

Guided Lab: Creating a Custom Virtual Private Cloud (VPC) from scratch

Description

Amazon Virtual Private Cloud (VPC) is a foundational component of AWS that allows you to provision a logically isolated section of the AWS Cloud. Think of a VPC as a private estate within a bustling city (the AWS Cloud). Within this estate, you have the freedom to construct various properties and infrastructure according to your specific requirements.

- **Virtual Private Cloud (VPC):** Acts as the cornerstone of your network on AWS. Imagine it as owning a large piece of land where you can establish different areas for various purposes — residential, commercial, and recreational.
- **Subnet:** If the VPC is your large piece of land, a subnet is akin to sectioning off parts of this land into different plots. Each plot can be developed independently, with specific characteristics such as security measures and connectivity options, similar to dividing a large estate into smaller, manageable lots for specific uses.
- **Internet Gateway:** This is like the main gate of your estate that allows access to and from the public roads. It manages the traffic between your estate and the outside world, ensuring that residents can reach global destinations outside your private land.
- **Route Table:** Think of this as the map and directional signs within your estate. It guides the traffic, directing it where to go within the estate or how to exit efficiently to reach external destinations. It ensures that all traffic flows smoothly according to predefined rules, like how a traffic control system manages vehicles' movements.

In this lab, you'll gain hands-on experience with these components by setting up a custom VPC from scratch. While AWS accounts come with a default VPC, understanding how to create and configure a custom VPC is essential for tailored network solutions that fit specific security and network requirements.

Prerequisites

This lab assumes you have basic knowledge of IP addressing & network subnets, and familiarity with AWS core services like EC2 (Elastic Compute Cloud).

If you find any gaps in your knowledge, consider taking the following lab:

- [Creating an Amazon EC2 instance \(Linux\)](#)
- [Setting up a Web server on an EC2 instance](#)
- [Launching an EC2 Instance with User Data](#)

Objectives

In this lab, you will:

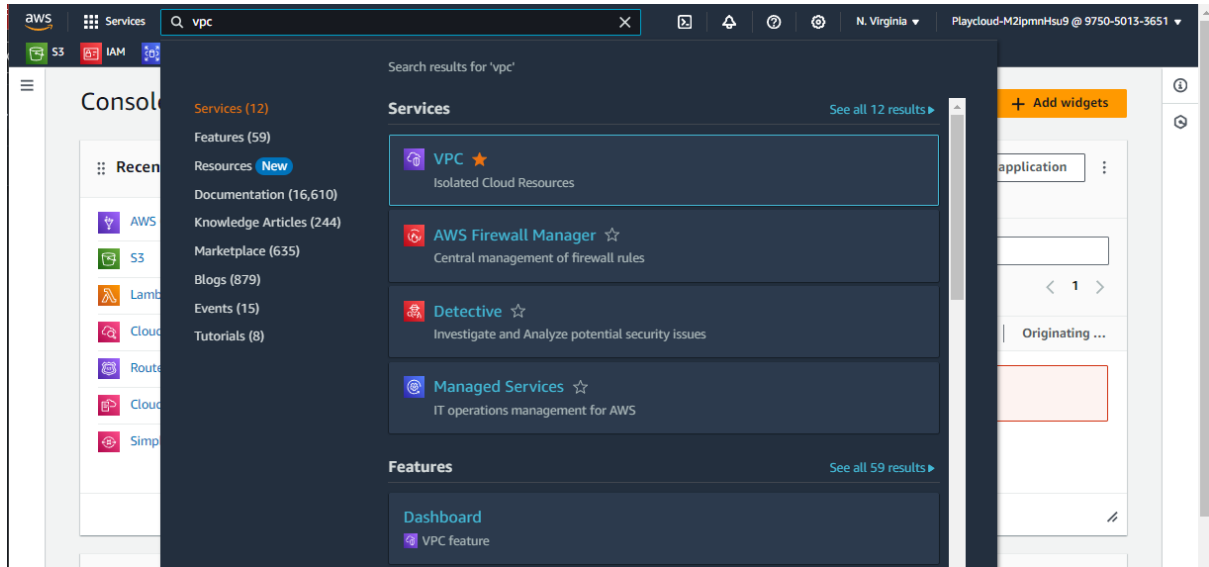
- Understand the structure and components of an Amazon VPC.
- Learn how to create a VPC, including subnets, route tables, and an internet gateway.
- Demonstrate practical skills in isolating network environments within AWS.

[Subscribe to access AWS PlayCloud Labs](#)

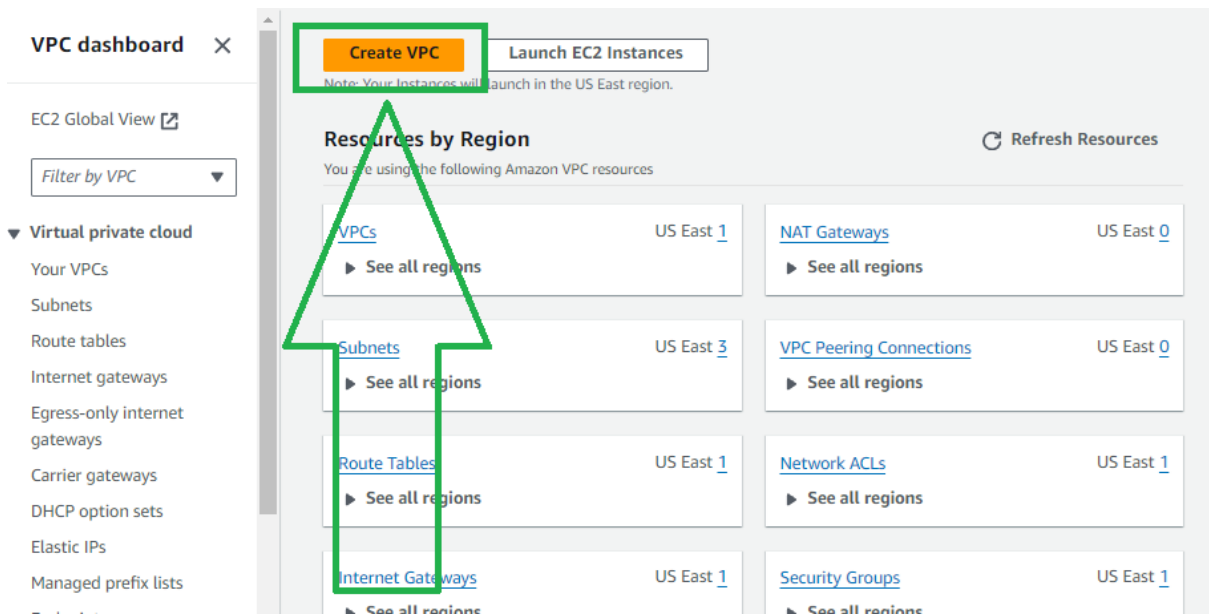
Lab Steps

Creating a Custom VPC

1. Navigate to the VPC dashboard.



2. Click on “Create VPC”



3. Let's select VPC only in the Resources to create to do this lab step by step.

[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.

VPC settings

Resources to create [Info](#)

Create only the VPC resource or the VPC and other networking resources.

☒ VPC only

☐ VPC and more

Note: *VPC and more* – is an option if you want to create VPC, subnets, Route Table, etc. all at once.

4. Enter the following details:

- Name tag: **td-Lab-VPC**
- IPv4 CIDR block: **10.0.0.0/16**

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.

td-Lab-VPC

IPv4 CIDR block [Info](#)

☒ IPv4 CIDR manual input

☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/16

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

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block

☐ IPAM-allocated IPv6 CIDR block

☐ Amazon-provided IPv6 CIDR block

☐ IPv6 CIDR owned by me

Tenancy [Info](#)

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	
<div><div>Q</div>Name<div>X</div></div>	<div><div>Q</div>td-Lab-VPC<div>X</div></div>	<div>Remove tag</div>
<div>Add tag</div> <p>You can add 49 more tags</p>		

Cancel

Create VPC

- Click on **“Create.”**

5. A new VPC will be created with the specified CIDR block, establishing the network space for this lab.

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

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

▼ Security

Network ACLs

Security groups

▼ DNS firewall

Rule groups

Domain lists

...

You successfully created vpc-04a8b66f7ce7cfee1 / td-Lab-VPC

VPC > Your VPCs > vpc-04a8b66f7ce7cfee1

vpc-04a8b66f7ce7cfee1 / td-Lab-VPC

Actions ▾

Details Info

VPC ID vpc-04a8b66f7ce7cfee1	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-0af73d635c2e2cf67	Main route table rtb-01377e76e36a15de8	Main network ACL acl-0551387a53353bf0a
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups Failed to load rule groups	Owner ID 975050133651	

Resource map CIDRs Flow logs Tags Integrations

Resource map Info

VPC Show details
Your AWS virtual network
td-Lab-VPC

Subnets (0)
Subnets within this VPC

Route tables (1)
Route network traffic to resources
rtb-01377e76e36a15de8

Setting Up Subnets

1. Within the VPC dashboard, select “Subnets”

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

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

You successfully created vpc-04a8b66f7ce7cfee1 / td-Lab-VPC

VPC > Your VPCs > vpc-04a8b66f7ce7cfee1

vpc-04a8b66f7ce7cfee1 / td-Lab-VPC

Actions ▾

Details Info

VPC ID vpc-04a8b66f7ce7cfee1	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-0af73d635c2e2cf67	Main route table rtb-01377e76e36a15de8	Main network ACL acl-0551387a53353bf0a
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups Failed to load rule groups	Owner ID 975050133651	

Resource map CIDRs Flow logs Tags Integrations

Resource map Info

2. Then click on “Create subnet.”

VPC dashboard ×

EC2 Global View

Filter by VPC ▾

Virtual private cloud

Your VPCs

Subnets

Route tables

Subnets (3) Info

Last updated 12 minutes ago

Actions ▾ **Create subnet**

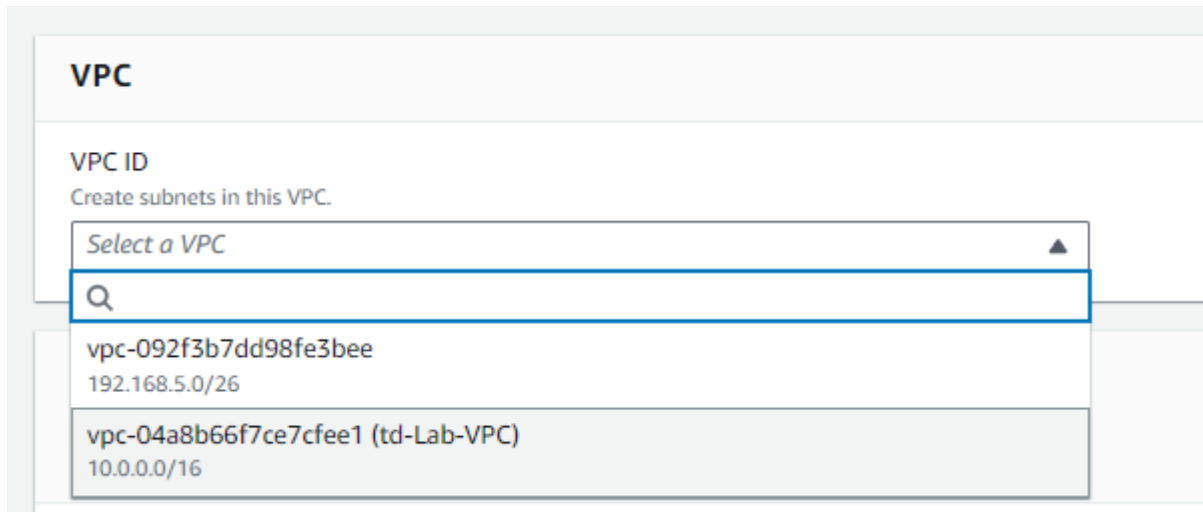
Find resources by attribute or tag

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR
<input type="checkbox"/>	-	subnet-0a234fc2136c9af52	Available	vpc-092f3b7dd98fe3bee	192.168.5.16/28
<input type="checkbox"/>	-	subnet-09abbbbc333543f75e	Available	vpc-092f3b7dd98fe3bee	192.168.5.32/28
<input type="checkbox"/>	-	subnet-0dd450d5eababfb13	Available	vpc-092f3b7dd98fe3bee	192.168.5.0/28

Note: Notice that there are already default subnets which comes along with the default VPC

3. Create subnets:

- **VPC ID:** Select **td-Lab-VPC**



The screenshot shows the 'VPC ID' dropdown menu in the AWS console. The dropdown is open, displaying a search bar and two options. The first option is 'vpc-092f3b7dd98fe3bee' with a CIDR block of '192.168.5.0/26'. The second option is 'vpc-04a8b66f7ce7cfee1 (td-Lab-VPC)' with a CIDR block of '10.0.0.0/16'. The second option is highlighted.

VPC

VPC ID
Create subnets in this VPC.

Select a VPC

Q

vpc-092f3b7dd98fe3bee
192.168.5.0/26

vpc-04a8b66f7ce7cfee1 (td-Lab-VPC)
10.0.0.0/16

- **Name tag:** PublicSubnet-1
- **Availability Zone:** US East (N. Virginia) / us-east-1a
- **IPv4 CIDR block:** 10.0.1.0/24

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

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

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.

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

< > ^ v

▼ Tags - optional

Key

×

Value - optional

×

Remove

Add new tag

You can add 49 more tags.

Remove

Add new subnet

Cancel

Create subnet

- Add another subnet by clicking the “Add new subnet”

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.

PublicSubnet

The name can be up to 256 characters long.

Availability Zone [Info](#)

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

US East (N. Virginia) / us-east-1a

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.

10.0.0/16

IPv4 subnet CIDR block

10.0.1.0/24

256 IPs

▼ Tags - optional

Key

Q Name

X

Value - optional

Q PublicSubnet

X

Remove

Add new tag

You can add 49 more tags.

Remove

Add new subnet

Note: While you can create multiple subnets within a VPC, remember that the number depends on the VPC's CIDR block size and AWS quotas. Each subnet needs a unique range of IP addresses. By default, AWS allows up to 200 subnets per VPC, but this can be increased by requesting a service quota increase from AWS support. Plan your subnets wisely to accommodate future growth and manage different network environments effectively.

- Follow the configurations below:
 - **Name tag:** PublicSubnet-2
 - **Availability Zone:** US East (N. Virginia) / us-east-1b
 - **IPv4 CIDR block:** 10.0.2.0/24

Subnet 2 of 2

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

PublicSubnet-2

The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US East (N. Virginia) / us-east-1b

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

10.0.2.0/24 256 IPs

< > ^ v

▼ **Tags - optional**

Key	Value - optional	
Q Name	Q PublicSubnet-2	Remove

Add new tag

You can add 49 more tags.

Remove

Add new subnet

- Click on **“Create.”**

✓ You have successfully created 2 subnets: subnet-05fbd12117c9530d7, subnet-0e42438ffae03897f

Subnets (2) [Info](#) Last updated less than a minute ago [Refresh](#) [Actions](#) [Create subnet](#)

Find resources by attribute or tag

Subnet ID : subnet-05fbd12117c9530d7 Subnet ID : subnet-0e42438ffae03897f Clear filters

	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
<input type="checkbox"/>	PublicSubnet-2	subnet-0e42438ffae038...	Available...	vpc-04a8b66f7ce7cfee1 td...	10.0.2.0/24	-
<input type="checkbox"/>	PublicSubnet-1	subnet-05fbd12117c953...	Available...	vpc-04a8b66f7ce7cfee1 td...	10.0.1.0/24	-

Establishing an Internet Gateway

1. In the left sidebar find and click on **“Internet Gateways.”**

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
- Managed prefix lists
- Endpoints
- Endpoint services
- NAT gateways

Subnets (2) Info

Last updated 1 minute ago

Actions

Create subnet

Find resources by attribute or tag

Subnet ID : subnet-05fbd12117c9530d7 X Subnet ID : subnet-0e42438ffae03897f X Clear filters

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR
<input type="checkbox"/>	PublicSubnet-2	subnet-0e42438ffae038...	Available...	vpc-04a8b66f7ce7cfee1 td-...	10.0.2.0/24
<input type="checkbox"/>	PublicSubnet-1	subnet-05fbd12117c953...	Available...	vpc-04a8b66f7ce7cfee1 td-...	10.0.1.0/24

Select a subnet

2. Click on “Create internet gateway”

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

Internet gateways (1) Info

Search

Actions

Create internet gateway

<input type="checkbox"/>	Name	Internet gateway ID	State	VPC ID
<input type="checkbox"/>	-	igw-0118335fc00ac56c0	Attached	vpc-092f3b7dd98

3. Name it td-LabInternetGateway

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.

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	
<input type="text" value="Name"/>	<input type="text" value="td-LabInternetGateway"/>	<input type="button" value="Remove"/>

You can add 49 more tags.

4. Click on **Create internet gateway**

5. Choose the “**Attach to VPC**” in the **Action dropdown** or the notification that pops up after you created the **internet gateway** or in the **Actions** dropdown

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-044255d775ce222c4 - td-LabInternetGateway. You can now attach to a VPC to enable the VPC to communicate with the internet.

VPC > Internet gateways > igw-044255d775ce222c4

igw-044255d775ce222c4 / td-LabInternetGateway

Details

Internet gateway ID igw-044255d775ce222c4	State Detached	VPC ID -	Owner 9
--	-------------------	-------------	------------

Tags

Key	Value
Name	td-LabInternetGateway

Actions

- Attach to VPC
- Detach from VPC
- Manage tags
- Delete

< 1 > ⚙

6. Attach the internet gateway to td-Lab-VPC

VPC > Internet gateways > Attach to VPC (igw-044255d775ce222c4)

Attach to VPC (igw-044255d775ce222c4) [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-04a8b66f7ce7cfee1 - td-Lab-VPC

▶ AWS Command Line Interface command

Cancel

Attach internet gateway

7. Click **Attach internet gateway**

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

Internet gateway igw-044255d775ce222c4 successfully attached to vpc-04a8b66f7ce7cfee1

VPC > Internet gateways > igw-044255d775ce222c4

igw-044255d775ce222c4 / td-LabInternetGateway

Actions

Details [Info](#)

Internet gateway ID	State	VPC ID	Owner
igw-044255d775ce222c4	Attached	vpc-04a8b66f7ce7cfee1 td-Lab-VPC	975050133651

Tags

Search tags

Manage tags

Key	Value
Name	td-LabInternetGateway

Configuring Route Tables

1. Navigate to "Route Tables" in the VPC dashboard

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

Managed prefix lists

Subnets (2) [Info](#)

Last updated 1 minute ago

Actions

Create subnet

Find resources by attribute or tag

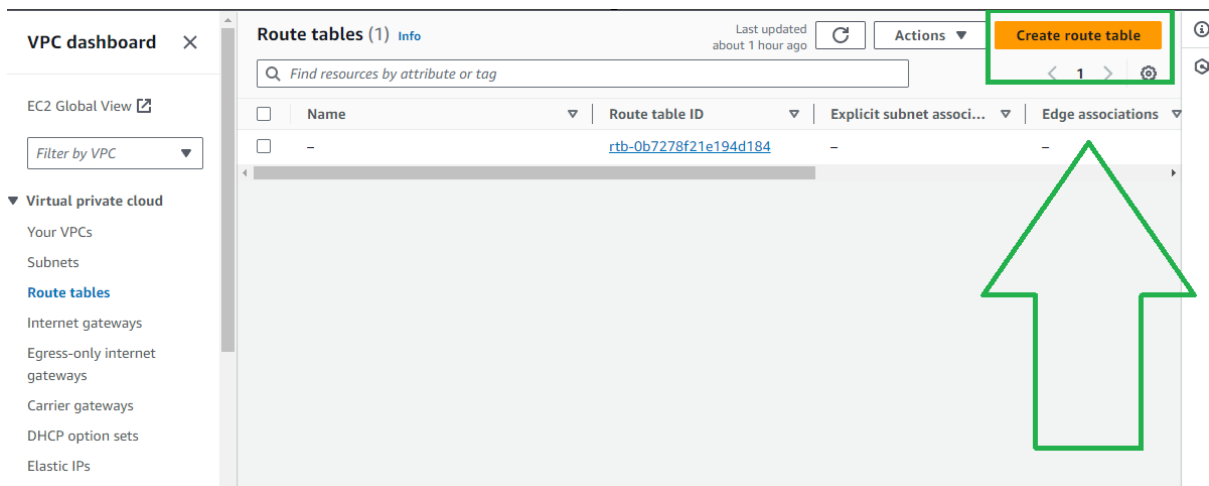
Subnet ID: subnet-05fbd12117c9530d7

Subnet ID: subnet-0e42438ffae03897f

Clear filters

	Name	Subnet ID	State	VPC	IPv4 CIDR
<input type="checkbox"/>	PublicSubnet-2	subnet-0e42438ffae038...	Available...	vpc-04a8b66f7ce7cfee1 td-...	10.0.2.0/24
<input type="checkbox"/>	PublicSubnet-1	subnet-05fbd12117c953...	Available...	vpc-04a8b66f7ce7cfee1 td-...	10.0.1.0/24

2. Click "Create route table."



Note: Notice that after creating a VPC, AWS automatically create route table for that VPC for you. You can either use this or reconfigure it. But for this lab we will manually create our own route table and its configurations.

3. Name it PublicRouteTable and associate it with td-Lab-VPC.

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.

VPC
The VPC to use for this route table.

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	
<input type="text" value="Name"/>	<input type="text" value="PublicRouteTable"/>	<input type="button" value="Remove"/>

You can add 49 more tags.

4. Click “Create route table”

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
- Managed prefix lists
- Endpoints
- Endpoint services
- NAT gateways

Route table rtb-0e7dac5dba137cf81 | PublicRouteTable was created successfully.

VPC > Route tables > rtb-0e7dac5dba137cf81

rtb-0e7dac5dba137cf81 / PublicRouteTable

Actions

Details Info

Route table ID rtb-0e7dac5dba137cf81	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-04a8b66f7ce7cfee1 td-Lab-VPC	Owner ID 975050133651		

Routes Subnet associations Edge associations Route propagation Tags

Routes (1) Both Edit routes

Filter routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

5. Click on "Edit routes"

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
- Managed prefix lists
- Endpoints
- Endpoint services
- NAT gateways

Route table rtb-0e7dac5dba137cf81 | PublicRouteTable was created successfully.

VPC > Route tables > rtb-0e7dac5dba137cf81

rtb-0e7dac5dba137cf81 / PublicRouteTable

Actions

Details Info

Route table ID rtb-0e7dac5dba137cf81	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-04a8b66f7ce7cfee1 td-Lab-VPC	Owner ID 975050133651		

Routes Subnet associations Edge associations Route propagation Tags

Routes (1) Both Edit routes

Filter routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

6. Click on "Add route"

VPC > Route tables > rtb-0e7dac5dba137cf81 > Edit routes

Edit routes

Route 1

Destination
10.0.0.0/16

Target
local

Status
Active

Propagated
No

Add route

Cancel Preview Save changes

7. Add the following:

- **Destination:** 0.0.0.0/0
- **Target:** Select **Internet Gateway** and the name of the internet gateway that you created.

Route 2

Destination:

Target:

Status: -

Propagated: No

By adding this route, you ensure that any internet-bound traffic (any IP address represented by 0.0.0.0/0) to pass through an internet gateway from your VPC is correctly routed through the internet gateway, thus enabling external connectivity. This setting is particularly important for public subnets that host web servers or other resources needing to communicate with the internet.

8. Click **Save changes**

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
- Managed prefix lists
- Endpoints
- Endpoint services
- NAT gateways
- Peering connections

Security

Updated routes for rtb-0e7dac5dba137cf81 / PublicRouteTable successfully

rtb-0e7dac5dba137cf81 / PublicRouteTable

Details

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-0e7dac5dba137cf81	No	-	-
VPC	Owner ID		
vpc-04a8b66f7ce7cfee1 td-Lab-VPC	975050133651		

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

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-044255d775ce222c4	Active	No
10.0.0.0/16	local	Active	No

9. Associate PublicRouteTable with PublicSubnet-1 and PublicSubnet-2

- Go to the **Subnet associations tab**

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
- Managed prefix lists
- Endpoints
- Endpoint services
- NAT gateways
- Peering connections

VPC > Route tables > rtb-0e7dac5dba137cf81

rtb-0e7dac5dba137cf81 / PublicRouteTable

Actions ▼

Details Info

Route table ID rtb-0e7dac5dba137cf81	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-04a8b66f7ce7cfee1 td-Lab-VPC	Owner ID 975050133651		

Routes Subnet associations Edge associations Route propagation Tags

Routes (2) Both ▼ Edit routes

Filter routes

Destination	Target	Status	Propagated
0.0.0.0/0	igw-044255d775ce222c4	Active	No
10.0.0.0/16	local	Active	No

- In this tab you will see:

VPC > Route tables > rtb-0e7dac5dba137cf81

rtb-0e7dac5dba137cf81 / PublicRouteTable

Actions ▼

Details Info

Route table ID rtb-0e7dac5dba137cf81	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-04a8b66f7ce7cfee1 td-Lab-VPC	Owner ID 975050133651		

Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (0) Edit subnet associations

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
No subnet associations You do not have any subnet associations.			

Subnets without explicit associations (2) Edit subnet associations

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

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
PublicSubnet-2	subnet-0e42438ffae03897f	10.0.2.0/24	-
PublicSubnet-1	subnet-05fbd12117c9530d7	10.0.1.0/24	-

CONCEPT:

Explicit Subnet Associations

This occurs when you manually associate a subnet with a specific route table. By doing this, you ensure that all the traffic from that subnet is directed according to the routes defined in the associated route table. This is typically used to enforce specific routing policies for different parts of your network, such as distinguishing between public (internet-facing) and private (internal-only) subnets.

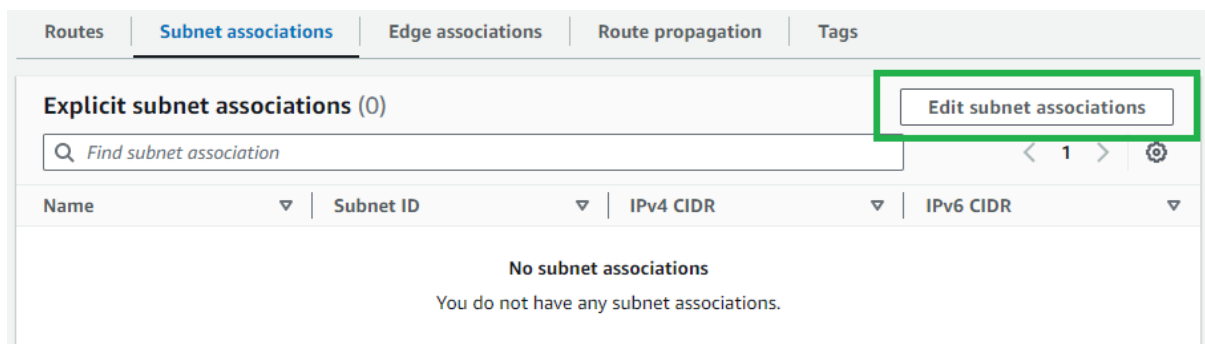
- **Example Usage:** You might explicitly associate a subnet with a route table that has a route to an internet gateway for public subnets, ensuring instances within these subnets can access the internet.

Subnets Without Explicit Associations

Any subnets in a VPC that do not have an explicit route table association will automatically be associated with the VPC's main route table. The main route table is the default route table that AWS creates with each VPC. This setup ensures that every subnet has at least basic routing capabilities, even if no custom routing has been configured.

- **Example Usage:** Private subnets that do not require direct access to the internet can be left with the default route table, which typically does not contain a route to the internet gateway. This helps in maintaining the security posture by limiting external access.

-
- Click on “**Edit subnet associations**” inside the **Explicit Subnet Associations**



- Select both PublicSubnet-1 and PublicSubnet-2 and click on **Save associations**

VPC > Route tables > rtb-0e7dac5dba137cf81 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/2)

< 1 > ⚙

<input checked="" type="checkbox"/>	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/>	PublicSubnet-2	subnet-0e42438ffae03897f	10.0.2.0/24	–	Main (rtb-01377e76e36a15de8)
<input checked="" type="checkbox"/>	PublicSubnet-1	subnet-05fbd12117c9530...	10.0.1.0/24	–	Main (rtb-01377e76e36a15de8)

Selected subnets

Cancel
Save associations

- This will be the output:

✓ You have successfully updated subnet associations for rtb-0e7dac5dba137cf81 / PublicRouteTable.

VPC > Route tables > rtb-0e7dac5dba137cf81

rtb-0e7dac5dba137cf81 / PublicRouteTable

Actions

Details Info

Route table ID rtb-0e7dac5dba137cf81	Main No	Explicit subnet associations 2 subnets	Edge associations –
VPC vpc-04a8b66f7ce7cfee1 td-Lab-VPC	Owner ID 975050133651		

Routes
Subnet associations
Edge associations
Route propagation
Tags

Explicit subnet associations (2)

< 1 > ⚙
Edit subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
PublicSubnet-2	subnet-0e42438ffae03897f	10.0.2.0/24	–
PublicSubnet-1	subnet-05fbd12117c9530d7	10.0.1.0/24	–

Subnets without explicit associations (0)

< 1 > ⚙
Edit subnet associations

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

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
No subnets without explicit associations All your subnets are associated with a route table.			

Testing Connectivity

1. Navigate to the EC2 Launch and launch an EC2 instance within PublicSubnet-1 or PublicSubnet-2.

▼ Network settings

Info

VPC - required

Info

vpc-04a8b66f7ce7cfee1 (td-Lab-VPC)

10.0.0.0/16

▼

↻

Subnet

Info

subnet-05fbd12117c9530d7

PublicSubnet-1

VPC: vpc-04a8b66f7ce7cfee1

Owner: 975050133651

Availability Zone: us-east-1a

IP addresses available: 251

CIDR: 10.0.1.0/24

▲

↻

Create new subnet

Q |

subnet-0e42438ffae03897f

PublicSubnet-2

VPC: vpc-04a8b66f7ce7cfee1

Owner: 975050133651

Availability Zone: us-east-1b

IP addresses available: 251

CIDR: 10.0.2.0/24

subnet-05fbd12117c9530d7

PublicSubnet-1

VPC: vpc-04a8b66f7ce7cfee1

Owner: 975050133651

Availability Zone: us-east-1a

IP addresses available: 251

CIDR: 10.0.1.0/24

✓

specific traffic to reach your instance.

2. During setup:

- Ensure the instance's security group allows inbound ssh access (e.g., allow all inbound traffic anywhere or simply your IP for security) and **HTTP** connection using source **0.0.0.0/0**
Note: Usually, you need to make ssh connection only to the trusted IPs but for this testing and simplicity we can use **anywhere** which is **0.0.0.0/0**
- Ensure that you **enable** Auto-assign public IP
- Created an SSH key.

Key pair name - required

my-key-pair [Create new key pair](#)

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-06ed3b3736d9ee319 (td-Lab-VPC)
10.0.0.0/16 [Create new VPC](#)

Subnet [Info](#)

subnet-02da11d92d36b536d [PublicSubnet-1](#) [Create new subnet](#)

VPC: vpc-06ed3b3736d9ee319 Owner: 654654537193
Availability Zone: us-east-1a IP addresses available: 251 CIDR: 10.0.1.0/24

Auto-assign public IP [Info](#)

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) [Info](#)

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

☒ Create security group ☐ Select existing security group

Security group name - required

launch-wizard-1

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ., -, /, @, _ [] + = & , ! *

Description - required [Info](#)

launch-wizard-1 created 2024-06-21T07:04:18.727Z

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) [Remove](#)

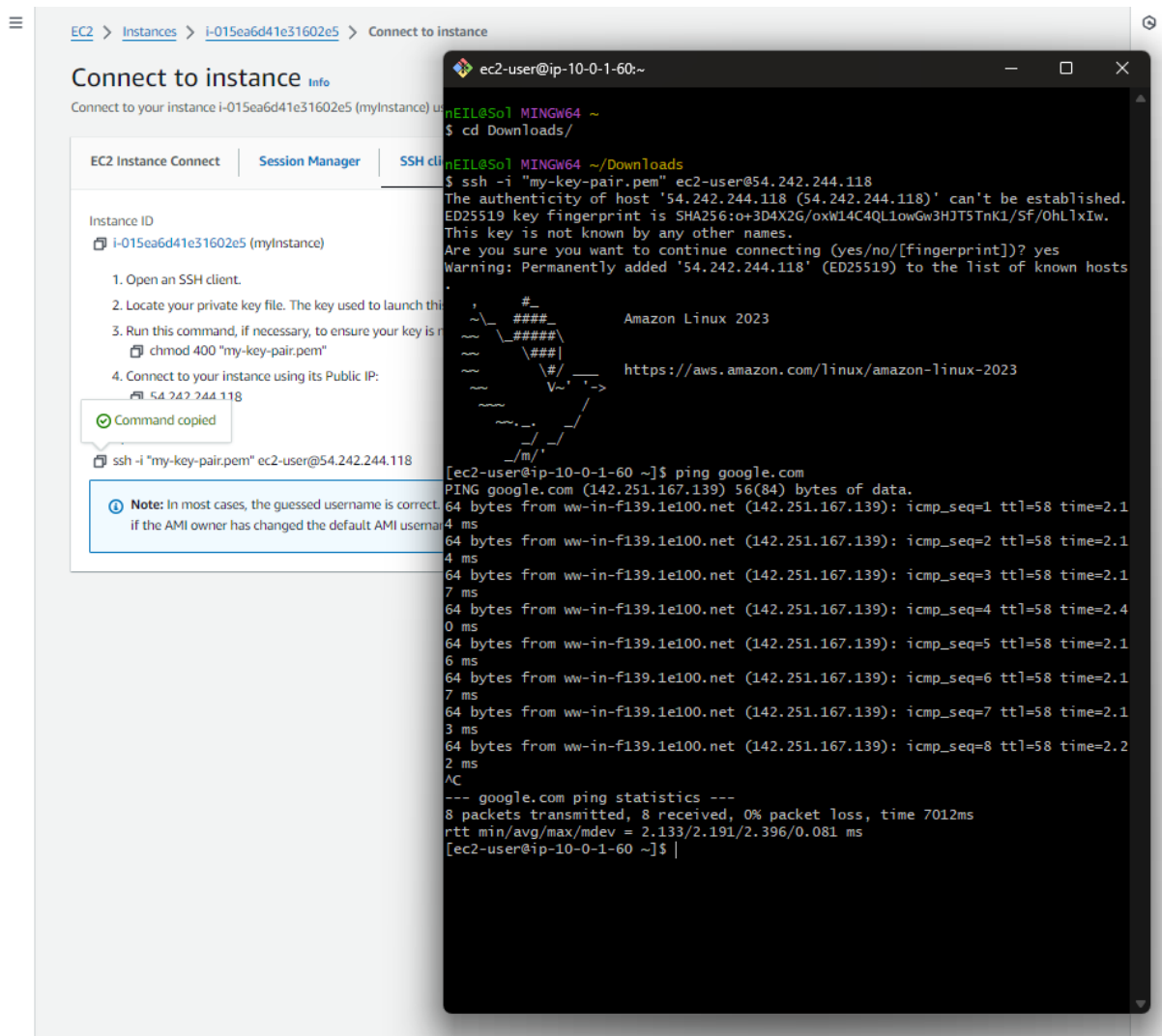
Type Info	Protocol Info	Port range Info	Source type Info	Source Info	Description - optional Info
ssh	TCP	22	Anywhere	<input type="text" value="0.0.0.0/0"/> <input type="button" value="Add CIDR, prefix list or security"/> <input type="button" value="X"/>	e.g. SSH for admin desktop

▼ Security group rule 2 (TCP, 80, 0.0.0.0/0) [Remove](#)

Type Info	Protocol Info	Port range Info	Source type Info	Source Info	Description - optional Info
HTTP	TCP	80	Custom	<input type="text" value="0.0.0.0/0"/> <input type="button" value="Add CIDR, prefix list or security"/> <input type="button" value="X"/>	e.g. SSH for admin desktop

- Launch your instance.

3. Once the instance is running, connect via SSH attempt to ping a public internet address to verify connectivity.



That's it. Congratulations! You've successfully set up a custom Amazon VPC, configured its subnets, established an internet gateway, and managed route table associations. This practical experience has enhanced your understanding of AWS network isolation and configuration. You've seen firsthand how to manage traffic flow within a VPC, ensuring secure and efficient network operations. This foundation will aid in further exploration of AWS networking features, enabling you to build more robust and scalable cloud solutions. Happy learning!