



AWS
re:Start
LAB

Configuring an Amazon VPC



WEEK 10





Overview

Amazon Virtual Private Cloud (Amazon VPC) gives you the ability to 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 selecting your IP address ranges, creating subnets, and configuring route tables and network gateways.

Configuring an Amazon VPC involves setting up a secure and customizable network environment tailored to your specific requirements. This process includes defining subnets within your IP address range, associating route tables to manage traffic flow, and establishing network gateways to enable communication between your VPC and the internet or other networks. Additionally, you can implement security groups and network ACLs to control inbound and outbound traffic at the instance and subnet level, ensuring robust protection and efficient traffic management within your VPC.

Topics covered

- Create a VPC with a private and public subnet, an internet gateway, and a NAT gateway.
- Configure route tables associated with subnets to local and internet-bound traffic by using an internet gateway and a NAT gateway.
- Launch a bastion server in a public subnet.
- Use a bastion server to log in to an instance in a private subnet.

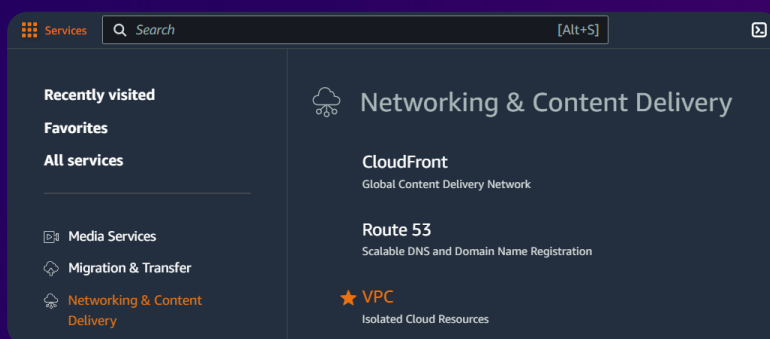


Task 1

Creating a VPC

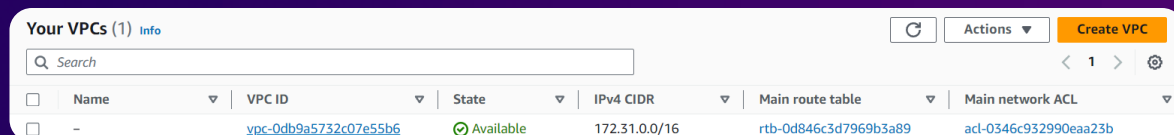
Step 1: Access the AWS Management Console

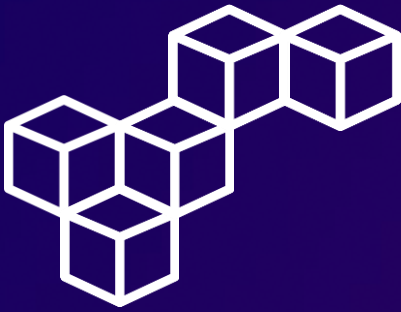
Open the AWS Management Console, and select VPC.



Step 2: Create VPC

Navigate to the **Your VPCs** section, and select [Create VPC](#).





Task 1

Creating a VPC

Step 3: VPC settings

In the **VPC settings** section, configure the following settings.

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.

Lab VPC

IPv4 CIDR block [Info](#)
☒ IPv4 CIDR manual input

IPv4 CIDR
10.0.0.0/16

IPv6 CIDR block [Info](#)
☒ No IPv6 CIDR block

Step 4: Edit DNS settings

Select the newly created **Lab VPC**, and choose [Edit VPC settings](#). In the **DNS settings** section, select [Enable DNS hostnames](#).

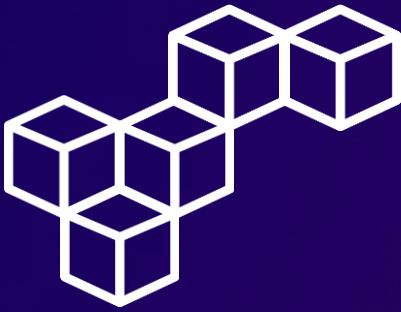
Your VPCs (1/2) [Info](#)

	Name	VPC ID	State	IPv4 CIDR	Main route table
<input type="checkbox"/>	-	vpc-0db9a5732c07e55b6	Available	172.31.0.0/16	rtb-0d846c3d7969b3a89
<input checked="" type="checkbox"/>	Lab VPC	vpc-0bc64cbec9ceea67a	Available	10.0.0.0/16	-

Actions
Create default VPC
Create flow log
Edit VPC settings
Edit CIDRs
Manage tags
Delete VPC

DNS settings

- ☒ Enable DNS resolution [Info](#)
- ☒ Enable DNS hostnames [Info](#)



Task 2

Creating subnets

Step 1: Create Public subnet

Navigate to the **Subnets** section, and select [Create subnet](#).

Subnets (4) Info							
<input type="text" value="Find resources by attribute or tag"/>							
<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	Availability Zone	
<input type="checkbox"/>	-	subnet-05badabebcff3fcf2	Available	vpc-0db9a5732c07e55b6	172.31.0.0/20	us-west-2c	
<input type="checkbox"/>	-	subnet-0f1456992857ca786	Available	vpc-0db9a5732c07e55b6	172.31.32.0/20	us-west-2a	
<input type="checkbox"/>	-	subnet-089e24a2f70b7c888	Available	vpc-0db9a5732c07e55b6	172.31.48.0/20	us-west-2d	
<input type="checkbox"/>	-	subnet-00e359721f3df28b3	Available	vpc-0db9a5732c07e55b6	172.31.16.0/20	us-west-2b	

Step 2: Public Subnet settings

In the **Create subnet** page, configure the following settings.

VPC

VPC ID
Create subnets in this VPC.

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

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

Availability Zone [Info](#)
Choose the zone in which your subnet will reside.

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.

IPv4 subnet CIDR block

256 IPs



Task 2

Creating subnets

Step 3: Edit Auto-assign IP settings

Select the newly created **Public Subnet**, and choose [Edit subnet settings](#). In the **Auto-assign IP settings** section, select [Enable auto-assign public IPv4 address](#).

Subnets (1/5) Info

Find resources by attribute or tag

	Name	Subnet ID	State	VPC	IPv4 CIDR
<input checked="" type="checkbox"/>	Public Subnet	subnet-04573ac718c3d995f	Available	vpc-0bc64cbec9ceea67a Lab VPC	10.0.0.0/24

Actions

Create subnet

View details

Create flow log

Edit subnet settings

Auto-assign IP settings [Info](#)

Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet.

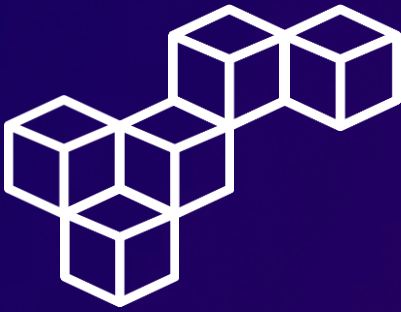
☒ [Enable auto-assign public IPv4 address](#) [Info](#)

☐ [Enable auto-assign customer-owned IPv4 address](#) [Info](#)
Option disabled because no customer owned pools found.

Step 4: Create Private subnet

Navigate to the **Subnets** section, and select [Create subnet](#).

Subnets (5) Info							Actions Create subnet	
<input type="text" value="Find resources by attribute or tag"/>								1
<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	Availability Zone		
<input type="checkbox"/>	Public Subnet	subnet-04573ac718c3d995f	Available	vpc-0bc64cbec9ceea67a Lab VPC	10.0.0.0/24	us-west-2a		



Task 2

Creating subnets

Step 5: Private Subnet settings

In the **Create subnet** page, configure the following settings.

VPC

VPC ID

Create subnets in this VPC.

vpc-0bc64cbec9ceea67a (Lab VPC)

Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet name

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

Private Subnet

Availability Zone

[Info](#)

Choose the zone in which your subnet will reside.

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.

10.0.0.0/16

IPv4 subnet CIDR block

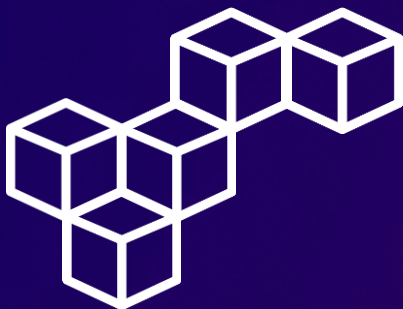
10.0.2.0/23

512 IPs

Step 6: Review Subnets creation

In the **Subnets** section, review the **Available** State of the newly created subnets **Public Subnet** and **Private Subnet**.

Subnets (6) Info								Refresh Actions		Create subnet
<input type="text" value="Find resources by attribute or tag"/>								< 1 > Settings		
<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	Availability Zone				
<input type="checkbox"/>	Public Subnet	subnet-04573ac718c3d995f	Available	vpc-0bc64cbec9ceea67a Lab VPC	10.0.0.0/24	us-west-2a				
<input type="checkbox"/>	Private Subnet	subnet-03241a35161803a92	Available	vpc-0bc64cbec9ceea67a Lab VPC	10.0.2.0/23	us-west-2a				



Task 3

Creating an internet gateway

Step 1: Create internet gateway

Navigate to the **Internet gateways** section, and select [Create internet gateway](#).

Internet gateways (1) Info					Refresh	Actions ▼	Create internet gateway
<input type="text" value="Search"/>					< 1 > ⓘ		
<input type="checkbox"/>	Name ▼	Internet gateway ID ▼	State ▼	VPC ID ▼			
<input type="checkbox"/>	-	igw-0c45264a06d13a5d0	✔ Attached	vpc-0db9a5732c07e55b6			

Step 2: Internet gateway settings

In the **Internet gateway settings** section, for the Name tag, enter [Lab IGW](#).

Internet gateway settings

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



Task 3

Creating an internet gateway

Step 3: Attach to VPC

Select the newly created **Lab IGW**, and choose [Attach to VPC](#).

Internet gateways (1/2) Info

<input type="checkbox"/>	Name	Internet gateway ID	State	VPC ID
<input type="checkbox"/>	-	igw-0c45264a06d13a5d0	Attached	vpc-0db9a573
<input checked="" type="checkbox"/>	Lab IGW	igw-027212748a46d37d2	Detached	-

Actions

Create internet gateway

View details

Attach to VPC

Detach from VPC

Manage tags

Delete internet gateway

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.

Step 4: Review Attachment

In the **Internet gateways** section, review the **Lab IGW** attachment to the **Lab VPC**.

Internet gateways (2) Info

<input type="checkbox"/>	Name	Internet gateway ID	State	VPC ID
<input type="checkbox"/>	-	igw-0c45264a06d13a5d0	Attached	vpc-0db9a5732c07e55b6
<input type="checkbox"/>	Lab IGW	igw-027212748a46d37d2	Attached	vpc-0bc64cbec9ceea67a Lab VPC

Actions

Create internet gateway



Task 4

Configuring route tables

Step 1: Edit Route Table Name

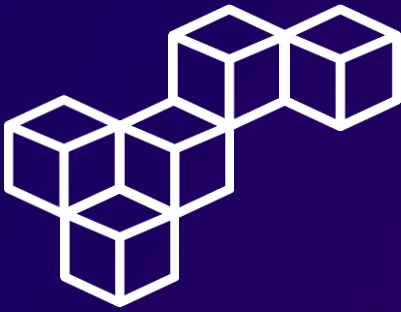
Navigate to the **Route tables** section, select the route table that includes Lab VPC in the VPC column. In the Name column, choose the edit icon, and enter **Private Route Table**.

Route tables (1/2) Info					Refresh	Actions ▼	Create route table
<input type="text" value="Find resources by attribute or tag"/>					< 1 > Filter		
<input type="checkbox"/>	Name ▼	Route table ID ▼	Explicit subnet associations ▼	VPC ▼			
<input type="checkbox"/>	-	rtb-0d846c3d7969b3a89	-	vpc-0db9a5732c07e55b6			
<input checked="" type="checkbox"/>	Private Route Table ✎	rtb-0b9ffdb8a82e57626	-	vpc-0bc64cbec9ceea67a Lab VPC			

Step 2: Review routes

Select the **Private Route Table**, and choose the **Routes** tab. There is currently only one route. It shows that all traffic destined for 10.0.0.0/16 (which is the range of the Lab VPC) will be routed locally. This option allows all subnets within a VPC to communicate with each other.

Routes (1)				Both ▼	Edit routes
<input type="text" value="Filter routes"/>				< 1 > Filter	
Destination ▼	Target ▼	Status ▼	Propagated ▼		
10.0.0.0/16	local	Active	No		



Task 4

Configuring route tables

Step 3: Create Public Route Table

In the **Route tables** section, select [Create route table](#).

Route tables (2) Info					Refresh	Actions ▼	Create route table
<input type="text" value="Find resources by attribute or tag"/>					< 1 > ⚙		
<input type="checkbox"/>	Name ▼	Route table ID ▼	Explicit subnet associations ▼	VPC ▼			
<input type="checkbox"/>	-	rtb-0d846c3d7969b3a89	-	vpc-0db9a5732c07e55b6			
<input type="checkbox"/>	Private Route Table	rtb-0b9ffdb8a82e57626	-	vpc-0bc64cbec9ceea67a Lab VPC			

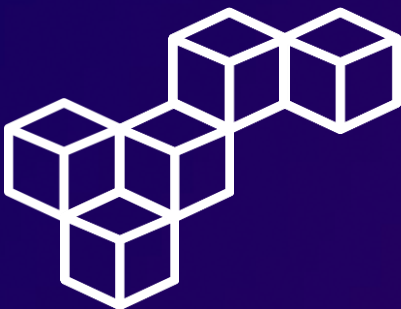
Step 4: Public Route table settings

In the **Route table settings** section, configure the following settings.

Route table settings

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

VPC
The VPC to use for this route table.



Task 4

Configuring route tables

Step 5: Edit routes

Select the **Public Route Table**, choose the **Routes** tab, and select [Edit routes](#).

Routes (1)				Both ▼	Edit routes
<input type="text" value="Filter routes"/>				< 1 >	⚙
Destination	Target	Status	Propagated		
10.0.0.0/16	local	Active	No		

Step 6: Add route

Add a route to direct internet-bound traffic (0.0.0.0/0) to the **Lab IGW** internet gateway.

Routes (2)				Both ▼	Edit routes
<input type="text" value="Filter routes"/>				< 1 >	⚙
Destination	Target	Status	Propagated		
0.0.0.0/0	igw-027212748a46d37d2	Active	No		
10.0.0.0/16	local	Active	No		

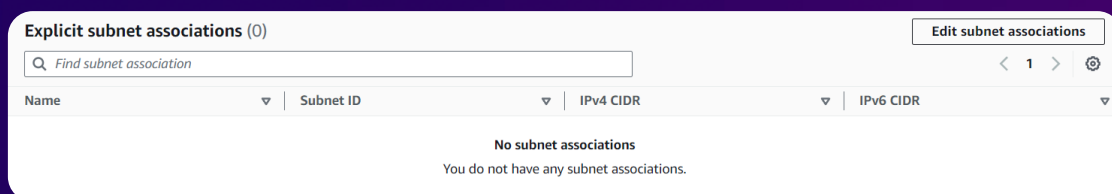


Task 4

Configuring route tables

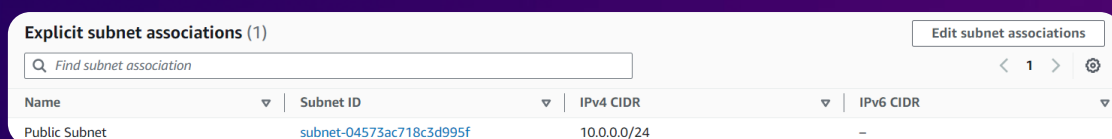
Step 7: Edit subnet associations

Choose the **Subnet associations** tab, and select [Edit subnet associations](#), and select the **Public Subnet**.



Step 8: Review Explicit subnet associations

Review the **Public Route Table Explicit subnet associations**. The **Public Subnet** is now public because it has a route table entry that sends traffic to the internet through the internet gateway.



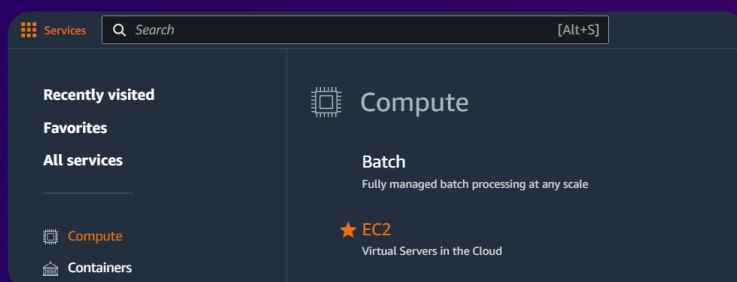


Task 5

Launching a bastion server in the public subnet

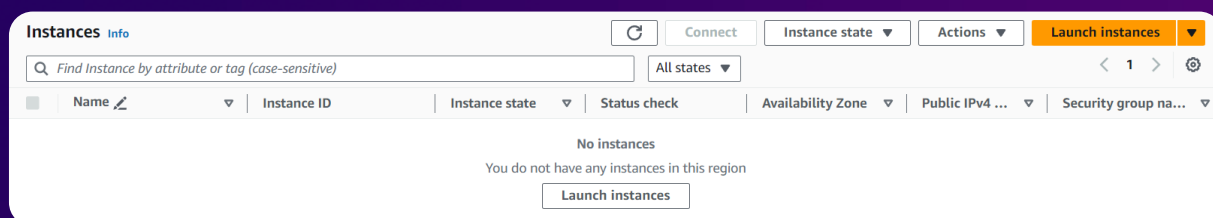
Step 1: Access the EC2 Management Console

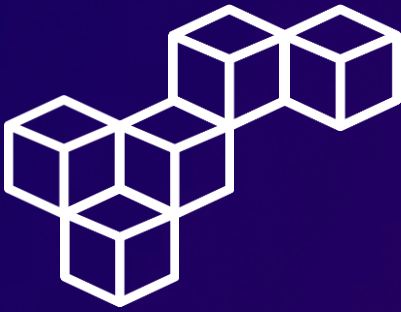
In the AWS Management Console, select EC2.



Step 2: Launch the Bastion Server

Navigate to the **Instances** section, and select [Launch instances](#).





Task 5

Launching a bastion server in the public subnet

Step 3: Set up the instance

Use the following parameters to configure the instance settings.

Name and tags [Info](#)

Name

Bastion Server

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI Free tier eligible

ami-0eb9d67c52f5c80e5 (64-bit (x86), uefi-preferred) / ami-0faea24786f93f390 (64-bit (Arm), uefi)

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 AMI 2023.4.20240528.0 x86_64 HVM kernel-6.1

Architecture

64-bit (x86)

Boot mode

uefi-preferred

AMI ID

ami-0eb9d67c52f5c80e5 Verified provider

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

Instance type

t3.micro

Family: t3 2 vCPU 1 GiB Memory Current generation: true

On-Demand SUSE base pricing: 0.0104 USD per Hour

On-Demand Windows base pricing: 0.0196 USD per Hour

On-Demand RHEL base pricing: 0.0704 USD per Hour

On-Demand Linux base pricing: 0.0104 USD per Hour

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

Proceed without a key pair (Not recommended) Default value

[Create new key pair](#)

Network settings [Info](#)

VPC - required [Info](#)

vpc-0bc64cbec9ceea67a (Lab VPC)

10.0.0.0/16

Subnet [Info](#)

subnet-04573ac718c3d995f Public Subnet

VPC: vpc-0bc64cbec9ceea67a Owner: 654654284832

Availability Zone: us-west-2a IP addresses available: 251 CIDR: 10.0.0.0/24

Auto-assign public IP [Info](#)

Enable

Firewall (security groups) [Info](#)

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

☒ Create security group ☐ Select existing security group

Security group name - required

Bastion Security Group

This security group will be added to all network interfaces.

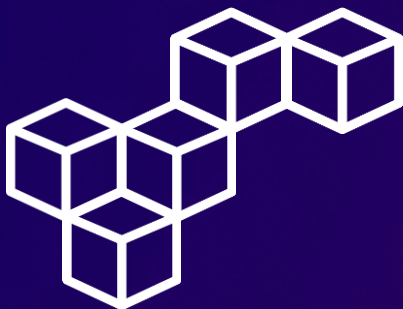
Description - required [Info](#)

Allow SSH

Inbound Security Group Rules

Type [Info](#) Source type [Info](#)

ssh Anywhere

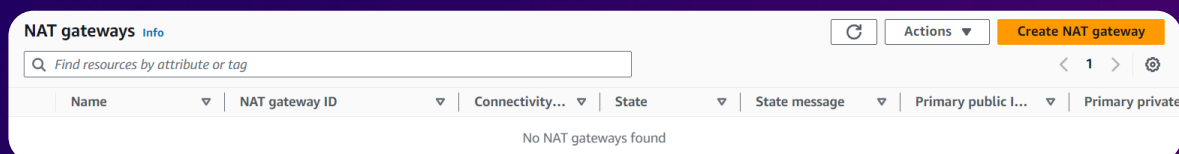


Task 6

Creating a NAT gateway

Step 1: Create NAT gateway

Navigate to the **NAT gateways** section, and select [Create NAT gateway](#).



Step 2: NAT gateway settings

In the **NAT gateway settings** section, configure the following settings.

NAT gateway settings

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

Subnet
Select a subnet in which to create the NAT gateway.

Elastic IP allocation ID [info](#)
Assign an Elastic IP address to the NAT gateway.



Task 6

Creating a NAT gateway

Step 3: Edit routes

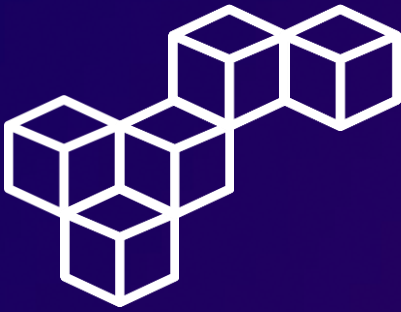
Select the **Private Route Table**, choose the **Routes** tab, and select [Edit routes](#).

Routes (1)				Both ▼	Edit routes
<input type="text" value="Filter routes"/>				< 1 >	⚙
Destination	Target	Status	Propagated		
10.0.0.0/16	local	Active	No		

Step 4: Add route

Add a route to direct internet-bound traffic (0.0.0.0/0) to the **Lab NAT gateway**. Resources in the private subnet that wish to communicate with the internet now have their network traffic directed to the NAT gateway, which forwards the request to the internet. Responses flow through the NAT gateway back to the private subnet.

Routes (2)				Both ▼	Edit routes
<input type="text" value="Filter routes"/>				< 1 >	⚙
Destination	Target	Status	Propagated		
0.0.0.0/0	nat-02583e8727cfa2077	Active	No		
10.0.0.0/16	local	Active	No		



Task 7

Optional challenge: Testing the private subnet

Step 1: Launch the Private Instance

Launch a new EC2 instance using the following settings.

Name and tags [Info](#)

Name

Private Instance

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

Instance type

t3.micro
Family: t3 2 vCPU 1 GiB Memory Current generation: true
On-Demand SUSE base pricing: 0.0104 USD per Hour
On-Demand Windows base pricing: 0.0196 USD per Hour
On-Demand RHEL base pricing: 0.0704 USD per Hour
On-Demand Linux base pricing: 0.0104 USD per Hour

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

Proceed without a key pair (Not recommended)
Default value

[Create new key pair](#)

Advanced details [Info](#)

User data - optional [Info](#)

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

Choose file

```
#!/bin/bash
# Turn on password authentication for lab challenge
echo 'lab-password' | passwd ec2-user --stdin
sed -i 's|[#]*PasswordAuthentication no|PasswordAuthentication yes|g' /etc/ssh/sshd_config
systemctl restart sshd.service
```

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI
ami-0eb9d67c52f5c80e5 (64-bit (x86), uefi-preferred) / ami-0faea24786f93f590 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Description

Amazon Linux 2023 AMI 2023.4.20240528.0 x86_64 HVM kernel-6.1

Architecture

64-bit (x86)

Boot mode

uefi-preferred

AMI ID

ami-0eb9d67c52f5c80e5

Verified provider

Network settings [Info](#)

VPC - required [Info](#)

vpc-0bc64cbec9ceea67a (Lab VPC)
10.0.0.0/16

Subnet [Info](#)

subnet-03241a35161803a92
VPC: vpc-0bc64cbec9ceea67a Owner: 654654284832
Availability Zone: us-west-2a IP addresses available: 507 CIDR: 10.0.2.0/23

Private Subnet

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

Security group name - required

Private Instance SG

This security group will be added to all network interfaces.

Description - required [Info](#)

Allow SSH from Bastion

Inbound Security Group Rules

Type [Info](#)

ssh

Port range [Info](#)

22

Source type [Info](#)

Custom

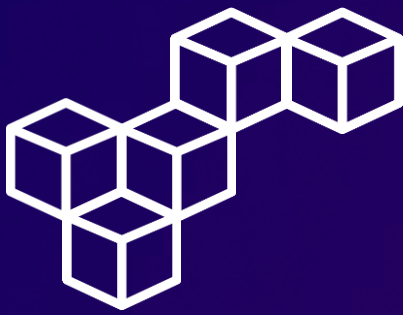
Source [Info](#)

Q Add CIDR, prefix list or security g

10.0.0.0/16 X

re/start





Conclusions

VPCs

VPCs provide isolated network environments within AWS, allowing full control over network configuration and security.

Subnets

Subnets partition your VPC into smaller network segments, enabling efficient resource organization and traffic management.

Internet Gateways

Internet Gateways facilitate internet access for resources within a VPC, allowing inbound and outbound traffic.

NAT Gateways

NAT Gateways enable instances in private subnets to access the internet while remaining inaccessible from the outside.

Routing Tables

Routing Tables direct traffic within your VPC, defining the paths for data to travel to its destination.

Bastion Hosts

Bastion Hosts serve as secure entry points for administrative access to instances in private subnets, enhancing overall security.



Cristhian Becerra



[cristhian-becerra-espinoza](https://www.linkedin.com/in/cristhian-becerra-espinoza)



+51 951 634 354



cristhianbecerra99@gmail.com



Lima, Peru

