



Creating a Private Subnet



mallangiharinathreddy727@gmail.com

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
< > ^ ▾

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) is a service that lets you create a private, isolated section of the Amazon Web Services (AWS) cloud. It's like having your own private network, but in the cloud.

How I used Amazon VPC in this project

In today's I created public and private subnets using amazon VPC.

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

In private subnet, we cannot access the same route table as we created for public subnet.that thing was not expected.

This project took me...

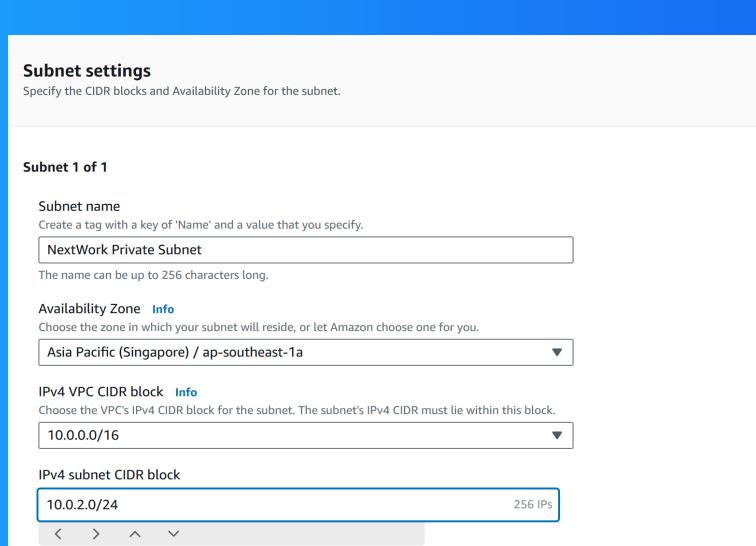
nearly 2 hours.

Private vs Public Subnets

The difference between public and private subnets is that public subnets are accessible by and can access the internet, while private subnets are completely isolated from the internet by default.

'Having private subnets are useful because keeping resources away from the internet is extremely important of confidential resources/data.

My private and public subnets cannot have the same IPv4 CIDR block i.e. the same range of IP addresses. The CIDR block for every subnet must be unique and cannot overlap with other subnets.



A dedicated route table

By default, my private subnet is associated with the default route table i.e. route table that has a route to an internet gateway.

To make my subnet private, I had to set up a new route table because my subnet can't have a route to an internet gateway.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows internal communication i.e. with a destination of another resource within my VPC.

rtb-0e0a069207a09de9d / NextWork Private Route Table				
Details	Routes	Subnet associations	Edge associations	Route propagation
Routes (1)				
<input type="button" value="Filter routes"/> Both ▾ <input type="button" value="Edit routes"/> < 1 > ⚙				
Destination	Target	Status	Propagated	
10.0.0.0/16	local	Active	No	▼

A new network ACL

By default, my private subnet is associated with default network ACL that's set up for every created in my AWS account.

I set up a dedicated network ACL for my private subnet because a network ACL becomes crucial in the event of security breaches.

My new network ACL has two simple rules - deny all inbound and all outbound traffic.

Outbound rules (1)							Edit outbound rules
<input type="text"/> Filter outbound rules							
Rule number	Type	Protocol	Port range	Destination	Allow/Deny	Action	
*	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

