



Launching VPC Resources



Sai Prasanth Reddy

The screenshot shows the 'Create VPC' interface on the AWS Management Console. On the left, the 'VPC settings' section includes fields for 'Name tag auto-generation' (set to 'Auto-generate'), 'IPv4 CIDR block' (set to '10.0.0.0/16'), and 'IPv6 CIDR block' (set to 'No IPv6 CIDR block'). The 'Tenancy' dropdown is set to 'Default'. On the right, the 'Preview' section displays the resulting VPC structure:

- VPC show details:** Your AWS virtual network named 'nextwork'.
- Subnets (6):** Subnets within this VPC, grouped into two AZs:
 - us-east-1a:** Contains three subnets: 'Public subnet without N', 'Private subnet without N', and 'Private subnet without N'.
 - us-east-1b:** Contains three subnets: 'Public subnet without N', 'Private subnet without N', and 'Private subnet without N'.
- Route tables (5):** Route network traffic to resources, connected to the subnets.
- Network connection:** Connections to other networks, including an Internet gateway and a VPC endpoint.



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a service that lets you create isolated cloud networks in AWS. It's useful because it provides control over networking, including IP ranges, subnets, and security, enabling secure, scalable, and customizable cloud infrastructure.

How I used Amazon VPC in this project

I used Amazon VPC in today's project to create a new VPC, set up public and private subnets, configured route tables, and attached an internet gateway for the public subnet, ensuring secure and isolated network communication for my EC2 instances.

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

One thing I didn't expect in this project was the need to configure different security groups for my public and private subnets to manage traffic rules, ensuring secure communication between instances while maintaining isolation.

This project took me...

This project took me about an hour, mainly due to setting up the VPC, configuring the subnets, route tables, and adjusting security groups for proper network and instance access control.



Sai Prasanth Reddy

NextWork Student

NextWork.org

Setting Up Direct VM Access

Directly accessing a virtual machine means connecting to your EC2 instance via SSH or RDP using a key pair, allowing you to interact with the instance, manage software, and perform configurations as if you were physically on the machine.

SSH is a key method for directly accessing a VM

SSH traffic means secure communication between a client and a server over the internet using the Secure Shell protocol. It enables encrypted remote access to EC2 instances or other servers for managing and configuring them securely.

To enable direct access, I set up key pairs

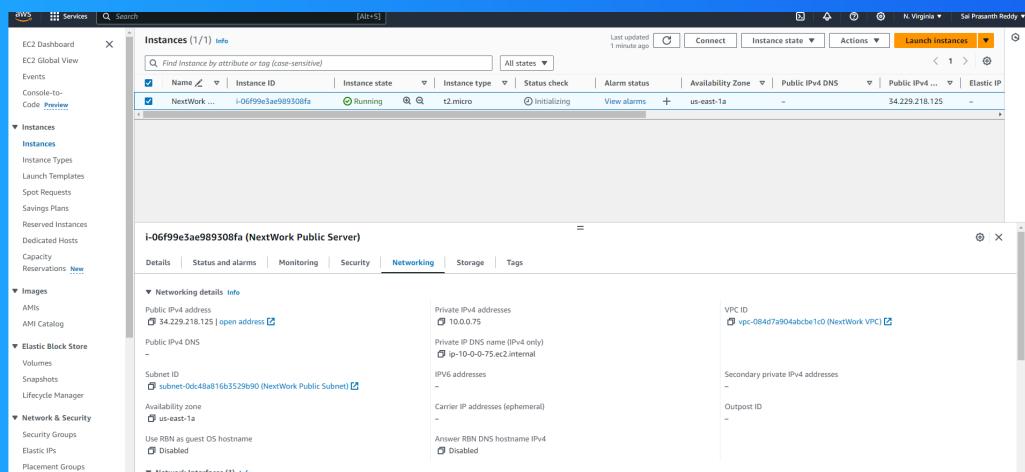
Key pairs are cryptographic security credentials used to authenticate access to instances. They consist of a public key stored by AWS and a private key that you download, which allows secure SSH access to your EC2 instances.

A private key's file format means the type of encoding used for the key, typically for secure access. My private key's file format was .pem, which is commonly used for SSH access to EC2 instances in AWS.



Launching a public server

I had to change my EC2 instance's networking settings by editing it to be part of my VPC and assigning it to the public subnet, allowing it to connect to the internet through the VPC's internet gateway.





Launching a private server

My private server has its own dedicated security group because it needs stricter access controls, allowing only internal VPC traffic and preventing direct internet access, unlike the public server, which requires broader external access.

My private server's security group's source is my public security group, which means only instances in the public subnet with that security group can communicate with the private server, ensuring secure internal communication.

The screenshot shows the AWS CloudFormation Launch Wizard interface. On the left, the 'Firewall (security groups)' section is active, displaying a configuration for a new security group named 'NextWork Private Security Group'. It includes an inbound rule for port 22 (TCP) from a specific security group ('sg-0cd2e1c60a35616ab'). On the right, the 'Summary' section shows the instance configuration: 1 instance, Amazon Linux 2023 AMI 2023.5.2, t2.micro instance type, and 1 volume(s) - 8 GiB storage. A tooltip for the free tier is visible, stating: 'Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GiB of bandwidth to the internet.' At the bottom right, there are 'Cancel' and 'Launch instance' buttons.

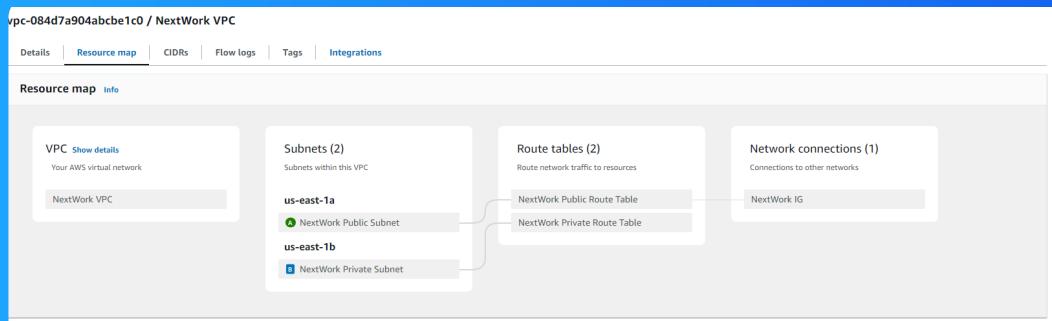


Speeding up VPC creation

I used an alternative way to set up an Amazon VPC! This time, I used the "VPC and more" option in the AWS VPC dashboard to create a new VPC, along with subnets, route tables, and an internet gateway for better network management.

A VPC resource map is a visual representation of all the resources within your VPC, such as subnets, route tables, internet gateways, and instances, helping you understand and manage the relationships and configurations of your network components.

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 they are isolated from each other and do not share routes, preventing any IP address conflicts.





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: one for each Availability Zone. This was because each public subnet must map to a distinct AZ to ensure high availability and fault tolerance across the VPC.

The setup page also offered to create NAT gateways, which are services that enable instances in private subnets to connect to the internet for outbound traffic while preventing inbound traffic from the internet, maintaining security.

The screenshot shows the 'Create VPC' setup page. On the left, the 'VPC settings' section includes fields for 'Resources to create' (set to 'VPC and more'), 'Name tag auto-generation' (set to 'Auto-generate'), 'IPv4 CIDR block' (set to '10.0.0.0/16'), 'IPv6 CIDR block' (set to 'No IPv6 CIDR block'), 'Tenancy' (set to 'Default'), and 'Number of Availability Zones (AZs)' (set to '2'). On the right, the 'Preview' section displays a hierarchical resource map. It starts with a 'VPC' node, which branches into 'Subnets (6)', 'Route tables (5)', and 'Network connection'. The 'Subnets' section shows two AZs: 'us-east-1a' and 'us-east-1b', each containing three subnets. The 'Route tables' section shows five route tables, each associated with a specific subnet. The 'Network connection' section shows an 'Internet gateway without N' and a 'VPC endpoint without N'.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for
more projects

