



Creating a Private Subnet



Coran Chunilall

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.

Associated VPC CIDRs

IPv4 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 lie within this block.

IPv4 subnet CIDR block
 256 IPs



Coran Chunilall
NextWork Student

nextwork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) creates an isolated virtual network in AWS where you can launch resources. It's useful for security isolation, custom networking, controlled access, hybrid connectivity, and organizing.

How I used Amazon VPC in this project

I used it to create a private subnet

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

I did not expect to create a private subnet

This project took me...

1 hour



Private vs Public Subnets

Public subnets have direct internet access via an internet gateway and can host resources with public IPs. Private subnets lack direct internet access and typically use NAT gateways/instances for outbound connectivity, keeping resources secure

Private subnets provide security by isolating sensitive resources (databases, application servers) from direct internet access, reducing attack surface. They enable defense-in-depth architecture, controlled outbound access via NAT.

My private and public subnets cannot have the same IPV4 address

The screenshot shows the 'Create subnet' wizard in the AWS Management Console. The 'Subnet settings' section is displayed, which includes fields for Subnet name, Availability Zone, IPv4 VPC CIDR block, and IPv4 subnet CIDR block. The 'Subnet name' field contains 'NextWork Private Subnet'. The 'Availability Zone' dropdown is set to 'No preference'. The 'IPv4 VPC CIDR block' dropdown is set to '10.0.0.0/16'. The 'IPv4 subnet CIDR block' dropdown is set to '10.0.1.0/24'. Other sections visible include 'VPC' (with VPC ID 'vpc-019551b001ef957d9 (NextWork VPC)'), 'Associated VPC CIDRs' (with 'IPv4 CIDRs' '10.0.0.0/16'), and 'Info' buttons for each section.



Coran Chunilall
NextWork Student

nextwork.org

A dedicated route table

By default, my private subnet is associated with my VPC

I had to set up a new route table because in a private subnet it cannot connect to the internet

My private subnet's dedicated route table only has one inbound and one outbound rule that allows local traffic

The screenshot shows the AWS Route Table configuration page for 'tb-023ed972828975584'. The top navigation bar includes fields for 'Route table ID' (tb-023ed972828975584), 'Subnet associations' (subnet-05fc3273603639851 / NextWork Private Subnet), 'Owner ID' (571600841781), and 'VPC' (vpc-019551b001ef957d9 | NextWork VPC). The main content area displays tabs for 'Details', 'Routes', 'Subnet associations', 'Edge associations', 'Route propagation', and 'Tags'. The 'Details' tab is selected, showing the following information:

Details	Main	Explicit subnet associations	Edge associations
Route table ID tb-023ed972828975584	Main No	subnet-05fc3273603639851 / NextWork Private Subnet	-
VPC vpc-019551b001ef957d9 NextWork VPC	Owner ID 571600841781		



A new network ACL

By default, my private subnet is associated with the network vpc

I set up a dedicated network ACL for my private subnet because i did not want my private subnet to be connected to the internet

My network has two simple rules to deny all traffic





nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

