



Launching VPC Resources



Sanjana Tripathy

Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.

VPC settings

Resources to create [Info](#)
Create only the VPC, resources in the VPC, and their underlying resources
 VPC only VPC and more

Name tag auto-generation [Info](#)
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.
 Auto-generate
NextWork

IPv4 CDR block [Info](#)
Determines the starting IP and the size of your VPC using CIDR notation
 No IPv4 CDR block (16.774.192.0/18)
CIDR block size must be between /16 and /28

IPv6 CDR block [Info](#)
 No IPv6 CDR block
 Amazon provided IPv6 CDR block

Tenancy [Info](#)
 Default

Number of Availability Zones (AZs) [Info](#)
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.
 1 2 3
Customize AZs

First availability zone [Info](#)
ap-south-1a

Second availability zone [Info](#)
ap-south-1b

Number of public subnets [Info](#)
The number of public subnets to add to your VPC. Use public subnets to connect to the public internet or to privately accessible over the internet.
 0 1 2

Number of private subnets [Info](#)
The number of private subnets to add to your VPC. Use private subnets to connect to other VPCs and other private endpoints.

0 1 2 3

► Customize subnets CIDR blocks

NAT gateways (1) [Info](#)
A NAT gateway translates private IP addresses from one AZ in a VPC to create NAT gateways. Note that there is a charge for each NAT gateway.
 None 1 per AZ

VPC endpoints [Info](#)
Endpoints can help reduce NAT gateway charges and improve security by connecting directly to the VPC. By default, full access policy is used. You can change the policy at any time.

None 1 per endpoint

DNS options [Info](#)
 Enable DNS Hostnames
 Enable DNS resolution

► Additional tags

[Cancel](#) [Preview code](#) [Create VPC](#)

Preview

VPC [Show details](#)
Use AWS virtual network

Subnets (6)
Subnets within this VPC

NextWork-vpc

ap-south-1a
NextWork-subnet-public1-ap-south-1a
NextWork-subnet-private1-ap-south-1a
NextWork-subnet-private2-ap-south-1a
NextWork-subnet-private3-ap-south-1a
NextWork-subnet-private4-ap-south-1a

ap-south-1b
NextWork-subnet-public2-ap-south-1b
NextWork-subnet-private2-ap-south-1b
NextWork-subnet-private3-ap-south-1b
NextWork-subnet-private4-ap-south-1b

Route tables (5)
Route network traffic to resources

NextWork-rtb-public
NextWork-rtb-private1-ap-south-1a
NextWork-rtb-private2-ap-south-1a
NextWork-rtb-private3-ap-south-1a
NextWork-rtb-private4-ap-south-1a

Network connections (2)
Connections to other resources

NextWork-igw
NextWork-vpcx-1



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) lets you launch AWS resources in a secure, isolated network you define. It gives control over IP ranges, subnets, route tables, and gateways, enabling you to securely build and manage cloud infrastructure.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to quickly set up a secure network with public and private subnets. I launched instances in each, configured route tables and gateways, enabling isolated access control.

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

One thing I didn't expect in this project was being able to complete a full VPC setup—subnets, route tables, gateways, and more—in just a few minutes. I was excited to see how seamlessly AWS enables quick and secure network configuration.



Sanjana Tripathy
NextWork Student

nextwork.org

This project took me...

This project took me approximately 3 hours to complete, including setting up the VPC, configuring subnets, route tables, gateways, and security components, along with reviewing and validating each step for a clear understanding.

Setting Up Direct VM Access

Directly accessing an EC2 instance means logging into its operating system via SSH or RDP to perform admin-level tasks like installing software or running scripts. Unlike the AWS Console, this gives you full control for deep configuration.

SSH is a key method for directly accessing a VM

SSH (Secure Shell) is a secure protocol used to remotely access and manage servers over a network. It encrypts the connection, allowing users to safely run commands, transfer files, and configure systems like EC2 instances from their local machines.

To enable direct access, I set up key pairs

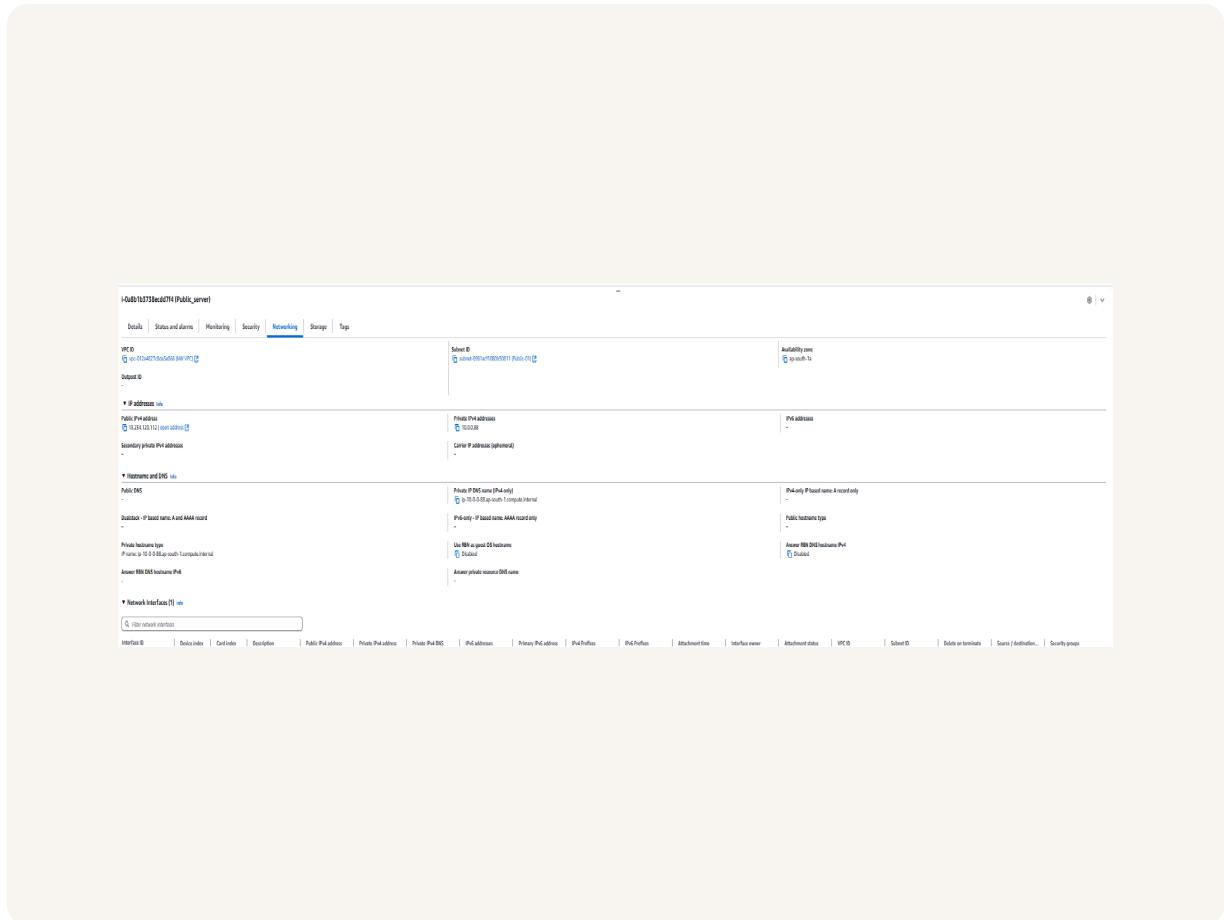
A key pair in AWS is a set of two cryptographic keys: a public key and a private key. The public key is stored by AWS, while the private key is downloaded by the user and used to securely connect (SSH) to EC2 instances.

A private key is usually stored in PEM format with a .pem file extension. This format is widely used for SSH access to EC2 instances. In my case, the private key was in .pem format, which is required for Linux-based EC2 connections using SSH.



Launching a public server

By default, all resources are launched into the default VPC that AWS has set up for your account. So to change that, I had to change my EC2 instance's networking settings by selecting the VPC, subnet and security group(Firewall) which I created.





Launching a private server

The private server uses a different security group from the one used by the public subnet's instances(NZ_SecurityGroup_Public) This limits access, allowing only trusted internal communication and blocking public internet traffic for added security.

My new security group's source is the NZ_SecurityGroup_Public.This means only instances associated with that public security group can send traffic to the private instance, ensuring secure, internal communication only.

The screenshot shows the 'Network settings' section of the AWS VPC configuration for a private subnet. Key details include:

- VPC - required:** vpc-012a4827c8da5e066 (NW VPC)
- Subnet:** Private_01 (subnet-08c5ae75f4473e69)
- Auto-assign public IP:** Disable
- Firewall (security groups):** A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
 - Create security group:** Selected
 - Select existing security group:** Not selected
- Security group name - required:** Private_SecurityGroup
- Description - required:** Security group for private subnet
- Inbound Security Group Rules:** Security group rule 1 (TCP 22, sg-08681513469990a3a)
 - Type:** ssh
 - Protocol:** TCP
 - Port range:** 22
 - Source type:** Custom
 - Source:** sg-08681513469990a3a
 - Description - optional:** e.g. SSH for admin desktop

Speeding up VPC creation

I set up my new VPC using the Launch Instance wizard, which allowed me to configure the VPC, subnets, route tables, and security settings all in one place—quickly setting up a complete VPC environment without switching pages.

A VPC resource map is a visual diagram in the AWS Console that shows all the components inside your VPC—like subnets, route tables, internet gateways, NAT gateways, and more—and how they're connected.

My new VPC can have the same IPv4 CIDR block as the NextWork VPC because VPCs are isolated from each other. Even with overlapping IP ranges, they don't conflict unless connected (like through peering), where unique CIDRs are then required.





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 because I selected two Availability Zones during setup. AWS creates one public subnet per AZ to ensure high availability and redundancy, following best practices.

NAT gateways allow instances in private subnets to access the internet for updates or downloads, while preventing inbound traffic from reaching them. This keeps resources secure while enabling necessary outbound communication.

The screenshot shows the 'Create VPC' wizard in the AWS Management Console. On the left, the 'VPC settings' section includes fields for 'Name tag auto-generation' (set to 'VPC only'), 'CIDR block' (set to '10.0.0.0/16'), and 'Tenancy' (set to 'Default'). Under 'Number of Availability Zones (AZs)', it says 'Two Availability Zones are required for high availability and redundancy. We recommend at least three Availability Zones for optimal performance and fault tolerance.' The 'Customize AZs' section shows 'First availability zone' as 'ap-south-1a' and 'Second availability zone' as 'ap-south-1b'. The 'Number of public subnets' field is set to '1'. The 'Number of private subnets' field is set to '2'. The 'Customize subnet CIDR blocks' section shows 'NET gateway ID' set to '1'. The 'VPC endpoints' section has 'None' selected. The 'DNS options' section includes 'Enable DNS hostnames' and 'Enable DNS support for VPC endpoints'. At the bottom, there are 'Cancel', 'Preview only', and 'Create VPC' buttons.



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

