



Creating a Private Subnet

J

Michael K.

Screenshot of the AWS VPC Create Subnet wizard:

Create subnet Info

VPC
VPC ID
Create subnets in this VPC.
`vpc-0f1b956fd1260a62 (My Test VPC)`

Associated VPC CIDRs
IPv4 CIDRs
`10.0.0.0/16`

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.
`My-test-private-subnet`
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.
`United States (N. Virginia) / us-east-1a (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
`10.0.1.0/24` 256 IPs



Michael K.

NextWork Student

nextwork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a logically isolated virtual network within AWS where I can launch and manage AWS resources (such as EC2 instances, RDS databases, and load balancers) using my own defined IP address range, subnets, route tables, and network gateways.

How I used Amazon VPC in this project

In today's project, I used my already created Amazon VPC and configured a more secure traffic within it, adding a private Neighborhood (subnet) for resources that are meant to be inaccessible from the internet.

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

One thing I didn't expect in this project is to have some deep understanding on the difference between a public and a private subnet.



J

Michael K.

NextWork Student

nextwork.org

This project took me...

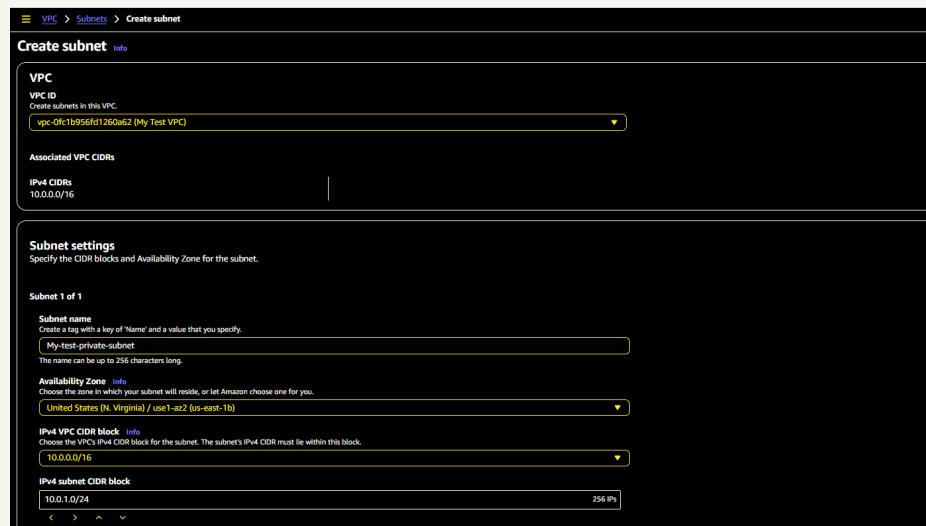
This project took me 30mins.

Private vs Public Subnets

One of the difference between public and private subnets is in their CIDR Block range. Even though they might have the same number of available IP Adresses (because of the same number of changeable bits), their static bits will differ.

Having private subnets are useful because i can host resources which are meant to be private and not accessible from the internet there.

My private and public subnets cannot have the same CIDR Block range number.



A dedicated route table

By default, my private subnet is associated with the public route table that AWS created as I created my VPC.

I had to set up a new route table because that public route table linked to my private subnet contains a route to an Internet gateway which would make my private subnet public if ever attached to it.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows traffic within the VPC.

Name	Route table ID	Explicit subnet associ...	Main	VPC
My-test-private-route-table	rtb-08ef6599ae2bb093f	subnet-01ab1899f834c7...	-	No vpc-0fc1b956fd1260a62 My T...
-	rtb-0b99fe1b1bed72052	-	-	Yes vpc-086c814283b364f04
My-test-public-route-table	rtb-04e9812a8d1e0b047	subnet-036c315df0f4b4f...	-	Yes vpc-0fc1b956fd1260a62 My T...

rtb-08ef6599ae2bb093f / My-test-private-route-table					
Details	Routes	Subnet associations	Edge associations	Route propagation	Tags
Details Route table ID: rtb-08ef6599ae2bb093f VPC: vpc-0fc1b956fd1260a62 My Test VPC	Main: No Owner ID: 109648734195	Explicit subnet associations: subnet-01ab1899f834c752f / My-test-private-subnet	Edge associations: -		

A new network ACL

By default, my private subnet is associated with the public Network ACL created by AWS when my VPC was created.

I set up a dedicated network ACL for my private subnet because if I leave it attached to that public Network ACL and it later gets compromised, an attacker can use its vulnerability to access resources in my private subnet.

My new network ACL has two simple rules - Deny all inbound and outbound traffic for NOW.

The screenshot shows the AWS Network ACLs page. At the top, a success message says: "You have successfully updated subnet associations for acl-05978966087efdabc / My-test-private-NACL." Below this is a "Details" link. The main table lists "Network ACLs (1/4) Info". It shows two rows: one for "My-test-private-NACL" (selected) with ID "acl-05978966087efdabc", associated with "subnet-01ab1899fb34c752f / My-test-private-s...", and another row for "acl-03939030cbbb6f405" which is not selected. The "Associated with" column shows "No" for the selected row and "Yes" for the other. The "Default" column shows "No" for both. Below the table is a section for "acl-05978966087efdabc / My-test-private-NACL". It includes tabs for "Details", "Inbound rules", "Outbound rules", "Subnet associations", and "Tags". The "Inbound rules (1)" tab is selected, showing a single rule: "Rule number: *, Type: All traffic, Protocol: All, Port range: All, Source: 0.0.0.0/0, Allow/Deny: Deny". There is also an "Edit inbound rules" button.



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

