



Launching VPC Resources

R

Roshan Shrestha

The screenshot shows the 'Create VPC' wizard in the AWS Management Console. On the left, the 'VPC settings' section includes fields for Name (auto-generated), Subnet range (10.0.0.0/16), and Availability Zones (us-east-2a and us-east-2b). On the right, the 'Preview' section shows a hierarchical tree of resources:

- VPC:** Your AWS virtual network (name: nextrwork-vpc)
- Subnets (6):** Subnets within this VPC
 - us-east-2a
 - nextrwork-rtb-public
 - nextrwork-subnet-public1-us-east-2a
 - nextrwork-subnet-private1-us-east-2a
 - nextrwork-subnet-private2-us-east-2a
 - nextrwork-subnet-private3-us-east-2a
 - nextrwork-subnet-private4-us-east-2a
 - us-east-2b
 - nextrwork-rtb-public
 - nextrwork-subnet-public1-us-east-2b
 - nextrwork-subnet-private1-us-east-2b
 - nextrwork-subnet-private2-us-east-2b
 - nextrwork-subnet-private3-us-east-2b
 - nextrwork-subnet-private4-us-east-2b
- Route tables (5):** Route network traffic to resources
 - nextrwork-rtb-public
 - nextrwork-rtb-private1-us-east-2a
 - nextrwork-rtb-private2-us-east-2a
 - nextrwork-rtb-private3-us-east-2a
 - nextrwork-rtb-private4-us-east-2b
- Network connectio:** Connections to other network
 - nextrwork-igw
 - nextrwork-vpc-s5

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a space within the Amazon cloudspace that is allocated to us and helps us isolate and identify our resources from other resources.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to launch EC2 instances in both public and private subnets in my VPC. I also used the VPC & more option to create VPC along with the subnets, routes, and network connections for that VPC.

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

The VPC resource map and the ease to create VPC using the VPC & more option.

This project took me...

This project took me about an hour.

Setting Up Direct VM Access

Directly accessing a virtual machine means logging into a VM and using it as if it is right in front of you but through the internet.

SSH is a key method for directly accessing a VM

SSH traffic means encrypted traffic that uses the Secure Shell protocol.

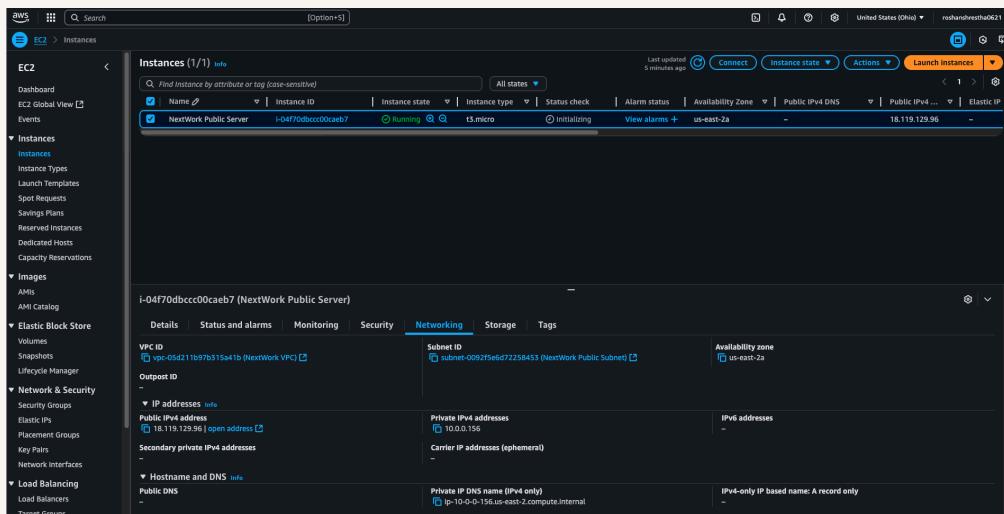
To enable direct access, I set up key pairs

Key pairs are security keys that allow us access. Public key stays with the resource and we have the private key which is used to validate access.

A private key's file format means the format that the key is saved in. Eg: PDF, PEM, etc. My private key's file format was .pem (privacy enhanced mail).

Launching a public server

I had to change my EC2 instance's networking settings by choosing to create it in the NextWork VPC instead of the default VPC. The public subnet in NextWork VPC and use the NextWork Public Security Group.

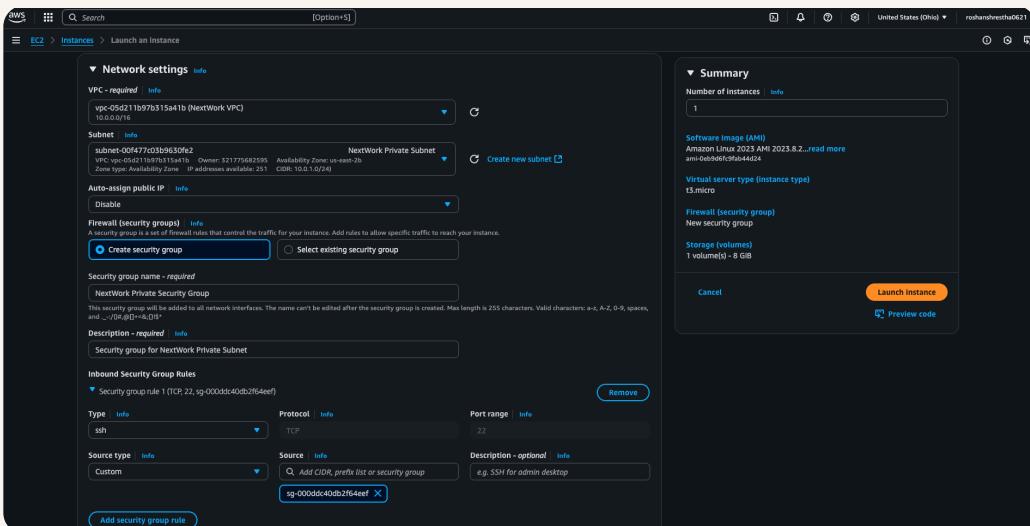




Launching a private server

My private server has its own dedicated security group because we don't want to allow all IP addresses to access our private resources but limit the access to a known list of IP addresses

My private server's security group's source is NextWork Public Security Group which means that only the resources that are part of the NextWork Public Security group can communicate with my resources in the private server's security group.

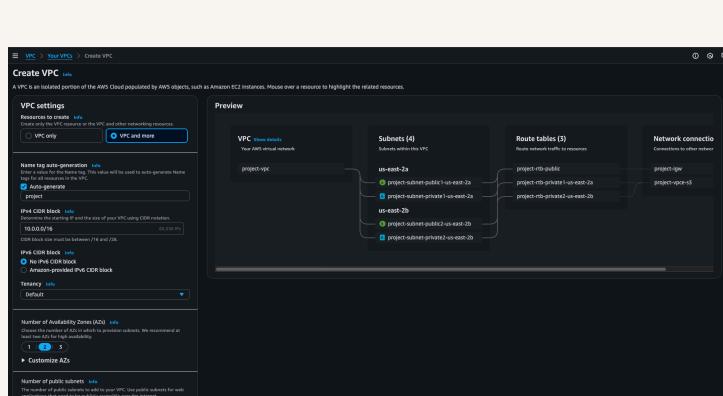


Speeding up VPC creation

I used an alternative way to set up an Amazon VPC! This time, I used the VPC and more option which allows us to create the VPC along with the public/private subnets, route tables, and network connections.

A VPC resource map is an overview of the subnets, routes, and network connections within that VPC.

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 AWS isolates one VPC from another. Use different CIDR blocks if you plan to enable communication between two VPCs.

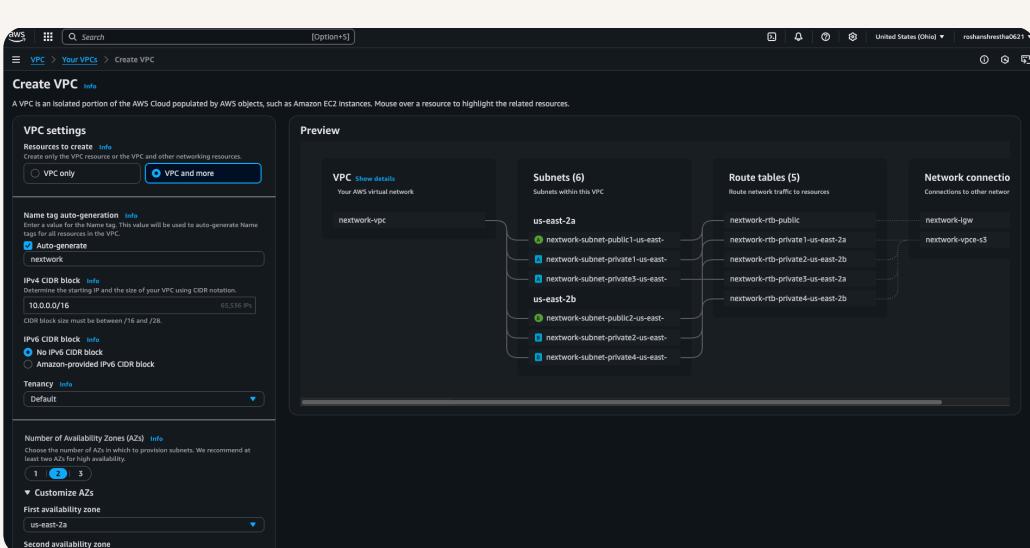


Speeding up VPC creation

Tips for using the VPC resource map

When determining the number of public subnets in my VPC, I only had two options 0 or 2. This was because AWS allows us to create one public subnet per availability zone to keep things simple in this step. You can always add more manually.

The setup page offered to create NAT gateways, which are gateways that allow private subnets to access the internet for updates & patches, while blocking inbound traffic. It handles translation to a public IP and keeps the subnet's private IP hidden.





nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

