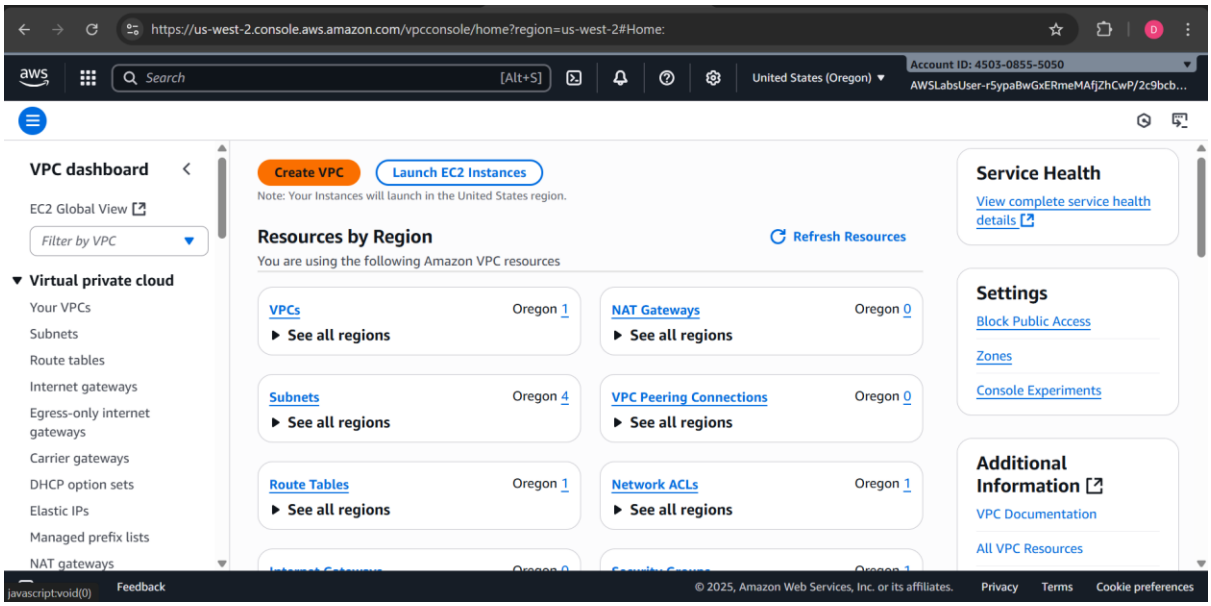
Image description: The preceding diagram depicts an Amazon Virtual Private Cloud (VPC) consisting of a public subnet and a private subnet. An internet gateway is attached to the Amazon VPC, and a Network Address Translation (NAT) gateway is launched in the public subnet.

Each component is explained in more detail later in this lab.

3. At the top of the AWS Management Console, in the search bar, search for and choose VPC



4. Choose **Create VPC**.



5. On **Create VPC** page, under **VPC settings** section:
    1. Choose **VPC and more** (the second option).

       Note: You are now presented with parameters to customize the VPC configuration.

    2. For **Name tag auto-generation**, select **Auto-generate** and enter

       `Lab`

       in the text box.

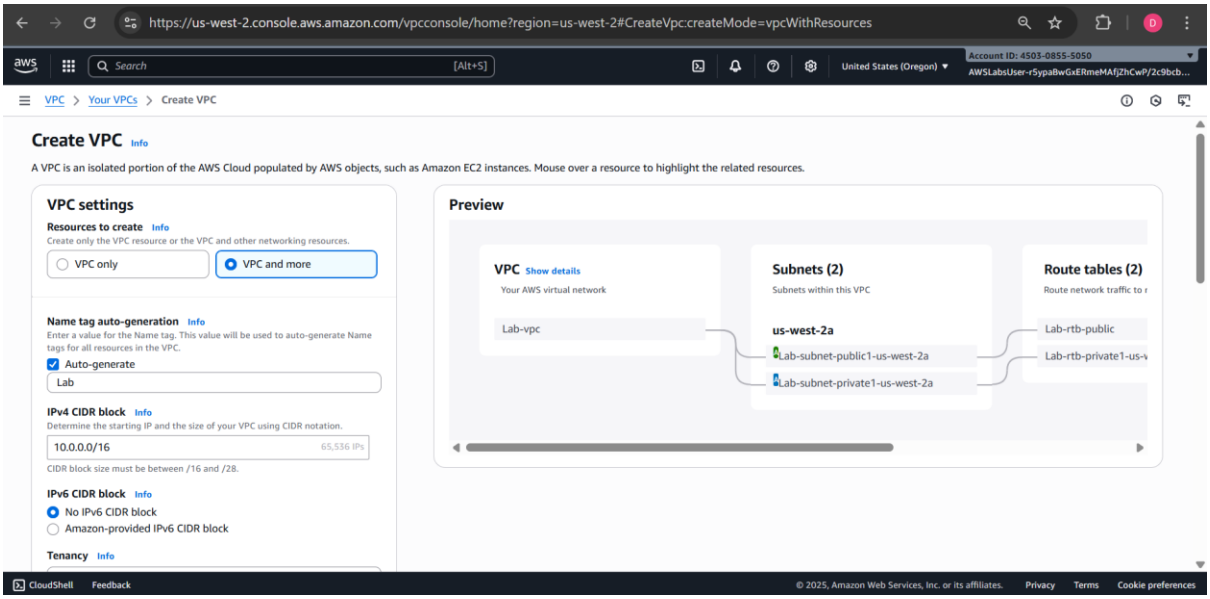
    3. For **Number of Availability Zones (AZs)**, choose **1**.
    4. For **Number of public subnets**, choose **1**.
    5. For **Number of private subnets**, choose **1**.
    6. Expand **Customize subnets CIDR blocks** and then:
        1. For **Public subnet CIDR block**, enter

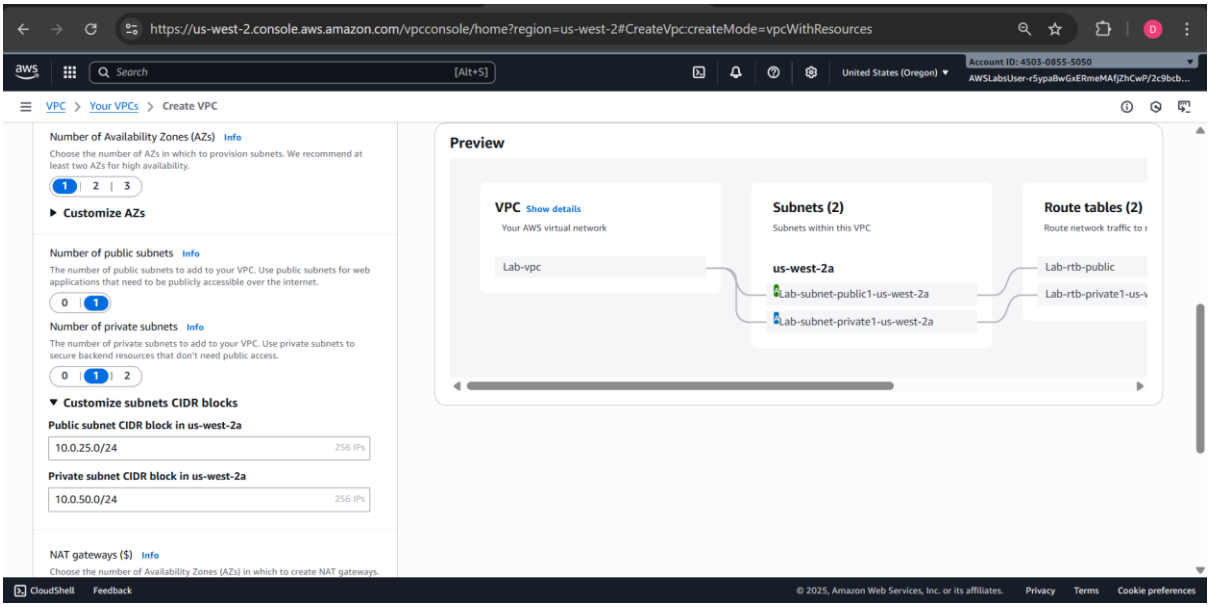
           `10.0.25.0/24`

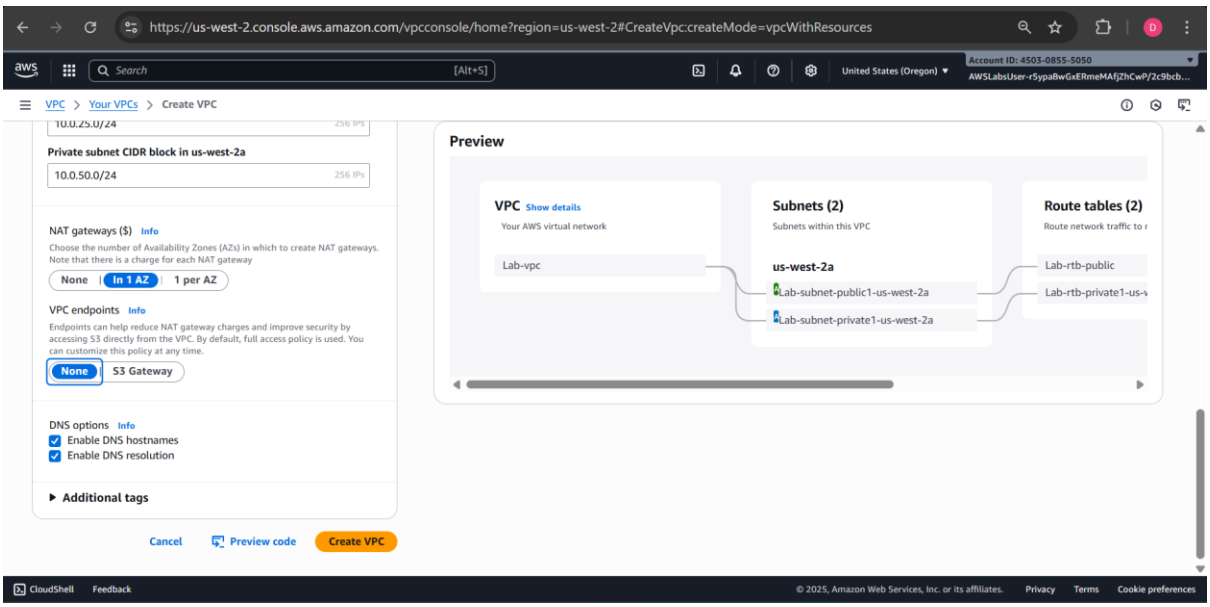
        2. For **Private subnets CIDR block**, enter

           `10.0.50.0/24`

    7. For **NAT gateways ($)**, choose **In 1 AZ**.
    8. For **VPC endpoints**, choose **None**.

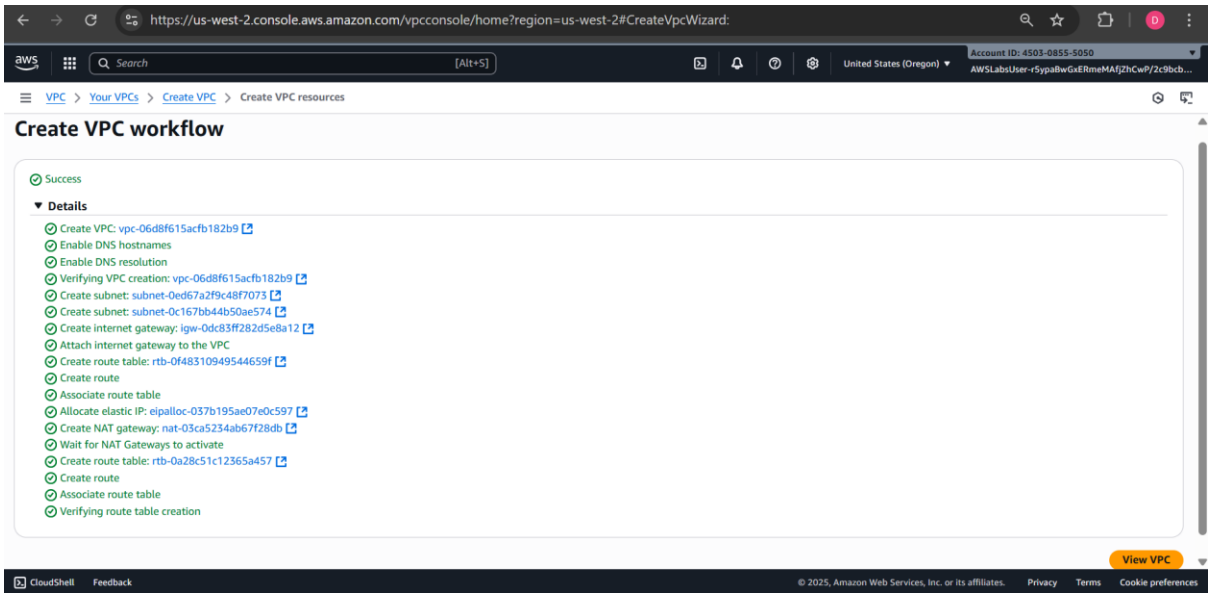

https://us-west-2.console.aws.amazon.com/vpcconsole/home?region=us-west-2#CreateVpc:createMode=vpcWithResources
Search [Alt+S]
United States (Oregon)
Account ID: 4503-0855-5050
AWSLabsUser-r5ypaBwGxERmeMAfjZhCwP/2c9bcb...
VPC > Your VPCs > Create VPC
Create VPC Info
A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.
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 auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.
Auto-generate
Lab
IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.
10.0.0.0/16
65,536 IPs
CIDR block size must be between /16 and /28.
IPv6 CIDR block Info
No IPv6 CIDR block
Amazon-provided IPv6 CIDR block
Tenancy Info
Preview
VPC Show details
Your AWS virtual network
Lab-vpc
Subnets (2)
Subnets within this VPC
us-west-2a
Lab-subnet-public1-us-west-2a
Lab-subnet-private1-us-west-2a
Route tables (2)
Route network traffic to
Lab-rtb-public
Lab-rtb-private1-us-
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences


https://us-west-2.console.aws.amazon.com/vpcconsole/home?region=us-west-2#CreateVpc:createMode=vpcWithResources
Search [Alt+S]
United States (Oregon)
Account ID: 4503-0855-5050
AWSLabsUser-r5ypaBwGxERmeMAfjZhCwP/2c9bcb...
VPC > Your VPCs > Create VPC
Number of Availability Zones (AZs) Info
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.
1 | 2 | 3
Customize AZs
Number of public subnets Info
The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.
0 | 1
Number of private subnets Info
The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.
0 | 1 | 2
Customize subnets CIDR blocks
Public subnet CIDR block in us-west-2a
10.0.25.0/24
256 IPs
Private subnet CIDR block in us-west-2a
10.0.50.0/24
256 IPs
NAT gateways ($) Info
Choose the number of Availability Zones (AZs) in which to create NAT gateways.
Preview
VPC Show details
Your AWS virtual network
Lab-vpc
Subnets (2)
Subnets within this VPC
us-west-2a
Lab-subnet-public1-us-west-2a
Lab-subnet-private1-us-west-2a
Route tables (2)
Route network traffic to
Lab-rtb-public
Lab-rtb-private1-us-
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

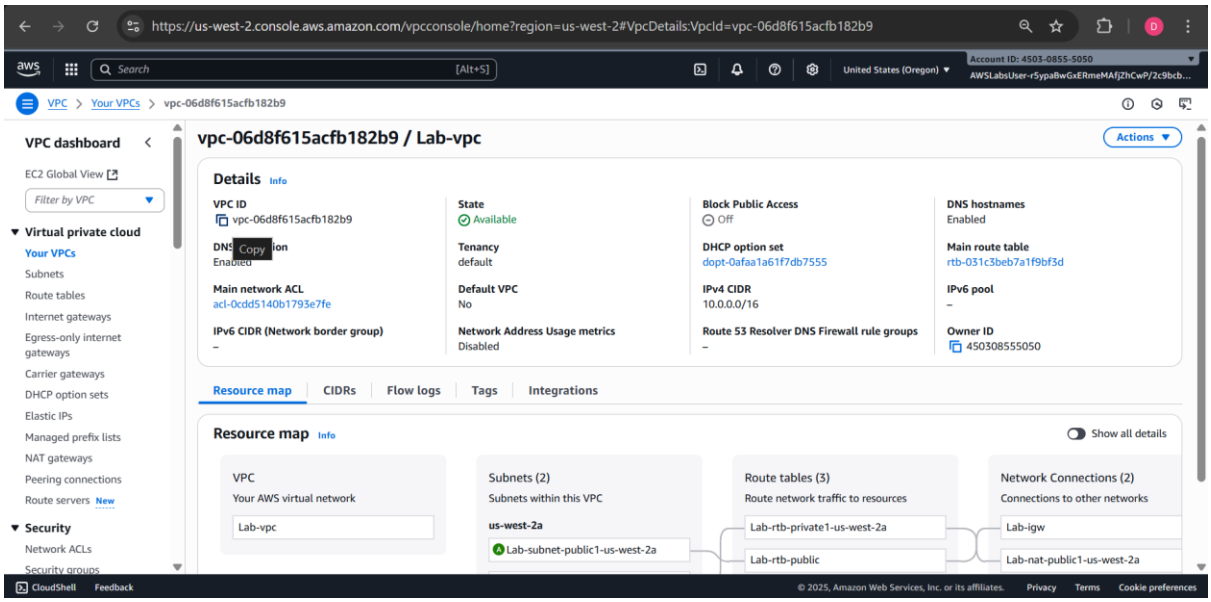

https://us-west-2.console.aws.amazon.com/vpcconsole/home?region=us-west-2#CreateVpc:createMode=vpcWithResources
Search [Alt+S]
United States (Oregon)
Account ID: 4503-0855-5050
AWSLabsUser-r5ypaBwGxERmeMAfjZhCwP/2c9bcb...
VPC > Your VPCs > Create VPC
Private subnet CIDR block in us-west-2a
10.0.50.0/24
256 IPs
NAT gateways ($) Info
Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway
None | In 1 AZ | 1 per AZ
VPC endpoints Info
Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.
None
S3 Gateway
DNS options Info
Enable DNS hostnames
Enable DNS resolution
Additional tags
Cancel
Preview code
Create VPC
Preview
VPC Show details
Your AWS virtual network
Lab-vpc
Subnets (2)
Subnets within this VPC
us-west-2a
Lab-subnet-public1-us-west-2a
Lab-subnet-private1-us-west-2a
Route tables (2)
Route network traffic to
Lab-rtb-public
Lab-rtb-private1-us-
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

6. Choose **Create VPC**.

   Your VPC is now created. A status window displays progress. When the VPC completes, a status window confirms that your VPC has been successfully created. This may take a few minutes to create.



7. Choose **View VPC**.

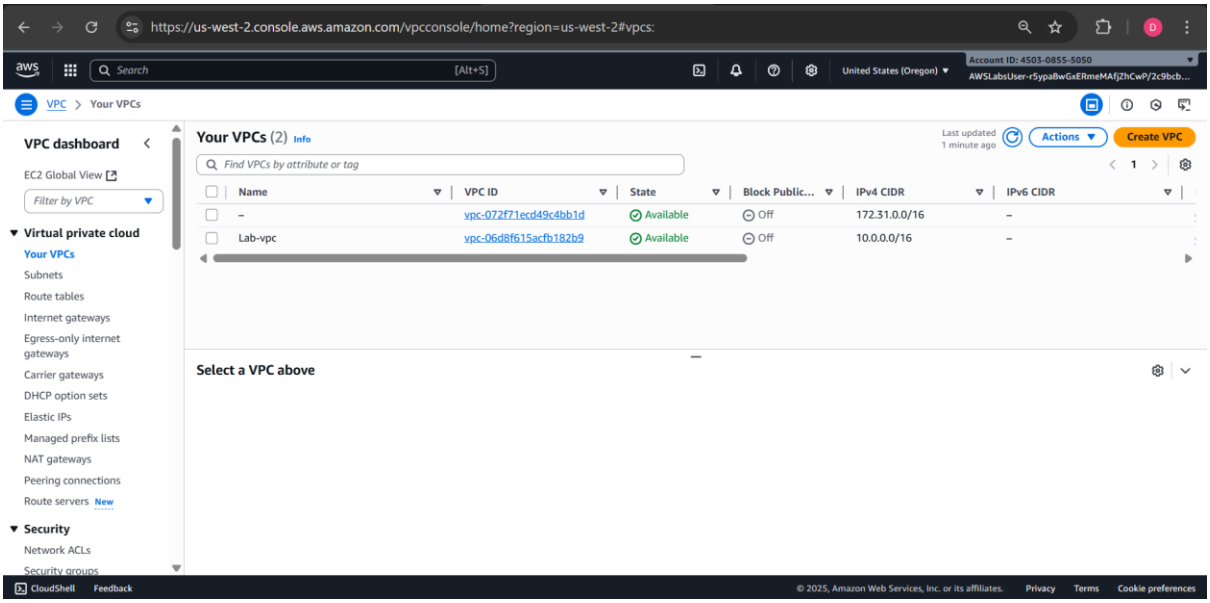


8. **Copy edit:** Copy the **VPC ID** value and paste it into your text editor to use this later in the lab.

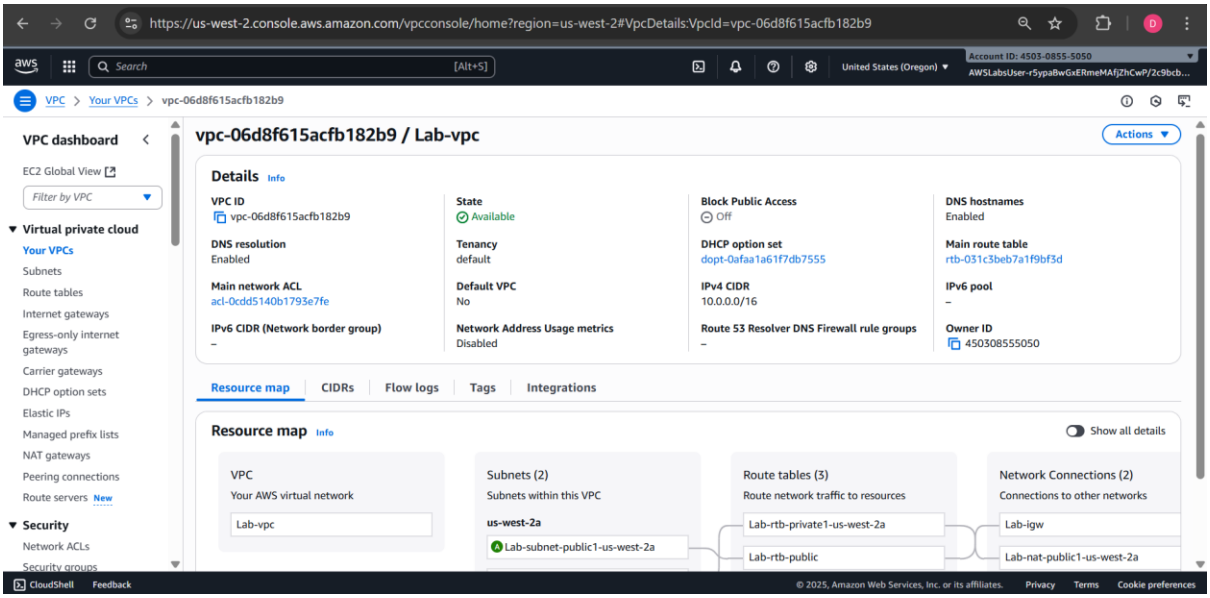
Task 2: Explore your VPC

In this task, you explore the VPC components created by the VPC Wizard.

9. In the left navigation pane, under **Virtual private cloud**, choose **Your VPCs**.



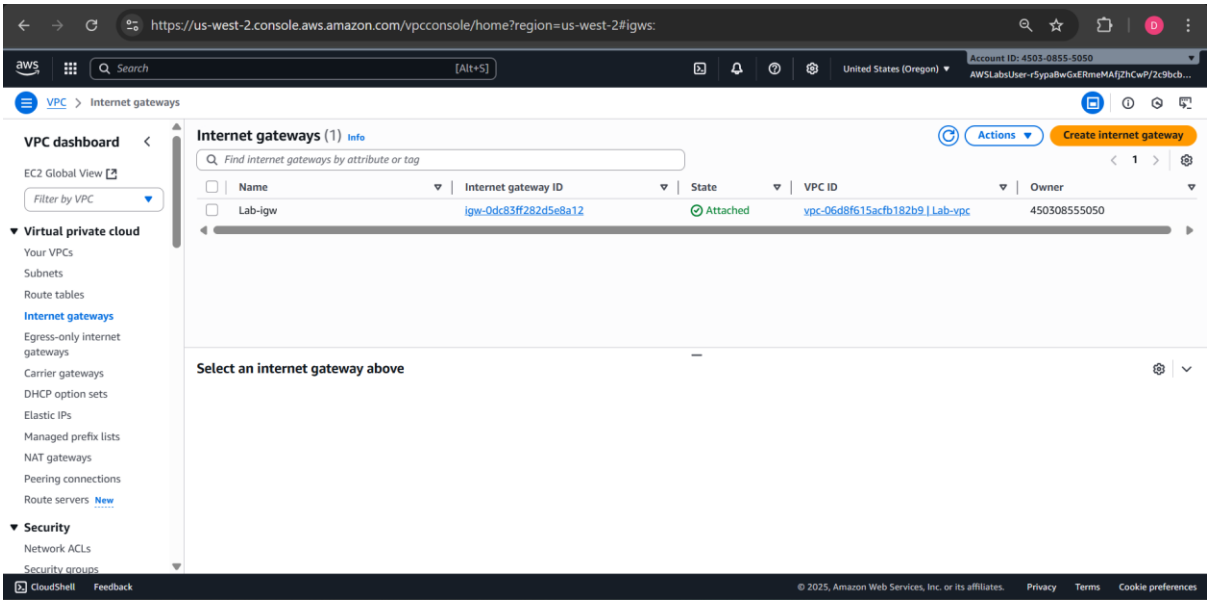
10. Locate Your VPCs's **Name** column, your VPC is created with the name **lab-vpc**.



11. In the left navigation pane, under **Virtual private cloud**, choose **Internet gateways**.

    The Internet gateway for your VPC is displayed.

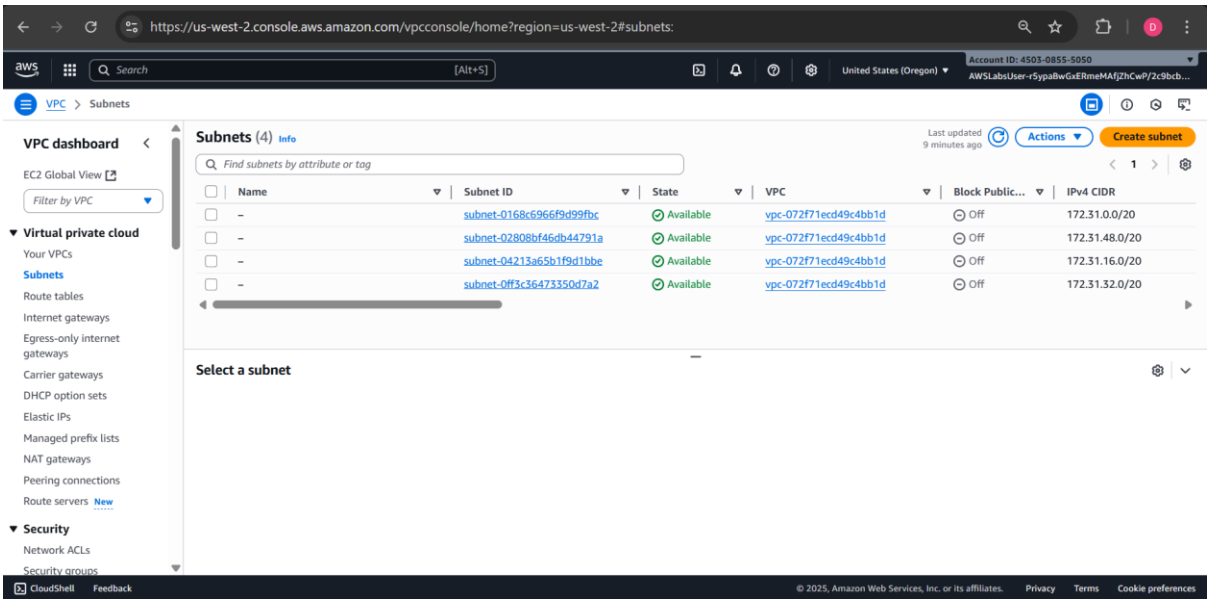
    Learn more: An Internet gateway connects your VPC to the Internet. If the Internet gateway was not present, then the VPC would have *no* connectivity to the Internet. An Internet gateway is a horizontally scaled, redundant and highly available VPC component. It therefore imposes no availability risks or bandwidth constraints on your network traffic.



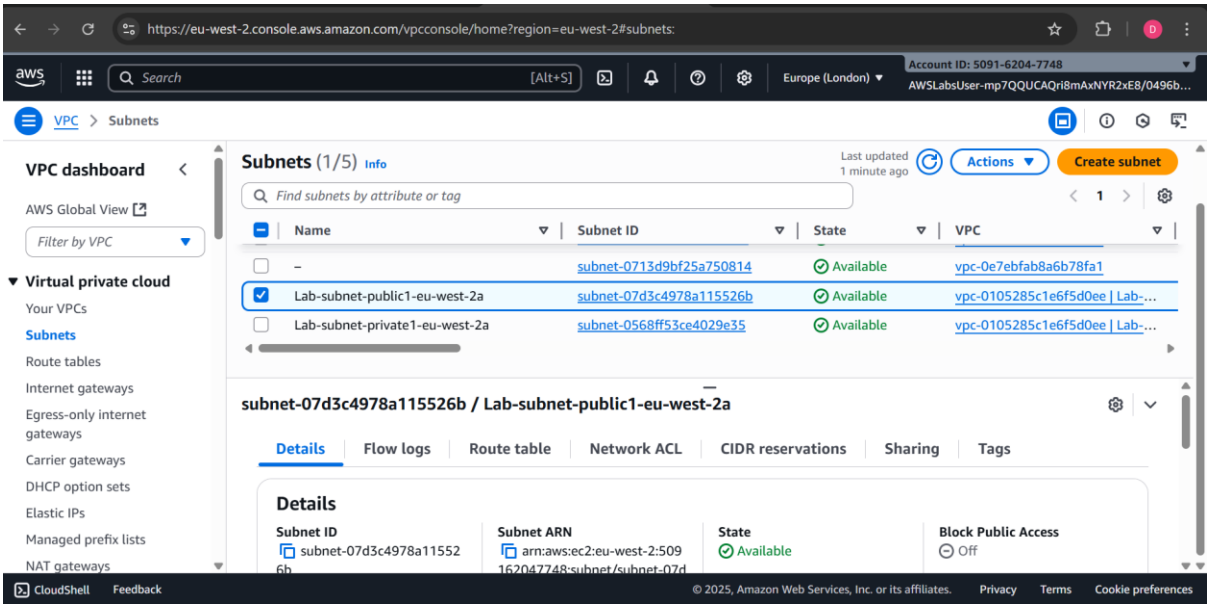
12. In the left navigation pane, under **Virtual private cloud**, choose **Subnets**.

    Learn more: A Subnet is a subset of a VPC. A subnet:

    - Belongs to a specific **VPC**
    - Exists in a single **Availability Zone** (while a VPC can span multiple Availability Zones)
    - Has a **range of IP addresses** (known as a CIDR range, which stands for Classless Inter-Domain Routing)



13. Select the **Public subnet** which starts with **Lab-subnet-public** in the **Name** column.

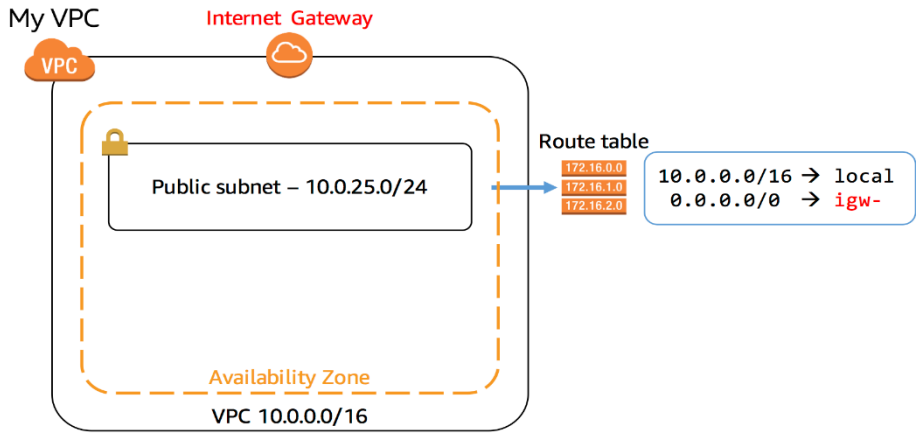


14. Examine the information displayed in the lower window pane:
    - Each subnet is assigned a unique **Subnet ID**.
    - The **IPv4 CIDR** of *10.0.25.0/24* means that the subnet contains the range of IP addresses from *10.0.25.0* to *10.0.25.255*. (IPv6 is also supported, but is not part of this lab.)
    - The subnet only has 250 **Available IPs** out of 256 possible addresses. This is because there are several reserved addresses in each subnet and one IP address has been consumed by the NAT gateway.

Consider: Why is this subnet considered to be a *Public* subnet? The answer lies in the Subnet *Routing*.

15. Choose the **Route table** tab.

Learn more: Each subnet is associated with a **Route table**, which specifies the routes for outbound traffic leaving the subnet. Think of it like an address book that lists where to direct traffic based upon its destination.



15. Choose the **Route table** tab.

Learn more: Each subnet is associated with a **Route table**, which specifies the routes for outbound traffic leaving the subnet. Think of it like an address book that lists where to direct traffic based upon its destination.

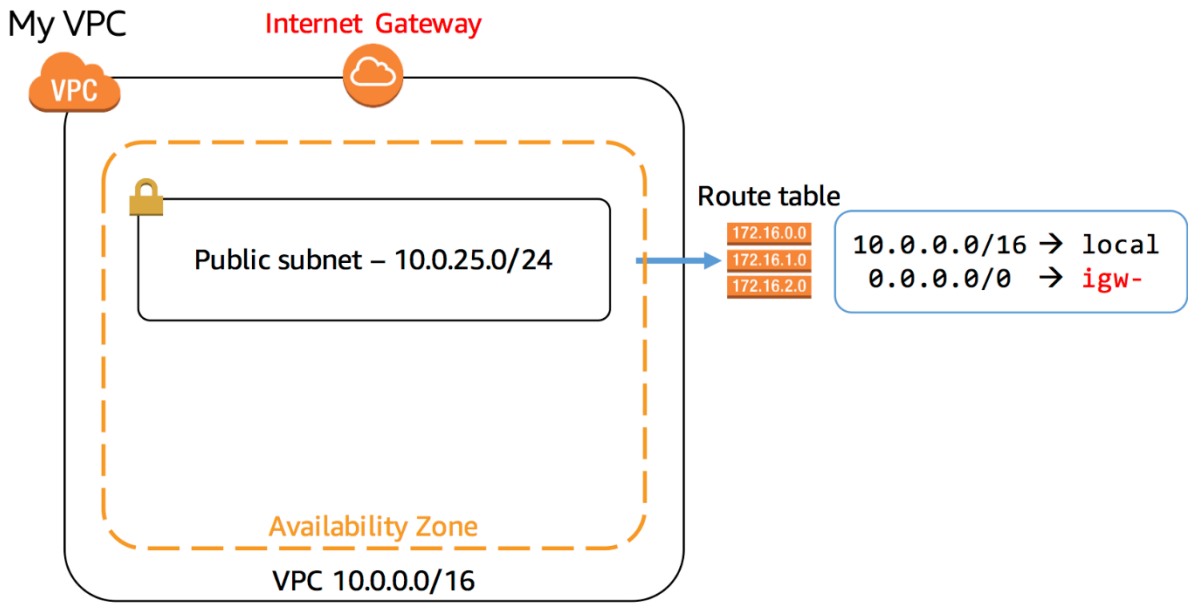
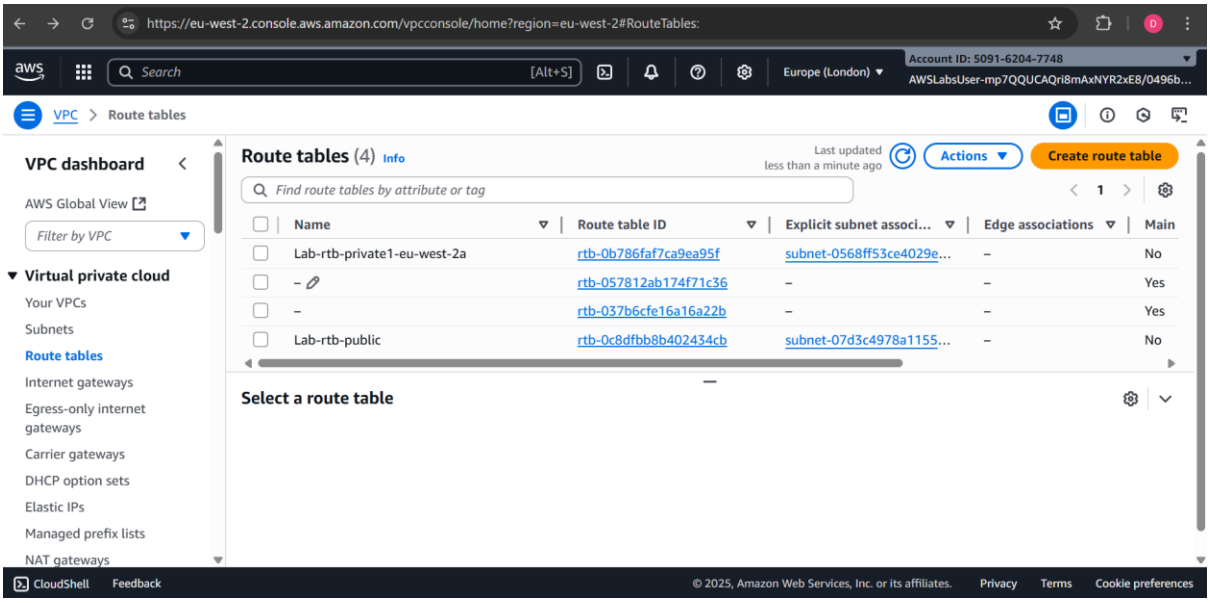


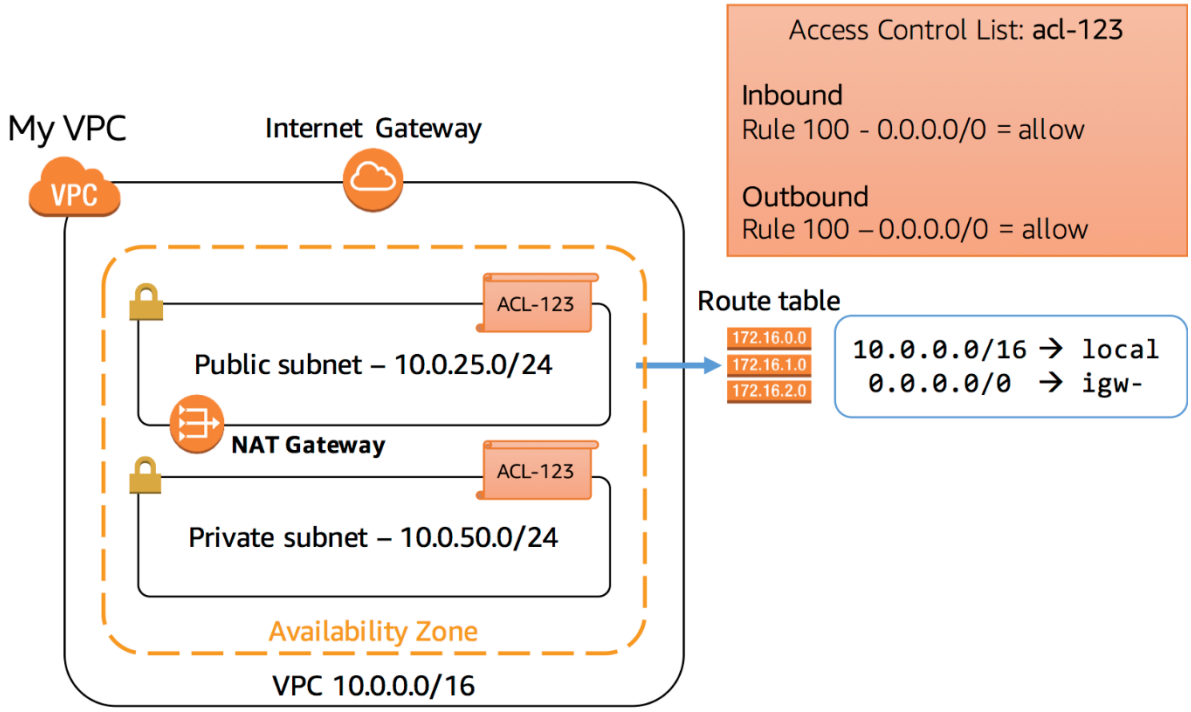
Image description: The preceding diagram depicts that the route table associated with the public subnet contains two routes. The first route is the local route (destination: 10.0.0.0/16), which allows communication within the Virtual Private Cloud (VPC) for the specified CIDR range. Traffic destined for this local route never leaves the VPC. The second route is the default route (destination: 0.0.0.0/0), which directs all IPv4 traffic destined for the internet to the Internet Gateway (IGW).

Learn more: Routing rules are evaluated from the most restrictive (with the bigger number after the slash) through to the least restrictive (which is *0.0.0.0/0* since it refers to the entire Internet). Thus, traffic is first sent within the VPC if it falls within the range of the VPC, otherwise it is send to the Internet. The rules can further be edited based upon your particular network configuration.

Note: This subnet is associated with a Route Table that has a route to an internet gateway which makes it a *Public Subnet*. This makes it reachable from the internet.



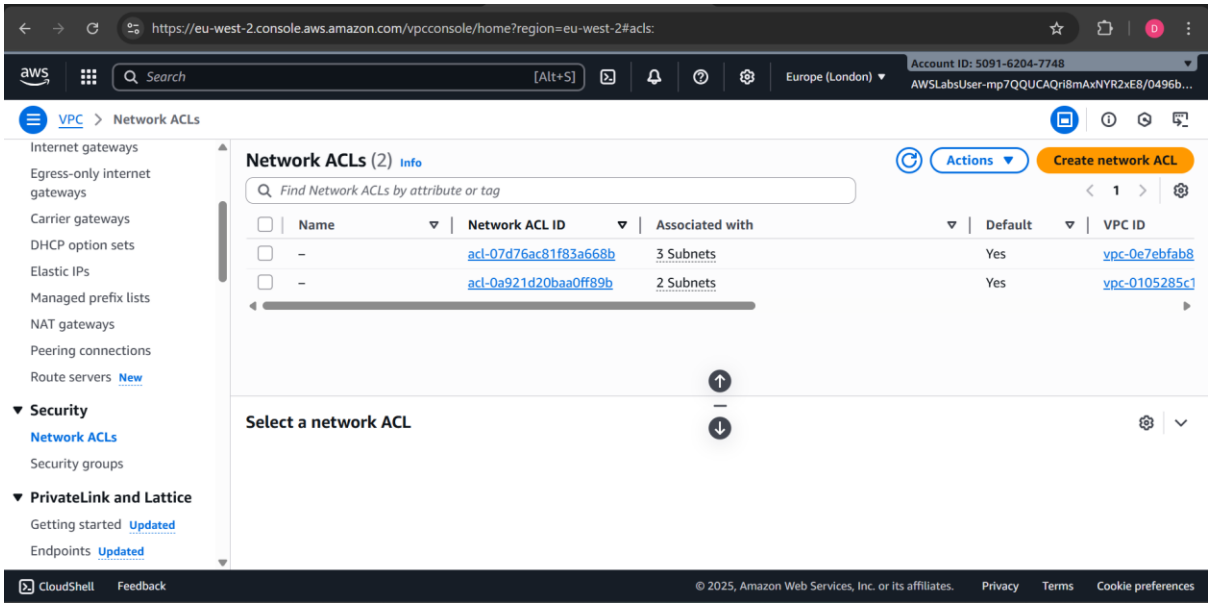
16. Choose the **Network ACL** tab.



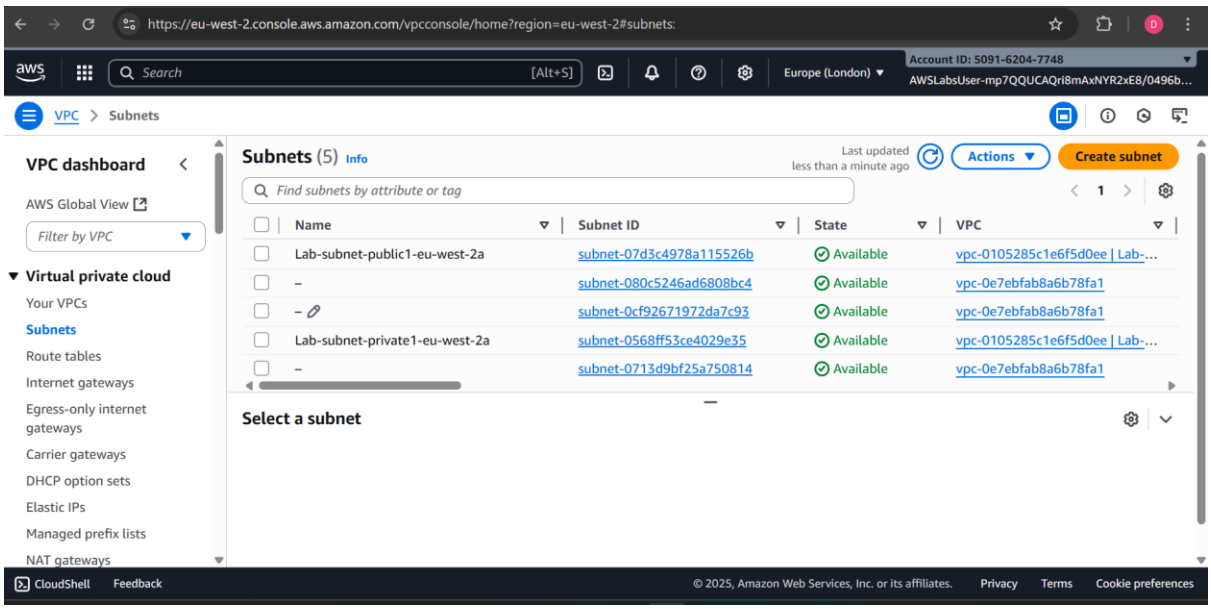
The preceding diagram depicts a Network Access Control List (ACL), which is an optional security layer for a Virtual Private Cloud (VPC) in AWS. It acts as a stateless firewall, controlling traffic in and out of subnets. The Network ACL is initially configured with default settings that allow all inbound and outbound traffic.

The following list details the rules in the diagram:

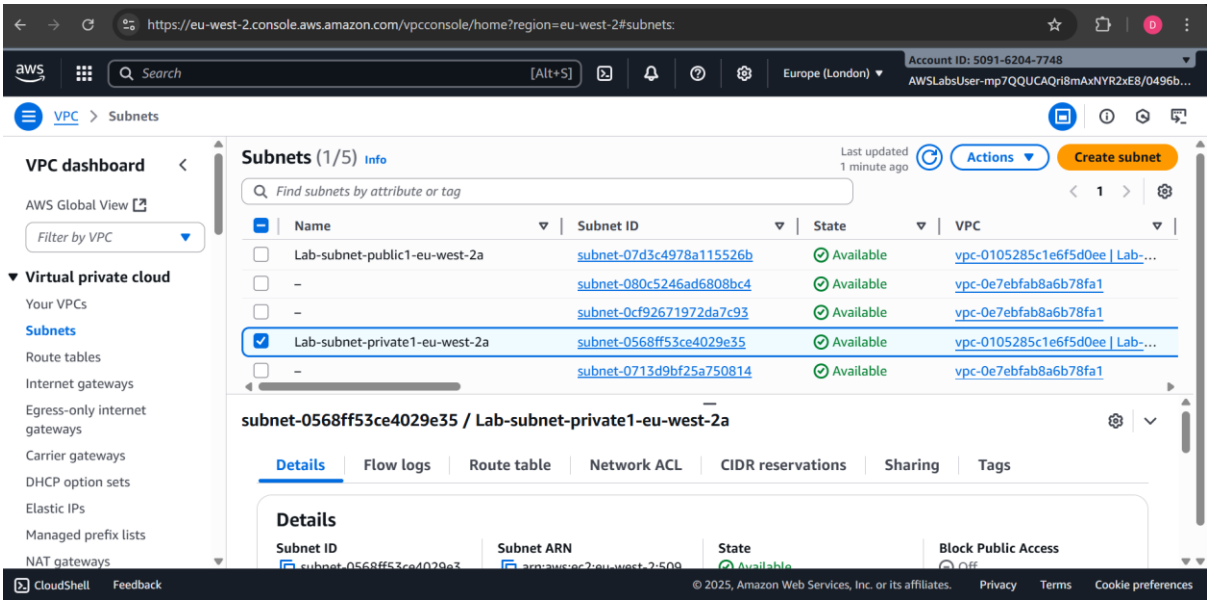
- *Rule 100 Inbound* allows all inbound traffic from any source to the public subnet.
- *Rule 100 Outbound* allows all outbound traffic from the public subnet to any destination.
- The second line in each ruleset is represented by an asterisk (*), which acts as a catch-all rule. If the incoming or outgoing traffic does not match any of the earlier rules in the Network ACL, this catch-all rule ensures that the traffic is denied by default, providing an additional layer of security.



17. In the left navigation pane, under **Virtual private cloud**, choose **Subnets**.

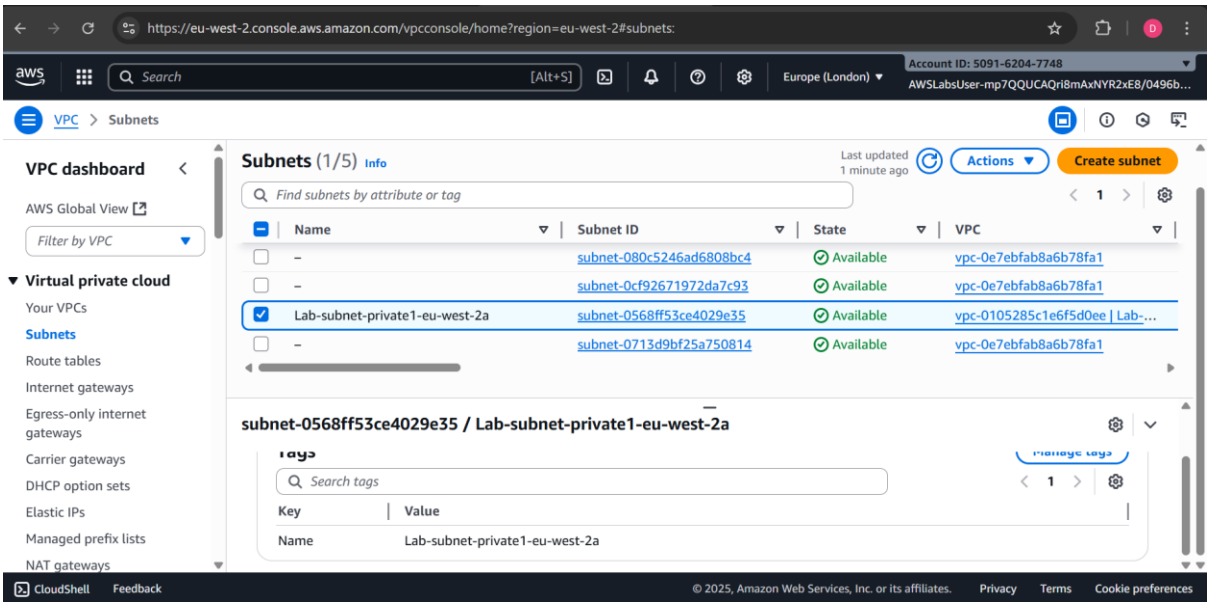


18. Select the **Private subnet** which starts with **Lab-subnet-private** in the **Name** column and ensure that it is the only line selected.



19. Choose the **Tags** tab.

Note: The subnet has been tagged with the key of **Name** starting with the value of **Lab-subnet-private**. Tags help you to manage and identify your AWS resources.



20. Choose the **Route table** tab.

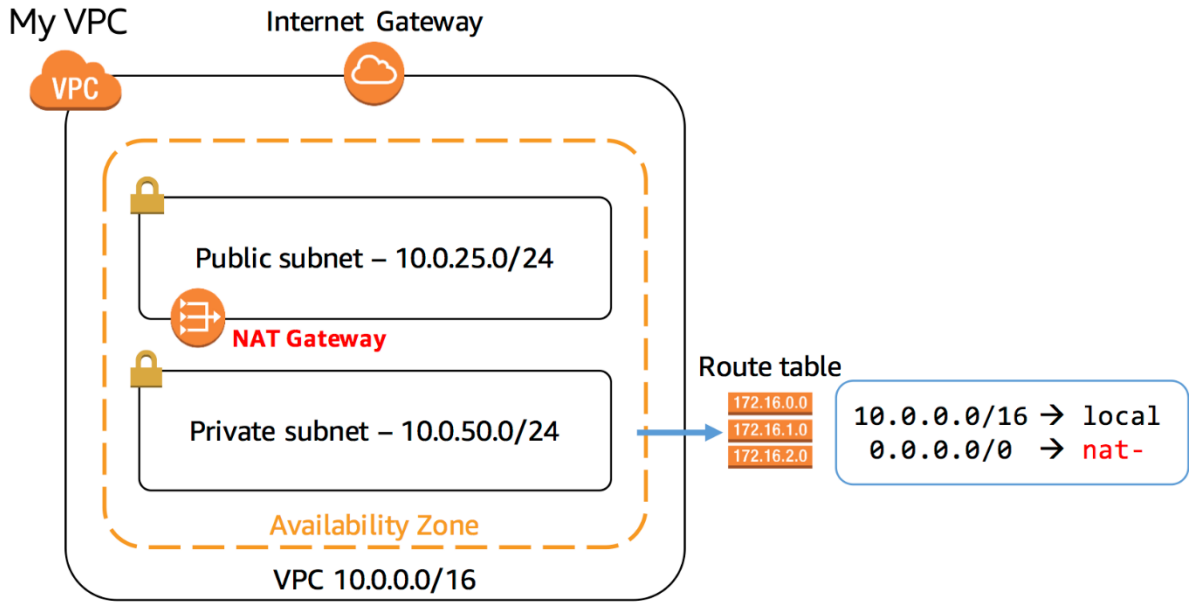
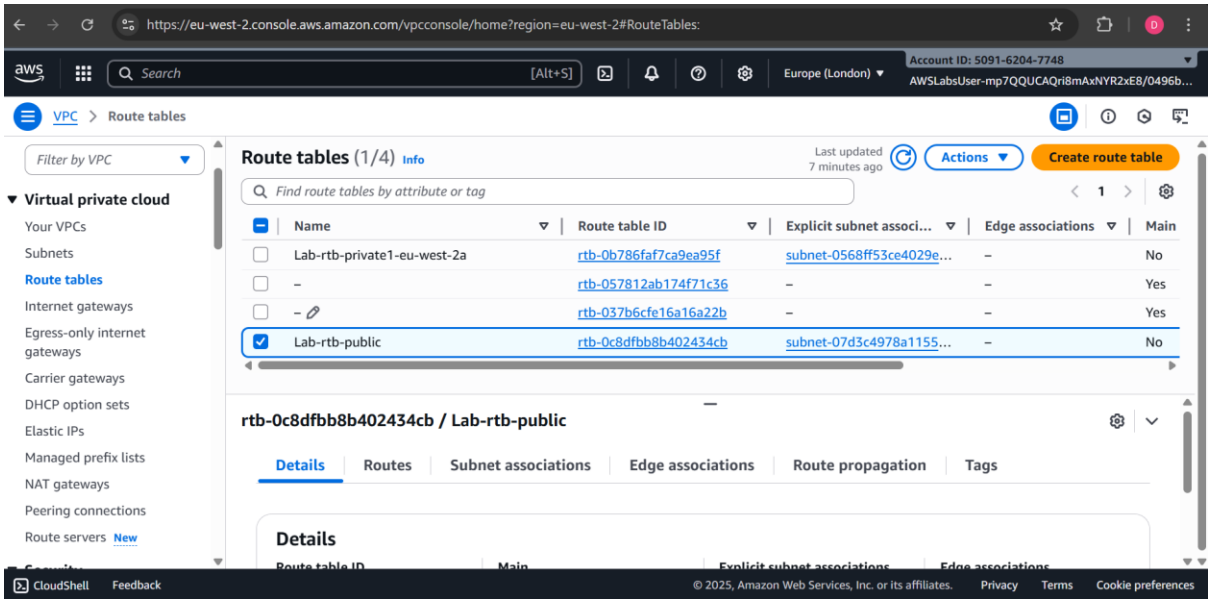


Image description: The preceding diagram depicts the route table configuration for the private subnet within the Virtual Private Cloud (VPC).

The route table contains the following two routes:

- *Route 10.0.0.0/16* | *local* is identical to the one in the public subnet's route table. It allows communication within the VPC for the specified CIDR range (10.0.0.0/16). Traffic destined for this local route never leaves the VPC.
- *Route 0.0.0.0/0* | *nat-* is the default route, directing all IPv4 traffic destined for the internet to the Network Address Translation (NAT) gateway. The NAT gateway is an AWS-managed service that enables instances in the private subnet to connect to the internet or other AWS services, but prevents the internet from initiating connections to those instances.

Note: The route table for the private subnet does not include a route to the Internet Gateway (IGW). This absence of a direct internet route is what defines this subnet as a *private subnet*. Instances in this private subnet cannot be directly accessed from the internet, providing an additional layer of security and isolation.



21. In the left navigation pane, under **Virtual private cloud**, choose **NAT gateways**.

    A NAT gateway is displayed.

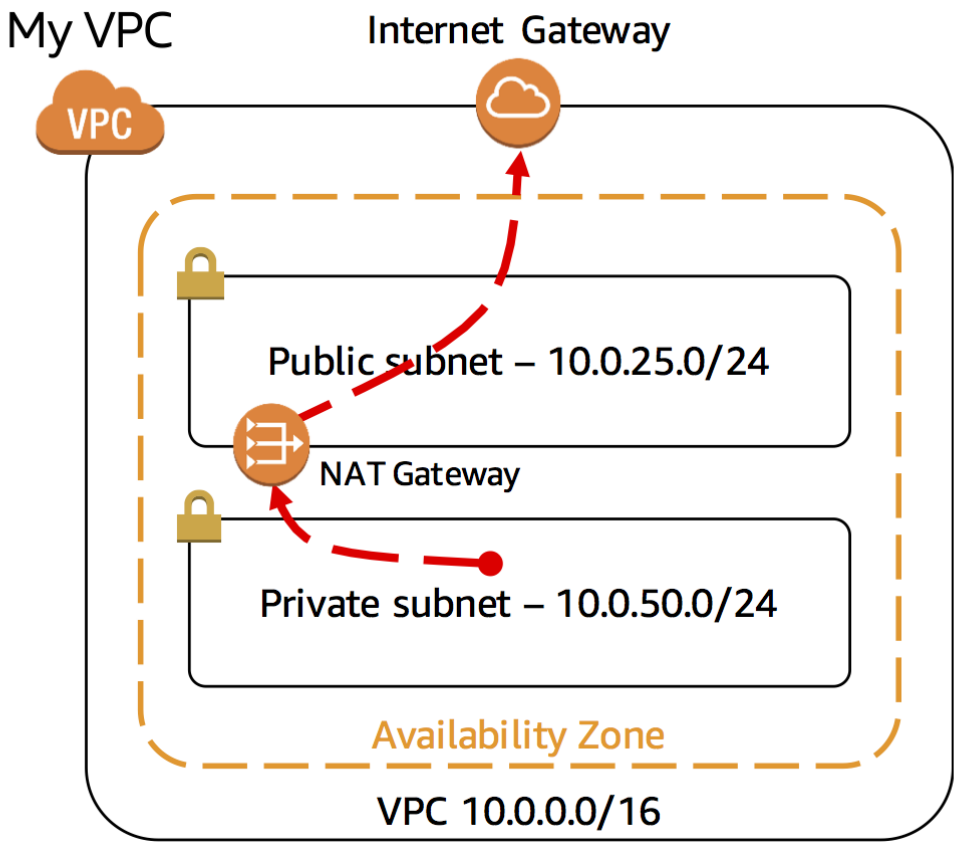


Image description: The preceding diagram depicts the resource within the private subnet initiates an outbound connection to the internet. The traffic from the private subnet is routed to the NAT gateway, as specified in the private subnet's route table. The NAT gateway then forwards the traffic to the Internet Gateway, acting as an intermediary for the communication.

Note: A Network Address Translation (NAT) gateway allows resources in a private subnet to connect to the Internet and other resources outside the VPC. This is an *outbound-only* connection, which means that the connection must be initiated from within the private subnet. Resources on the Internet cannot initiate an inbound connection. Therefore, it is a means of keeping resources private and improving security for VPC resources.

22. In the left navigation pane, under **Security**, choose **Security groups**.

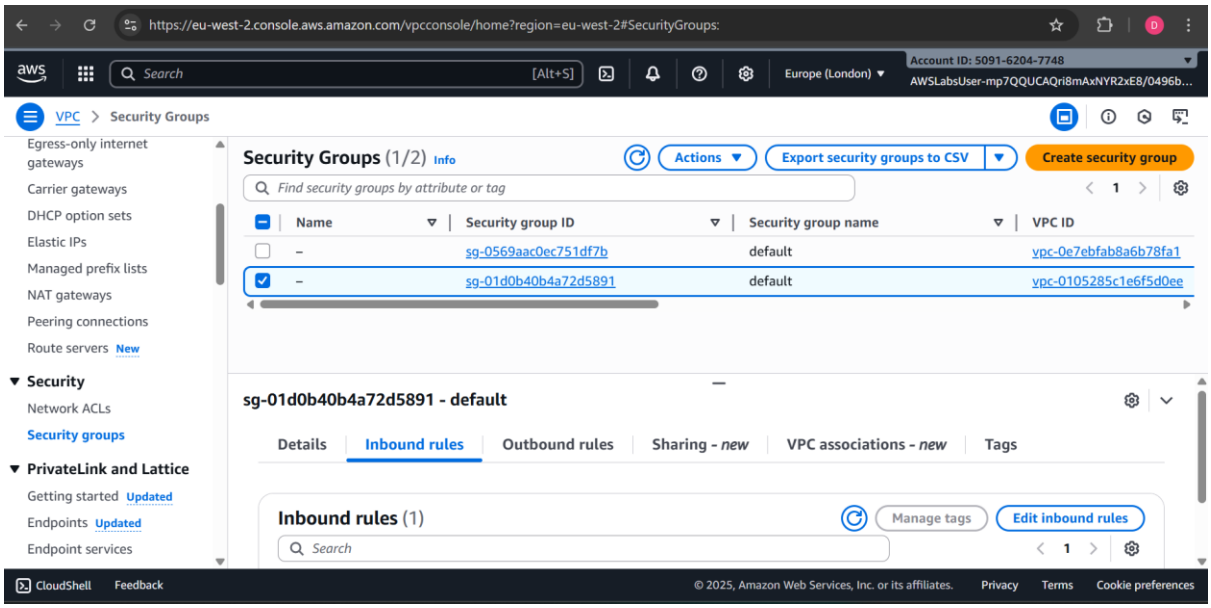
23. Select the Security group that matches with the **VPC ID** that you copied to your text editor and choose the **Inbound rules** tab.

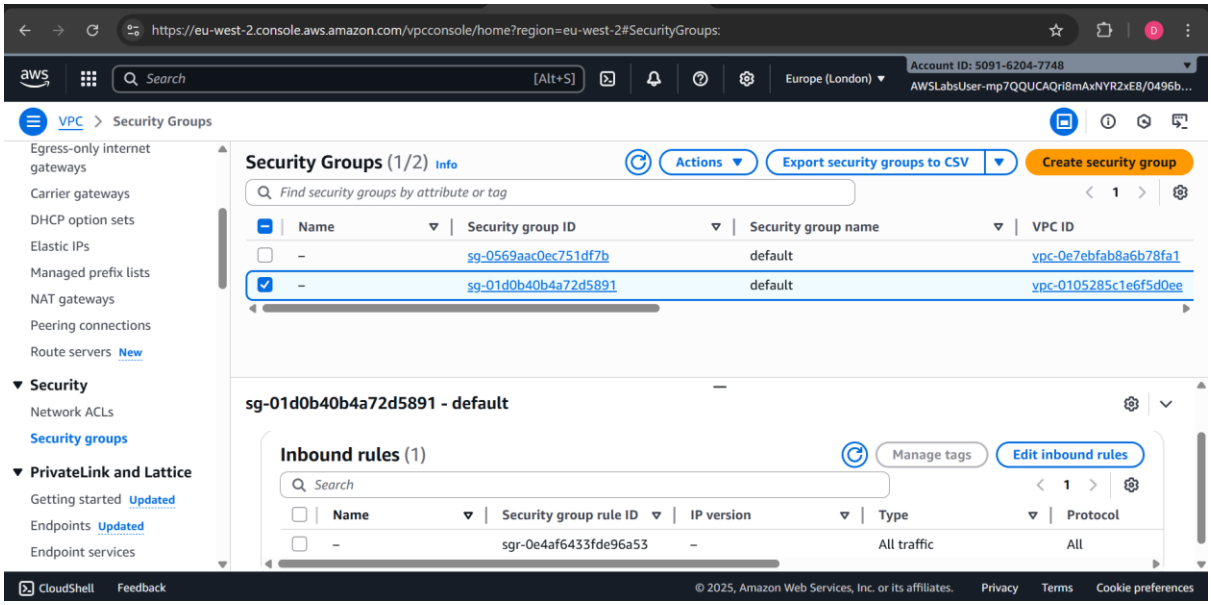
    Learn more: Security groups act as virtual firewall for your instances to control inbound and outbound traffic. When you launch an Amazon EC2 instance into a VPC, you can assign up to five security groups to the instance. Security groups act at the instance level and not the subnet level. Your VPC automatically comes with a default security group. If you do not specify a different security group when you launch an Amazon EC2 instance, it uses the default security group.

    The default security group permits *ALL traffic* to access associated resources, but only if the *Source* is the default security group. This self-reference might appear strange, but this configuration simply means that any EC2 instance associated with the default security group can communicate with any other EC2 instance that is associated with the default security group. All other traffic is denied. This is a very safe default setting because it limits any access from other resources.

    When adding resources to the VPC, you can create additional security groups to permit desired access to resources such as web servers, application servers and database servers.

    Note: Launching Amazon EC2 instances in this lab is out of the scope of the lab. Please do not attempt to launch an Amazon EC2 instance. This lab does not allow you to launch EC2 instances.





You have successfully explored the VPC components created by the *VPC Wizard*.

Conclusion

You successfully did the following:

- Created an Amazon VPC Using the **VPC Wizard**.
- Explored the basic components of a VPC.

End lab

Follow these steps to close the console and end your lab.

24. Return to the **AWS Management Console**.

25. At the upper-right corner of the page, choose **AWSLabsUser**, and then choose **Sign out**.

26. Choose **End Lab** and then confirm that you want to end your lab.