

# Launching VPC Resources

RA

Ranjith D B

**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 resource or the VPC and other networking 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 CIDR block** Info  
Determine the starting IP and the size of your VPC using CIDR notation.  
10.0.0.0/16 65,536 IPs

**IPv6 CIDR block** Info  
 No IPv6 CIDR block  
 Amazon-provided IPv6 CIDR 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

**Number of public subnets** Info  
The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.  
0  1

**Number of private subnets** Info  
The number of private subnets to add to your VPC. Use private subnets to segment backends or services that don't need public access.  
0  1  2

**Preview**

Your AWS virtual network

The diagram illustrates the VPC structure. It shows a central 'Subnets (6)' section with two groups: 'ap-south-1a' and 'ap-south-1b'. Each group contains three subnets: 'public', 'private1', and 'private2'. Arrows point from these subnets to a 'Route tables (5)' section, which then connects to a 'Network connections (2)' section. The 'Network connections' section includes 'network-igw' and 'network-vpc-e-s3'.

**Subnets (6)**  
Subnets within this VPC

**Route tables (5)**  
Route network traffic to resources

**Network connections (2)**  
Connections to other networks

# Introducing Today's Project!

## What is Amazon VPC?

Amazon VPC is a virtual private cloud that allows you to create an isolated network within AWS. It provides control over IP ranges, subnets, and routing, enabling secure communication and resource segmentation for cloud deployments.

## How I used Amazon VPC in this project

I used Amazon VPC to create a private and public subnet, configure routing, and restrict access using security groups. I also customized CIDR blocks, skipped NAT gateways, and ensured secure communication between my EC2 instances.

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

One thing I didn't expect in this project was how changing the number of availability zones directly impacted the number of subnets and route tables. It helped me understand how AWS dynamically adjusts resources for reliability.

 RA

Ranjith D B  
NextWork Student

[NextWork.org](http://NextWork.org)

---

## This project took me...

This project took me about an hour. Setting up the VPC and subnets was straightforward, but fine-tuning the security groups and understanding NAT gateways took extra time to ensure the correct configurations were in place.

# Setting Up Direct VM Access

Directly accessing a virtual machine means logging into and managing the operating system remotely, using SSH or RDP, as if you were physically in front of it.

## SSH is a key method for directly accessing a VM

SSH traffic means encrypted communication between a client and a remote machine, allowing secure remote access to manage and control servers like EC2 instances.

## To enable direct access, I set up key pairs

Key pairs are cryptographic credentials used to securely access EC2 instances. They consist of a public key stored on the instance and a private key held by the user for authentication.

A private key's file format means the encoding used to store the key. My private key's file format was .pem, which is widely used for secure key storage.

 RA

Ranjith D B  
NextWork Student

[NextWork.org](http://NextWork.org)

---

# Launching a public server

I had to change my EC2 instance's networking settings by selecting NextWork VPC, choosing the public subnet, and assigning the NextWork Public Security Group.

RA

Ranjith D B  
NextWork Student

[NextWork.org](https://NextWork.org)

<b>▼ Networking details <small>info</small></b>	
<b>Public IPv4 address</b>	<a href="#">35.154.241.228</a>   open address <a href="#">🔗</a>
<b>Public IPv4 DNS</b>	–
<b>Subnet ID</b>	<a href="#">subnet-0f0004c732c11df74 (NextWork Public Subnet)</a> <a href="#">🔗</a>
<b>Availability zone</b>	<a href="#">ap-south-1a</a>
<b>Use RBN as guest OS hostname</b>	<input type="checkbox"/> Disabled
<b>Private IPv4 addresses</b>	<a href="#">10.0.0.86</a>
<b>Private IP DNS name (IPv4 only)</b>	<a href="#">ip-10-0-0-86.ap-south-1.compute.internal</a>
<b>IPv6 addresses</b>	–
<b>Carrier IP addresses (ephemeral)</b>	–
<b>Answer RBN DNS hostname IPv4</b>	<input type="checkbox"/> Disabled
<b>VPC ID</b>	<a href="#">vpc-06d350679a164ef2d (NextWork VPC)</a> <a href="#">🔗</a>
<b>Secondary private IPv4 addresses</b>	–
<b>Outpost ID</b>	–

# Launching a private server

My private server has its own dedicated security group because it needs stricter access controls, allowing only connections from trusted resources in the public subnet instead of open internet access.

My private server's security group's source is NextWork Public Security Group, which means only instances within that security group can communicate with the private instance, keeping it isolated from external traffic.

The screenshot shows the configuration of a security group rule within the AWS CloudFormation console. The rule is defined as follows:

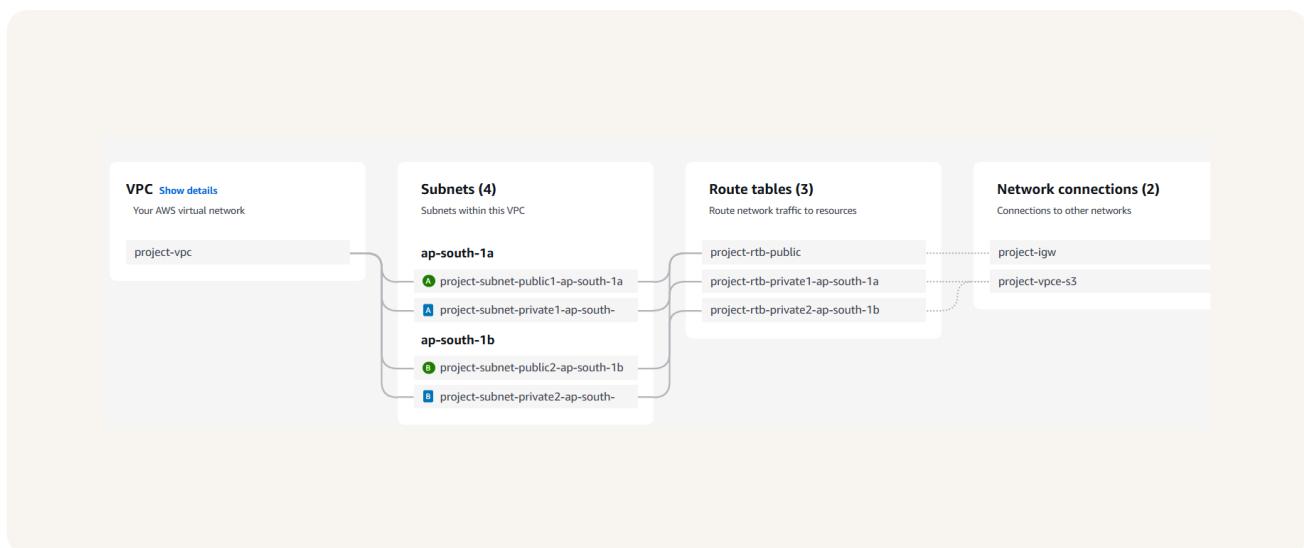
- Security group name - required:** NextWork Private Security Group
- Description - required:** Security group for NextWork Private Subnet.
- Inbound Security Group Rules:** Security group rule 1 (TCP, 22, sg-077bd356e44d20fae)
- Type:** ssh
- Protocol:** TCP
- Port range:** 22
- Source type:** Custom
- Source:** sg-077bd356e44d20fae
- Description - optional:** e.g. SSH for admin desktop

# Speeding up VPC creation

I used an alternative way to set up an Amazon VPC! This time, I adjusted the number of availability zones, reduced private subnets, updated CIDR blocks, and skipped NAT gateways and VPC endpoints to create a more controlled and cost-effective setup.

A VPC resource map is a visual representation of all components within a VPC, including subnets, route tables, and security groups. It helps in understanding the network structure, resource connections, and traffic flow.

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 isolated networks, and overlapping CIDR blocks only matter if they need to communicate



# Speeding up VPC creation

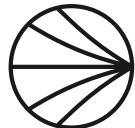
## Tips for using the VPC resource map

When determining the number of public subnets in my VPC, I only had two options: one or two. This was because the number of availability zones was set to either one or two, and each public subnet must reside in a different availability zone.

The set-up page also offered to create NAT gateways, which are used to allow instances in private subnets to access the internet while blocking inbound traffic. They provide a secure way for private instances to fetch updates without public exposure.

The screenshot shows the 'Create VPC' configuration page with the 'Preview' section expanded. The preview displays the following network components:

- VPC**: Shows details of the AWS virtual network named "nextwork-vpc".
- Subnets (6)**: Subnets within this VPC, categorized by Availability Zone:
  - ap-south-1a**: nextwork-subnet-public1-ap-south-1a, nextwork-subnet-private1-ap-south-1a, nextwork-subnet-private3-ap-south-1a
  - ap-south-1b**: nextwork-subnet-public2-ap-south-1b, nextwork-subnet-private2-ap-south-1b, nextwork-subnet-private4-ap-south-1b
- Route tables (5)**: Router network traffic to resources, connected to the subnets above.
  - nextwork-rtb-public
  - nextwork-rtb-private1-ap-south-1a
  - nextwork-rtb-private2-ap-south-1b
  - nextwork-rtb-private3-ap-south-1a
  - nextwork-rtb-private4-ap-south-1b
- Network connections (2)**: Connections to other networks.
  - nextwork-igw
  - nextwork-vpc-s3



NextWork.org

# **Everyone should be in a job they love.**

Check out nextwork.org for  
more projects

