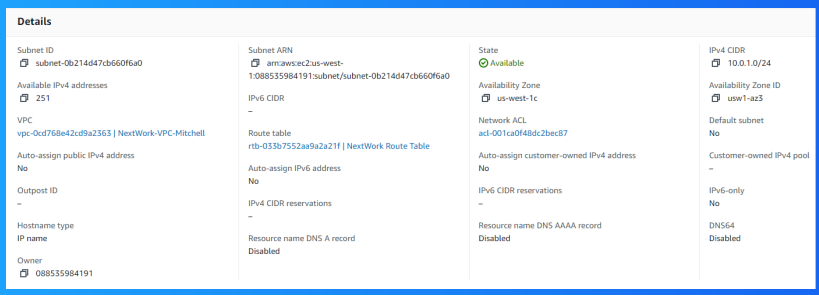
NextWork.org

Creating a Private Subnet

mmoorejr24@gmail.com



Details

Subnet ID subnet-0b214d47cb660f6a0	Subnet ARN arn:aws:ec2:us-west-1:088535984191:subnet/subnet-0b214d47cb660f6a0	State Available	IPv4 CIDR 10.0.1.0/24
Available IPv4 addresses 251	IPv6 CIDR –	Availability Zone us-west-1c	Availability Zone ID usw1-az3
VPC vpc-0cd768e42cd9a2363 | NextWork-VPC-Mitchell	Route table rtb-033b7552aa9a2a21f | NextWork Route Table	Network ACL acl-001ca0f48dc2bec87	Default subnet No
Auto-assign public IPv4 address No	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No	Customer-owned IPv4 pool –
Outpost ID –	IPv4 CIDR reservations –	IPv6 CIDR reservations –	IPv6-only No
Hostname type IP name	Resource name DNS A record Disabled	Resource name DNS AAAA record Disabled	DNS64 Disabled
Owner 088535984191			

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a virtual private cloud that is secure, isolated private cloud hosted within a public cloud. Customers can run code, store data, host websites, etc.

How I used Amazon VPC in this project

I used Amazon VPC to setup a public and private subnets with security on the route tables and network ACLs.

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

I didn't expect this project to be as straight forward as it was.

This project took me...

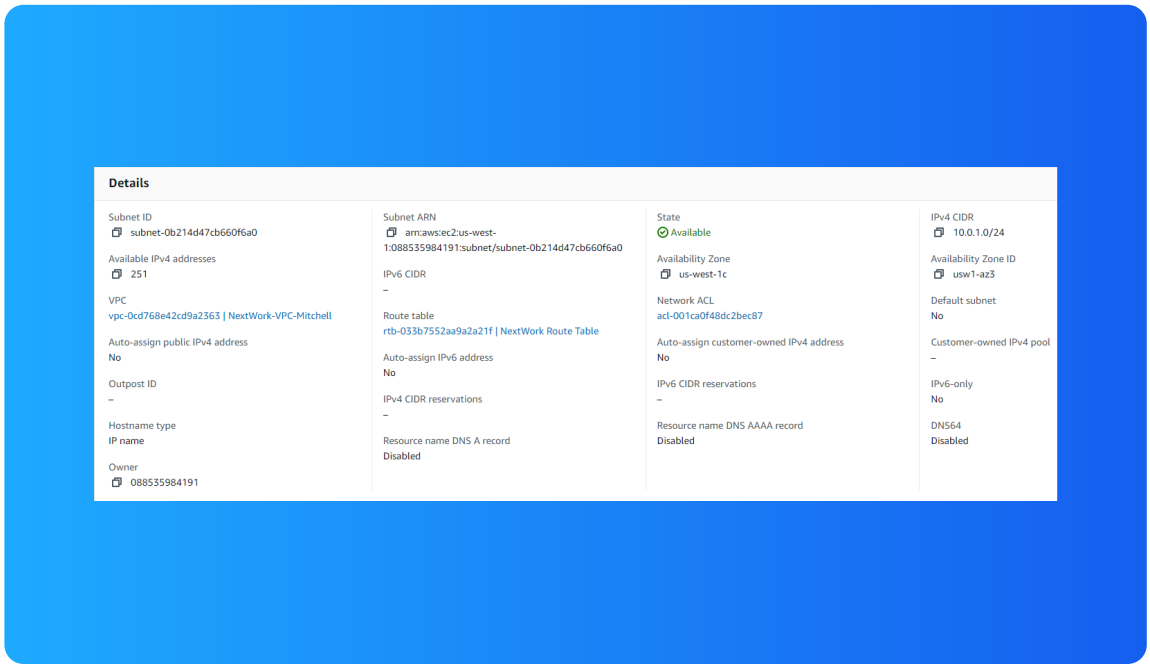
This project took me about an hour and 40 mins to complete.

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 are completely isolated from the internet by default.

Having private subnets are useful because keeping resources away from the internet is extremely important for the security 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 another subnet.



Details

Subnet ID
subnet-0b214d47cb660f6a0

Available IPv4 addresses
251

VPC
vpc-0cd768e42cd9a2363 | NextWork-VPC-Mitchell

Auto-assign public IPv4 address
No

Outpost ID
–

Hostname type
IP name

Owner
088535984191

Subnet ARN
arn:aws:ec2:us-west-1:088535984191:subnet/subnet-0b214d47cb660f6a0

IPv6 CIDR
–

Route table
rtb-033b7552aa9a2a21f | NextWork Route Table

Auto-assign IPv6 address
No

IPv4 CIDR reservations
–

Resource name DNS A record
Disabled

State
Available

Availability Zone
us-west-1c

Network ACL
acl-001ca0f48dc2bec87

Auto-assign customer-owned IPv4 address
No

IPv6 CIDR reservations
–

Resource name DNS AAAA record
Disabled

IPv4 CIDR
10.0.1.0/24

Availability Zone ID
usw1-az3

Default subnet
No

Customer-owned IPv4 pool
–

IPv6-only
No

DNS64
Disabled

mmoorejr24@gmail.com
NextWork Student

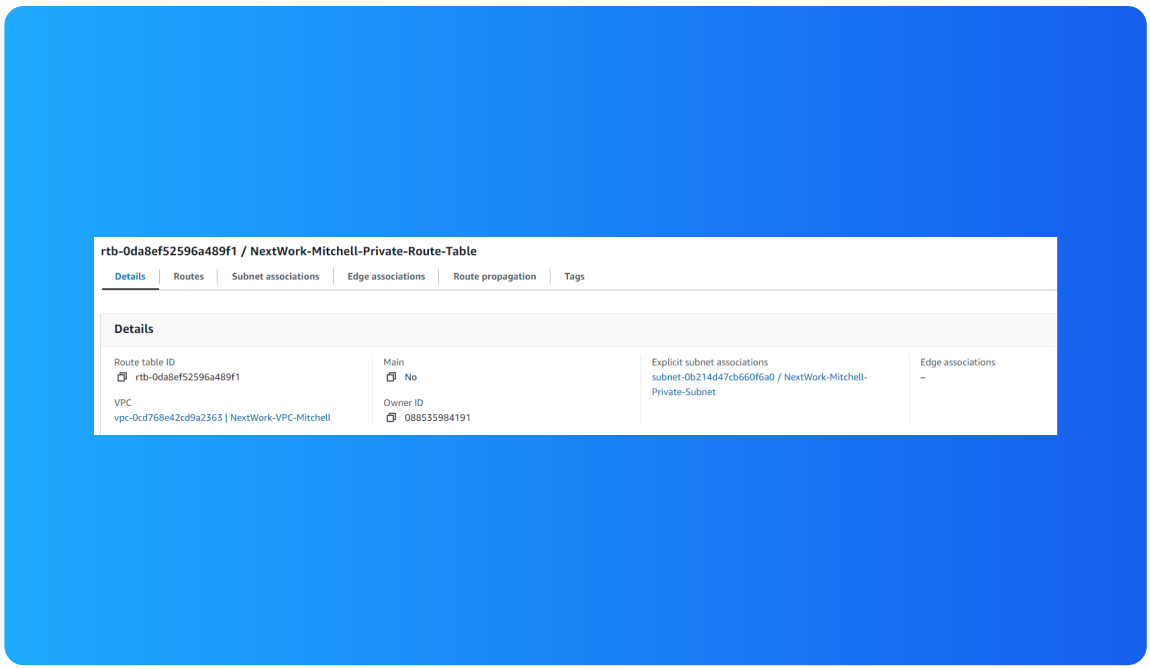
NextWork.org

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.

I had to set up a new route table because my private subnet can not 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.



mmoorejr24@gmail.com
NextWork Student

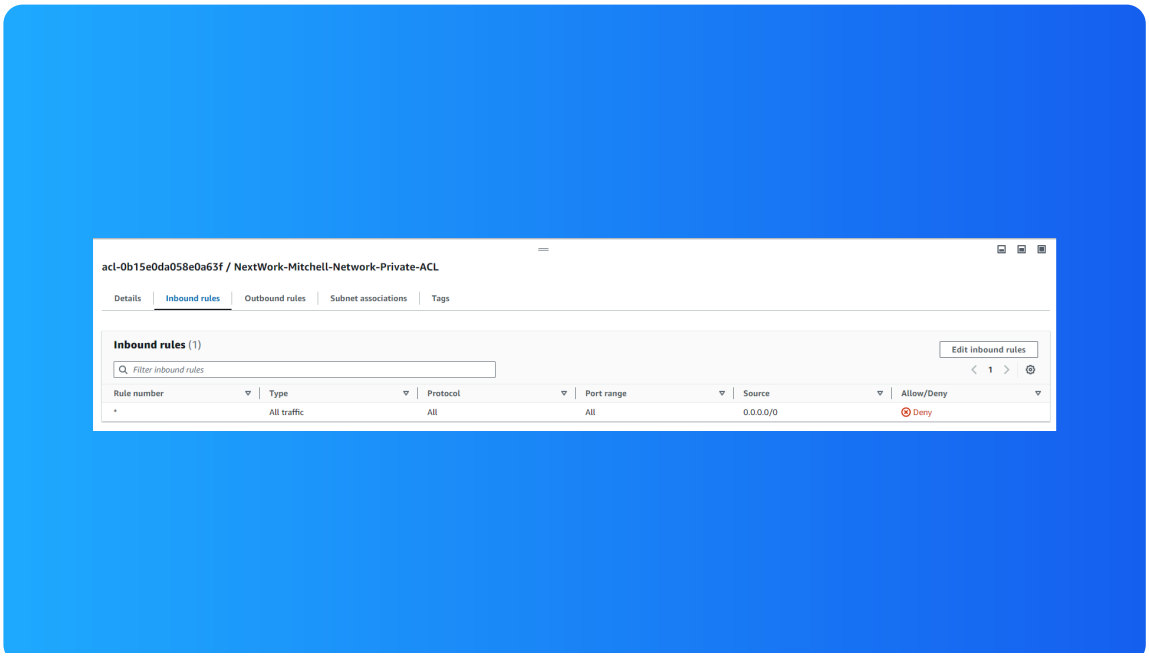
NextWork.org

A new network ACL

By default, my private subnet is associated with the default network ACL that's setup with every VPC created in my AWS account.

I set up a dedicated network ACL for my private subnet because in the event of 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 inbound/outbound traffic.

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



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects