



Creating a Private Subnet



Roshan Thomas

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.

Associated VPC CIDRs

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 be within this block.

IPv4 subnet CIDR block
 256 /8

Tags - optional

Key Value - optional

You can add 40 more tags.



Roshan Thomas
NextWork Student

NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a service that lets you create isolated virtual networks within AWS. It's useful for securely managing and controlling resources, providing privacy, and ensuring customized network configurations tailored to your needs.

How I used Amazon VPC in this project

I used Amazon VPC to create a private subnet for securely hosting internal resources, while keeping them isolated from public internet access. This included setting up dedicated route tables and network ACLs for enhanced security.

One thing I didn't expect in this project was...

I didn't expect that subnet CIDR blocks needed to be unique to avoid overlaps. It was surprising to see how critical it is to manage IP ranges to prevent routing conflicts within the VPC.

This project took me...

1 hour 40 minutes.



Roshan Thomas
NextWork Student

NextWork.org

Private vs Public Subnets

The difference between public and private subnets is that public subnets are like open streets connected to the internet, while private subnets are secluded neighborhoods, hidden away with no direct internet access!

Having private subnets is useful because they keep sensitive resources tucked away from the internet, like a secret hideout, allowing secure operations without public exposure!

My private and public subnets cannot have the same IP address range. It's like ensuring two neighborhoods don't share the same street names—each needs its own space to avoid confusion and traffic jams!

The screenshot shows the 'Create subnet' wizard in the AWS VPC console. The 'VPC' section shows a selected VPC ID: 'vpc-0f967c26207d0aa (NextWork VPC)'. The 'Associated VPC CIDRs' section shows a single CIDR block: '10.0.0.0/16'. The 'Subnet settings' section contains the following details:

- Subnet name:** 'NextWork Private Subnet'
- Availability Zone:** 'Asia Pacific (Mumbai) / ap-south-1b'
- IPv4 VPC CIDR block:** '10.0.0.0/16'
- IPv4 subnet CIDR block:** '10.0.1.0/24' (highlighted in blue)
- Tags - optional:** A key-value pair 'Name: NextWork Private Subnet' is listed.

A dedicated route table

By default, my private subnet is associated with the main route table, which doesn't have a route to the internet. It's like a neighborhood with roads that don't lead outside, keeping it off the map!

I had to set up a new route table because I needed to give my public subnet a path to the internet. It's like adding a highway to connect my neighborhood to the rest of the world!

My private subnet's dedicated route table only has one inbound and one outbound rule that allows local traffic within the VPC. It's like a private road, only letting cars from the same neighborhood pass through!

The screenshot shows the AWS Route Tables page with the following details:

Route tables (1/3) Info

Name	Route table ID	Explicit subnet associations	Main	VPC
<input checked="" type="checkbox"/> NextWork Public Route Table	rtb-0bbbce3927d9c7f2b	subnet-024c4ca89ee1562b3 / NextWork Public Subnet	Yes	vpc-0f9967e2620e7daaa
<input type="checkbox"/> -	rtb-0dc9a3b51d1d143f5	-	Yes	vpc-0be69ac1b04f5a2cc
<input type="checkbox"/> NextWork Private Route Table	rtb-0c64d440c7188a350	subnet-001b474e7c2d7f... / NextWork Private Subnet	No	vpc-0f9967e2620e7daaa

rtb-0bbbce3927d9c7f2b / NextWork Public Route Table

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

Details

Route table ID rtb-0bbbce3927d9c7f2b	Main <input checked="" type="checkbox"/> Yes	Explicit subnet associations subnet-024c4ca89ee1562b3 / NextWork Public Subnet	Edge associations -
Owner ID			

Roshan Thomas
NextWork Student

NextWork.org

A new network ACL

By default, my private subnet is associated with the default NACL, which allows all traffic in and out. It's like a neighborhood gate that doesn't stop anyone, letting everything flow freely!

I set up a dedicated network ACL for my private subnet because I wanted tighter security. It's like hiring extra security guards to control who gets in and out of my exclusive neighborhood!

My new network ACL has two simple rules - allow inbound traffic from within the VPC and allow outbound traffic to the VPC. It's like letting neighbors visit but only allowing trips within the local area!

You have successfully updated subnet associations for adl-011c390e59418eba4 / NextWork Private NACL.

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count	Outbound rules count
-	adl-005eb4ad2985db34a	3 Subnets	Yes	vpc-0be69ac1b04f5a2cc	2 Inbound rules	2 Outbound rules
-	adl-081dde7587c4cd17d	-	Yes	vpc-0f9967e2620e7daaa / NextWork VPC	2 Inbound rules	2 Outbound rules
NextWork Public NACL	adl-0fc91050f271824b0	subnet-024c4ca89ee1562b3 / NextWork Public...	No	vpc-0f9967e2620e7daaa / NextWork VPC	2 Inbound rules	2 Outbound rules
<input checked="" type="checkbox"/> NextWork Private N...	<input checked="" type="checkbox"/> adl-011c390e59418eba4	<input checked="" type="checkbox"/> subnet-001b474e7c2d7fbff / NextWork Private...	No	<input checked="" type="checkbox"/> vpc-0f9967e2620e7daaa / NextWork VPC	<input checked="" type="checkbox"/> 1 Inbound rule	<input checked="" type="checkbox"/> 1 Outbound rule

Inbound rules (1)

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



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for
more projects

