



Creating a Private Subnet



Sai Prasanth Reddy

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
<input type="text" value="Name"/>	<input type="text" value="NextWork Private Subnet"/>

[Add new tag](#)
You can add 49 more tags.
[Remove](#)

[Add new subnet](#)

[Cancel](#) [Create subnet](#)



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a service that lets you create isolated cloud networks in AWS. It's useful because it provides control over networking, including IP ranges, subnets, and security, enabling secure, scalable, and customizable cloud infrastructure.

How I used Amazon VPC in this project

I used Amazon VPC in today's project to create an isolated network, set up private subnets and configured route tables to ensure proper network access and security for my resources.

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

One thing I didn't expect in this project was encountering an error for assigning the same CIDR block to both subnets. I had to ensure each subnet had a unique CIDR range to avoid conflicts in routing traffic.

This project took me...

This project took me about 45 minutes, with extra time spent resolving the CIDR block conflict and configuring the route tables and network ACLs for the private subnet.



Private vs Public Subnets

The difference between public and private subnets is that public subnets have a route to the internet through an internet gateway, allowing external access, while private subnets do not, restricting them to internal network communication.

Having private subnets are useful because they enhance security by isolating sensitive resources from direct internet access, allowing internal communication while still accessing the internet through a NAT gateway for outbound traffic.

My private and public subnets cannot have the same IP address range, as each subnet must have a unique CIDR block within the VPC to properly route traffic without conflicts.

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

IPv4 VPC CIDR block
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

Tags - optional
Key Value - optional

You can add 49 more tags.



A dedicated route table

By default, my private subnet is associated with the main route table of the VPC, which does not have a route to the internet gateway, ensuring it remains isolated from external internet access.

I had to set up a new route table because my private and public subnets need different routing configurations, with the public subnet requiring a route to the internet gateway and the private subnet remaining isolated.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows traffic within the VPC, enabling internal communication without allowing direct internet access.

The screenshot shows the AWS VPC dashboard with the 'Route tables' section open. A message at the top indicates successful subnet association. The 'Create route table' button is visible. The table lists three route tables:

Name	Route table ID	Explicit subnet associ...	Main	VPC	Owner ID
-	rtb-05eae23ccbafedc9f	-	Yes	vpc-0474dd46d88b1082c	381491882145
NextWork Public Route Table	rtb-0a84c27d11b3b11ec	subnet-0d48a816b3529...	Yes	vpc-084d7a904abce1c0 Next...	381491882145
NextWork Private Route Table	rtb-0bdad9f2108ce3193	subnet-0d745924b4507c...	No	vpc-084d7a904abce1c0 Next...	381491882145

The 'Routes' tab for the 'rtb-0bdad9f2108ce3193 / NextWork Private Route Table' is selected, showing one route entry:

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No



A new network ACL

By default, my private subnet is associated with the VPC's default network ACL, which allows all inbound and outbound traffic unless custom rules are set to restrict it.

I set up a dedicated network ACL for my private subnet because I needed more granular control over inbound and outbound traffic, allowing me to enhance security by defining specific rules for traffic filtering at the subnet level.

My new network ACL has two simple rules — one inbound rule allowing internal VPC traffic and one outbound rule allowing traffic to other subnets within the VPC, while blocking all other unauthorized inbound and outbound traffic.

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count	Outbound rules count
-	ad-06b73679d00281c9	-	Yes	vpc-084d7a904abcb1c0 / NextWork VPC	2 Inbound rules	2 Outbound rules
-	ad-0bd06eca0beb052f	6 Subnets	Yes	vpc-0474dd46d88b1082c	2 Inbound rules	2 Outbound rules
NextWork Private NACL	ad-0954318feef3f139	subnet-0d745924b4507cc0 / NextWork Privat...	No	vpc-084d7a904abcb1c0 / NextWork VPC	1 Inbound rule	1 Outbound rule
NextWork Public NACL	ad-09eff99c32c6721f	subnet-0dc48a16b3529b90 / NextWork Publi...	No	vpc-084d7a904abcb1c0 / NextWork VPC	2 Inbound rules	2 Outbound rules

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

