



Creating a Private Subnet

K

Kehinde Abiuwa

The screenshot shows the AWS VPC Subnets page. On the left, there's a sidebar with 'VPC dashboard' and various cloud services like EC2 Global View, Route tables, Internet gateways, Egress-only Internet gateways, DHCP option sets, Elastic IPs, Managed prefix lists, NAT gateways, and Peering connections. The main area is titled 'Subnets (1/1) Info'. It shows a table with one row:

Name	Subnet ID	State	VPC
NextWork Private Subnet	subnet-0100a78c8f9dde40d	Available	vpc-0689fa519d0f3421 Next...

Below the table, there's a detailed view for 'subnet-0100a78c8f9dde40d / NextWork Private Subnet'. It has tabs for Details, Flow logs, Route table, Network ACL, CIDR reservations, Sharing, and Tags. The 'Details' tab is selected.

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a logically isolated network within AWS that allows you to securely launch and manage resources in a customizable virtual network, providing control over IP addressing, subnets, routing, and access

How I used Amazon VPC in this project

I created a vpc, and create both public and private subnets and setup some security for both subnets in my VPC

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

Nothing really

This project took me...

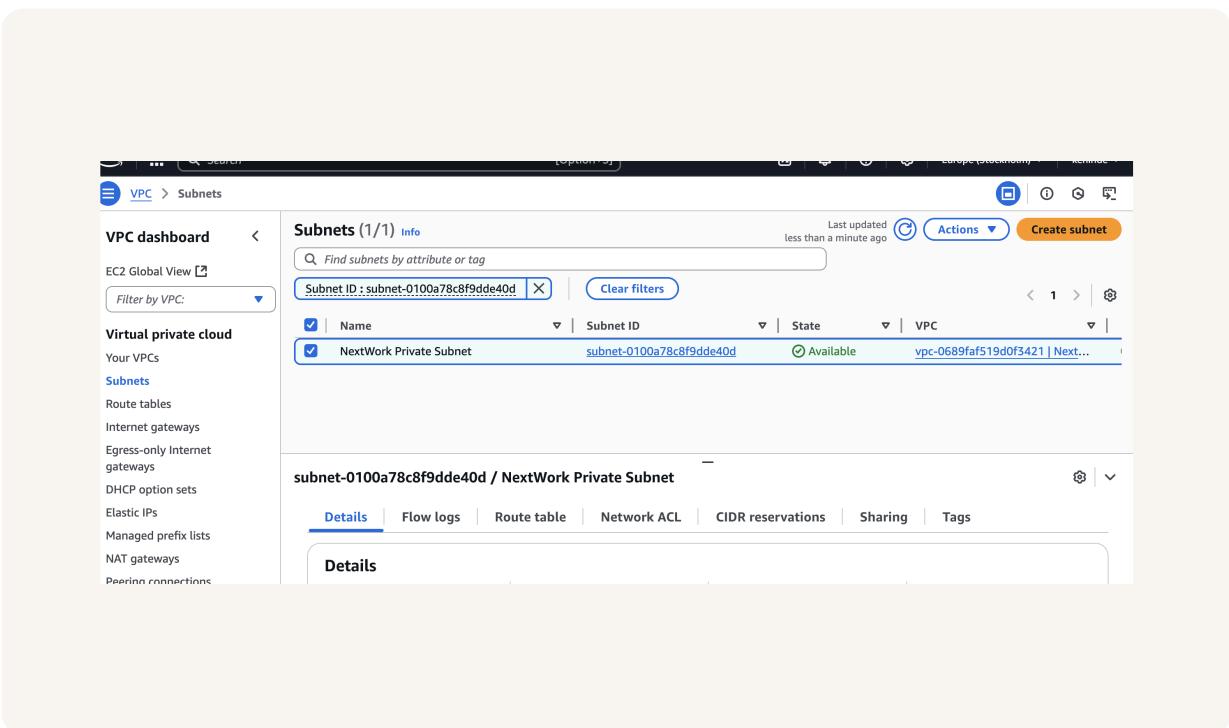
30mins

Private vs Public Subnets

The difference between public and private subnets is that A public subnet has a route to the internet via an internet gateway, while a private subnet does not, restricting its access to internal resources only

Having private subnets are useful because they enhance security by isolating internal resources from direct internet access

My private and public subnets cannot have the same CIDR block (IP address range) within the same VPC



A dedicated route table

By default, my private subnet is associated with the route table that was created for me by AWS when i created my VPC

I had to set up a new route table because that route is to an internet gateway making my private subnet properties public or accessible via the internet which is what i dont want

My private subnet's dedicated route table only has one inbound and one outbound rule that allows internal resources to be directed to my private subnet and not accessible via the internet

The screenshot shows the AWS VPC Route Tables page. A success message at the top states: "You have successfully updated subnet associations for rtb-09b6dd809a0d75518 / NextWork Private Route Table." The main table lists three route tables:

Name	Route table ID	Explicit subnet assoc...	Edge associations	Main
-	rtb-090fe0951879bd35c	-	-	Yes
NextWork Public Route Table	rtb-07f46e18acdfc545	subnet-0b1291a549bc00...	-	Yes
NextWork Private Route Table	rtb-09b6dd809a0d75518	subnet-0100a78c8f9dde...	-	No

The "NextWork Private Route Table" row is selected. Below the table, a detailed view for "rtb-09b6dd809a0d75518 / NextWork Private Route Table" is shown. The "Details" tab is selected, displaying the following information:

- Route table ID: rtb-09b6dd809a0d75518
- Main: No
- VPC: vpc-0689faf519d0f3421 | NextWork VPC
- Owner ID: 511239431868
- Explicit subnet associations: subnet-0100a78c8f9dde40d / NextWork Private Subnet
- Edge associations: -

A new network ACL

By default, my private subnet is associated with, my default NACL that was created automatically when i created my vpc

I set up a dedicated network ACL for my private subnet because i dont want any unauthorised access to my private subnet, its an added layer of security

My new network ACL has two simple rules -' deny inbound and also outbound access to me private subnet

The screenshot shows the NextWork interface for managing Network ACLs. On the left, there's a sidebar with various links like 'Link and Lattice', 'Networks', 'Firewall', etc. The main area shows 'Network ACLs (1/3)' with three entries:

Name	Network ACL ID	Associated with	Default	VPC ID
-	acl-01190da0eb15960e8	3 Subnets	Yes	vpc-042a1f6d
NextWork Public NACL	acl-07416d2015ed4a439	subnet-0b1291a549bc006d0 / NextWork Publi...	Yes	vpc-0689faf5
NextWork Private NACL	acl-0b01a8a74e2436174	subnet-0100a78c8f9dde40d / NextWork Privat...	No	vpc-0689faf5

Below this, it shows the details for the selected 'acl-0b01a8a74e2436174 / NextWork Private NACL'. Under 'Inbound rules', there is one rule:

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



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

