

Creating a Private Subnet

Erik Gonzalez

subnet-086b0142574263411 / nimbus-private-subnet

Actions

Details

Subnet ID

subnet-086b0142574263411

IPv4 CIDR

10.0.1.0/24

Availability Zone

use1-az2 (us-east-1b)

Network ACL

-

Auto-assign customer-owned IPv4 address
No

IPv6 CIDR reservations

-

Resource name DNS AAAA record
Disabled

Subnet ARN

arn:aws:ec2:us-east-1:312831649097:subnet/subnet-086b0142574263411

Available IPv4 addresses

251

Network border group

us-east-1

Default subnet

No

Customer-owned IPv4 pool

-

IPv6-only

No

DNS64

Disabled

State

Available

IPv6 CIDR

-

VPC

vpc-0629ca7556832552b | nimbus-vpc

Auto-assign public IPv4 address

No

Outpost ID

-

Hostname type

IP name

Owner

312831649097

Block Public Access

Off

IPv6 CIDR association ID

-

Route table

rtb-0720941bdb7c35185 | Nimbus-Route-Table

Auto-assign IPv6 address

No

IPv4 CIDR reservations

-

Resource name DNS A record

Disabled

Introducing Today's Project!

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create subnets, routing tables, inbound/outbound rules etc..

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

One thing I didn't expect in this project is how a VPC is already created when setting up an AWS account.

This project took me...










This project took me about one hour to complete.

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 can be completely isolated from the internet.

Having private subnets is useful because keeping resources away from the internet is extremely important for security and 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 so as to not cause any overlap.

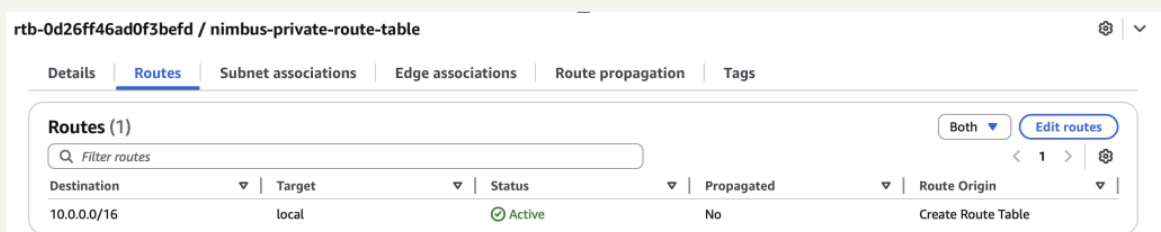
subnet-086b0142574263411 / nimbus-private-subnet			
<div> <div>Details</div> <div> <div> <div>Subnet ID</div> <div>  subnet-086b0142574263411 </div> </div> <div> <div>IPv4 CIDR</div> <div>  10.0.1.0/24 </div> </div> <div> <div>Availability Zone</div> <div>  use1-az2 (us-east-1b) </div> </div> <div> <div>Network ACL</div> <div>-</div> </div> <div> <div>Auto-assign customer-owned IPv4 address</div> <div>No</div> </div> <div> <div>IPv6 CIDR reservations</div> <div>-</div> </div> <div> <div>Resource name DNS AAAA record</div> <div>Disabled</div> </div> </div> </div>			
<div> <div>Subnet ARN</div> <div>  arn:aws:ec2:us-east-1:312831649097:subnet/subnet-086b0142574263411 </div> </div> <div> <div>Available IPv4 addresses</div> <div>  251 </div> </div> <div> <div>Network border group</div> <div>  us-east-1 </div> </div> <div> <div>Default subnet</div> <div>No</div> </div> <div> <div>Customer-owned IPv4 pool</div> <div>-</div> </div> <div> <div>IPv6-only</div> <div>No</div> </div> <div> <div>DNS64</div> <div>Disabled</div> </div>			
<div> <div>State</div> <div>  Available </div> </div> <div> <div>IPv6 CIDR</div> <div>-</div> </div> <div> <div>VPC</div> <div> vpc-0629ca7556832552b nimbus-vpc </div> </div> <div> <div>Auto-assign public IPv4 address</div> <div>No</div> </div> <div> <div>Outpost ID</div> <div>-</div> </div> <div> <div>Hostname type</div> <div>IP name</div> </div> <div> <div>Owner</div> <div>  312831649097 </div> </div>			
<div> <div>Block Public Access</div> <div>  Off </div> </div> <div> <div>IPv6 CIDR association ID</div> <div>-</div> </div> <div> <div>Route table</div> <div> rtb-0720941bdb7c35185 Nimbus-Route-Table </div> </div> <div> <div>Auto-assign IPv6 address</div> <div>No</div> </div> <div> <div>IPv4 CIDR reservations</div> <div>-</div> </div> <div> <div>Resource name DNS A record</div> <div>Disabled</div> </div>			

A Dedicated Route Table

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

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 another destination of another resource within my VPC.



The screenshot shows the AWS Management Console interface for a route table. The title bar reads 'rtb-0d26ff46ad0f3befd / nimbus-private-route-table'. Below the title bar are tabs for 'Details', 'Routes' (which is selected), 'Subnet associations', 'Edge associations', 'Route propagation', and 'Tags'. The 'Routes' tab displays a table with one route. The table has columns for 'Destination', 'Target', 'Status', 'Propagated', and 'Route Origin'. The single route has a destination of '10.0.0.0/16', a target of 'local', a status of 'Active' (indicated by a green checkmark), and is not propagated. There is a 'Create Route Table' link at the bottom right of the table.

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	Create Route Table

A New Network ACL

By default, my private subnet is associated with the default network ACL that's set up for every VPC 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—where traffic that has compromised my public subnet could access my private subnet if my network ACL rules allow all inbound and outbound traffic.

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

