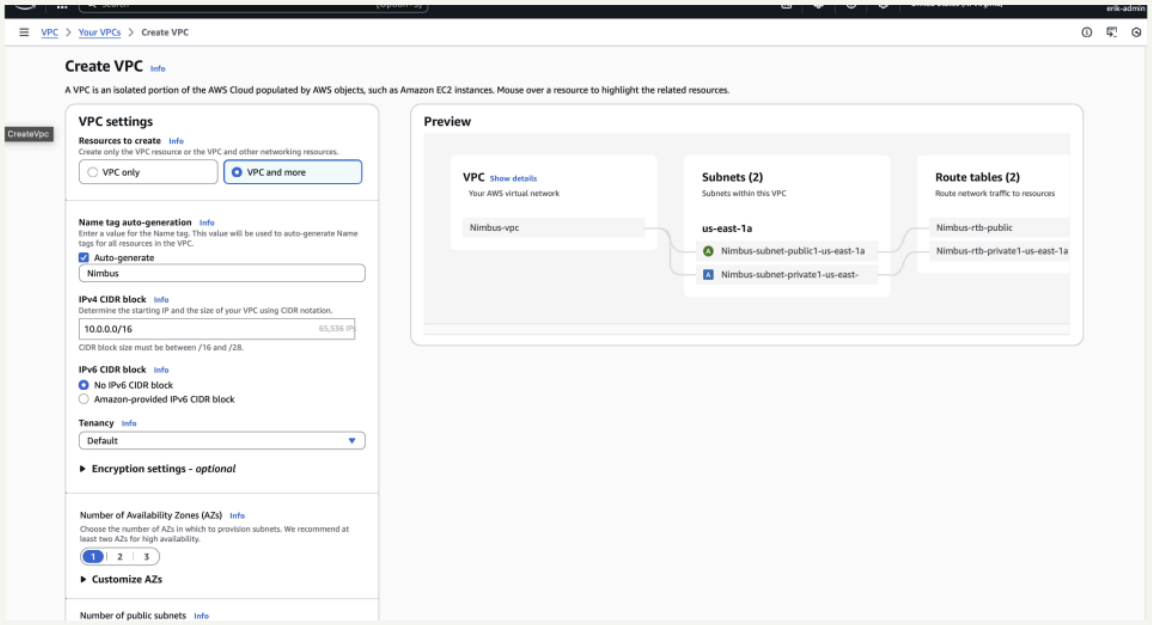
Launching VPC Resources

Erik Gonzalez



Introducing Today's Project!

How I used Amazon VPC in this project

I used Amazon VPC to create public and private subnets and other resources that I will continue to use in this VPC project.

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

One thing I didn't expect in this project was that you only have options for no AZ or 1 AZ.

This project took me...

This project took me a little over an hour to complete.

Setting Up Direct VMAccess

Directly accessing a virtual machine means logging into the EC2 instance instead of just managing it on a higher level with the AWS management console. This includes operations like installing software and changing my EC2 instances configurations.

SSH is a key method for directly accessing a VM

SSH traffic means Secure Shell and it is both a protocol and a traffic type. It is a protocol that matches key pairs, and enables direct VM access, and once a connection is set up, it is a traffic type that encrypts communication data being transferred.

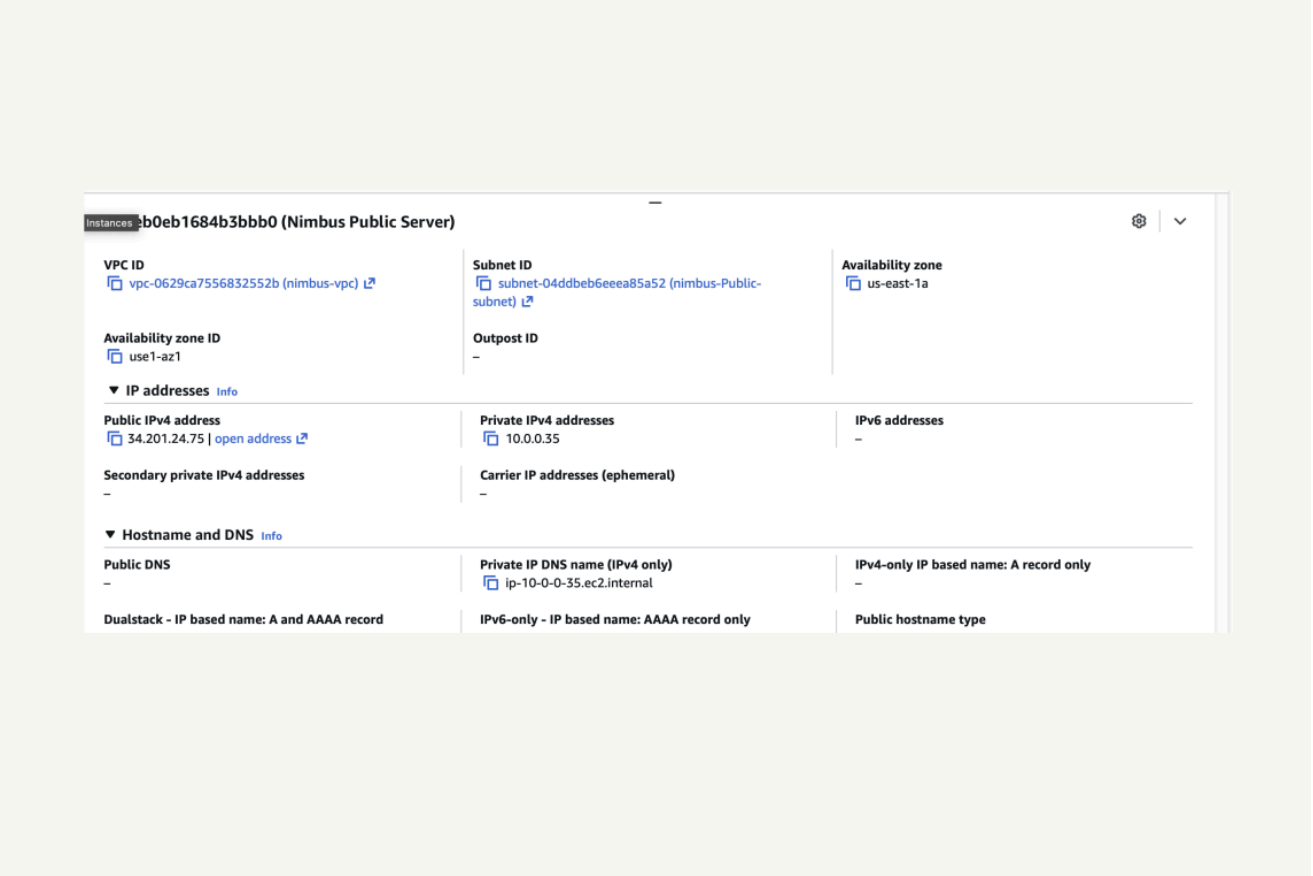
To enable direct access, I set up key pairs

Key pairs are tools that help developers and engineers authenticate themselves when trying to get direct access to virtual machines e.g. an EC2 instance. Key pairs work by having two private keys - a private key for the VM and a matching private key for the resource/user!

A private key's file format means the file type that my key is stored in. My private key's file format was .pem which is a widely accepted file format that most servers can read/use.

Launching a public server

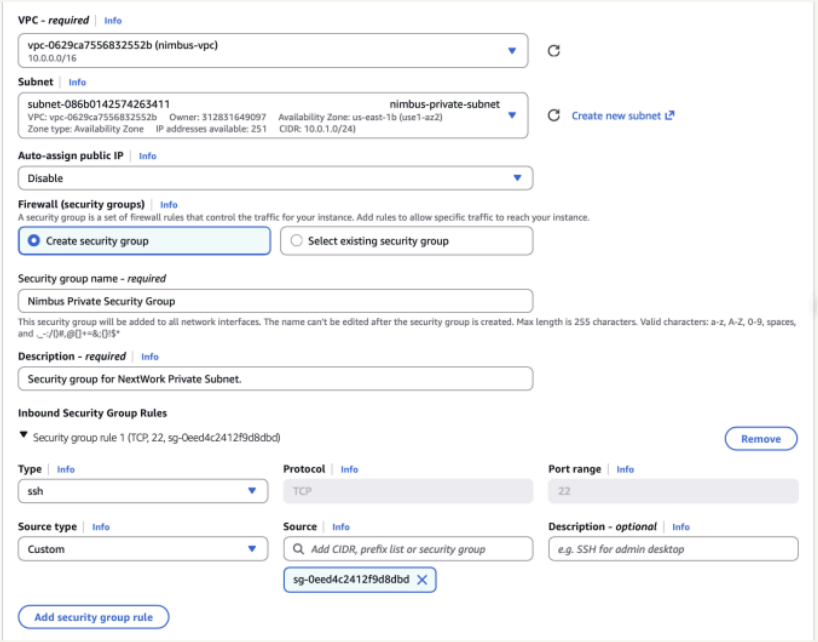
I had to change my EC2 instance's networking settings by changing the VPC and the subnet my EC2 instance was going to launch in. I updated both to my VPC and my public subnet respectively. I also used my existing public security.



Launching a private server

My private server has its own dedicated security group because the security group allows all HTTP traffic - which would leave my private server much more vulnerable to security attacks/risks.

My private server's security group's source is nimbus security group which means only SSH traffic coming from resources associated with that security group would be allowed.

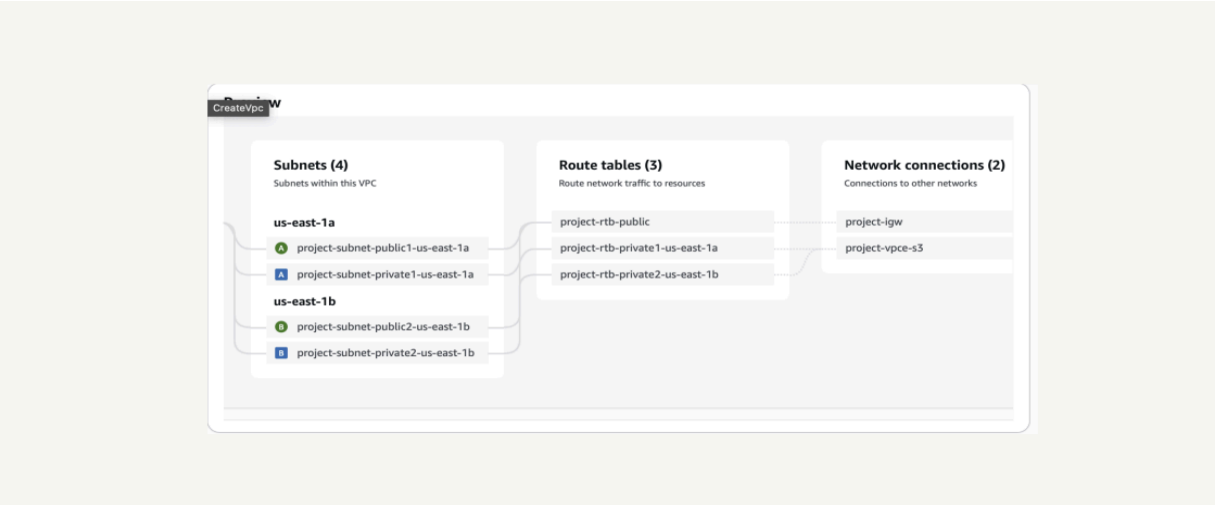


Speeding up VPC creation

I used an alternative way to set up an Amazon VPC! This time, I chose the 'VPC and More' option which gave me a VPC resource map to use when creating the VPC and all of its components e.g. security groups, route tables, internet gateways.

A VPC resource map is a visual diagram that maps out all my VPC components and the relationship/communications between them. A resource map is interactive, it will highlight the connections relevant to a resource that I highlight or hover over.

My new VPC has a CIDR block of 10.0.0.0/16 It is possible for my new VPC to have the same IPv4 CIDR block as my existing VPC because VPCs are already isolated from each other. Still, this is not best practice if we need VPC peering.



Speeding up VPC creation

Tips for using the VPC resource map

When determining the number of public subnets in my VPC, I only had two options: either none, or one in each availability zone. This was because it is best practice to have at least one subnet/AZ

The set up page also offered to create NAT gateways, which are connector gateways that will let resources in my private subnet get access to the internet (e.g. for security updates) while still blocking incoming traffic from the internet.