



Creating a Private Subnet



Juncheng Wang

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](#)

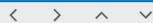
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

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 enables you to build a virtual network in the AWS cloud. You can define your own network space by controlling how your network and the Amazon EC2 resources inside your network are communicating with the internet.

How I used Amazon VPC in this project

I set up a private subnet with associated route table and network ACL.

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

Although setting up a route without an internet gateway would already prevent direct internet access to and from the subnet, setting up a dedicated network ACL is still a crucial practice to prevent internal traffic from public subnet.

This project took me...

1 hour



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.

Having private subnets is useful because keeping resources away from the internet is very important for security when it contains confidential resources and data.

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

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



A dedicated route table

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

I had to set up a new route table because my subnet can't have a route to an internet gateway. I need to make a new one to only allow the local target to make my subnet private.

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

You have successfully updated subnet associations for rtb-01495a686be1c46cb / NextWork-Private-Route-Table.

VPC > Route tables > rtb-01495a686be1c46cb

rtb-01495a686be1c46cb / NextWork-Private-Route-Table

Actions ▾

Details info

| | | | |
|---|--------------------------|--|------------------------|
| Route table ID rtb-01495a686be1c46cb | Main No | Explicit subnet associations subnet-0489a140a8b3d6583 / private-1 | Edge associations - |
| VPC vpc-0ff2f6592aad47c0a NextWork VPC | Owner ID 691784454033 | | |

Routes Subnet associations Edge associations Route propagation Tags

Routes (1) Both ▾ Edit routes

Filter routes

| 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 default network ACL that is set up for every VPC.

I setup a dedicated network ACL for my private subnet because a network ACL helps to prevent security breaches where traffic that has compromised my public subnet can get access to my private subnet if I have network ACL rules that allow all traffic.

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

You have successfully updated subnet associations for `acl-0b6093a191bf2a5a0` / NextWork Private Network ACL.

Details

VPC > Network ACLs > `acl-0b6093a191bf2a5a0` / NextWork Private Network ACL

acl-0b6093a191bf2a5a0 / NextWork Private Network ACL Actions

Details info

| | | | |
|---|---|---------------|--|
| Network ACL ID acl-0b6093a191bf2a5a0 | Associated with subnet-0489a140a8b3d6583 / private-1 | Default No | VPC ID vpc-0ff2f6592aad47c0a / NextWork VPC |
| Owner 691784454033 | | | |

Inbound rules Outbound rules Subnet associations Tags

Inbound rules (1) Edit inbound rules

Filter inbound rules

| 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

