



# Launching VPC Resources



Louis Moyo

The screenshot shows the AWS VPC Preview interface with the following details:

- VPC**: louismoyo-vpc
- Subnets (6)**:
  - eu-west-2a
    - louismoyo-subnet-public1-eu-west-2a
    - louismoyo-subnet-private1-eu-west-2a
    - louismoyo-subnet-private3-eu-west-2a
  - eu-west-2b
    - louismoyo-subnet-public2-eu-west-2b
    - louismoyo-subnet-private2-eu-west-2b
    - louismoyo-subnet-private4-eu-west-2b
- Route tables (5)**:
  - louismoyo-rtb-public
  - louismoyo-rtb-private1-eu-west-2a
  - louismoyo-rtb-private2-eu-west-2b
  - louismoyo-rtb-private3-eu-west-2a
  - louismoyo-rtb-private4-eu-west-2b
- Network connections**:
  - louismoyo-lgw
  - louismoyo-vpce-s3



# Introducing Today's Project!

## What is Amazon VPC?

Amazon VPC is a service that lets you create a logically isolated network within AWS to launch resources securely. It's useful because it gives full control over IP ranges, subnets, routing, and security for building customized cloud environments.

## How I used Amazon VPC in this project

I used Amazon VPC to launch EC2 instances in both public and private subnets and to explore how the VPC wizard can quickly create a complete networking setup with the required components for faster deployment.

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

One thing I didn't expect in this project was how quickly the VPC wizard could create a ready-to-use networking setup, including subnets and route tables, without having to build each component manually.



## This project took me...

This project took me around 60 minutes to complete, including launching EC2 instances in public and private subnets and using the VPC wizard to set up a complete networking environment automatically.



# Setting Up Direct VM Access

Directly accessing a virtual machine means connecting to it over the internet or network using secure protocols like SSH or RDP. This allows you to manage, configure, and control the server just as if you were operating a physical computer.

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

SSH traffic means using the Secure Shell protocol to connect securely to a remote server or virtual machine over a network. It encrypts communication, allowing safe administration and data transfer between your computer and the EC2 instance.

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

Key pairs are a set of security credentials, consisting of a public key and a private key, used to securely connect to an EC2 instance. AWS stores the public key, while I keep the private key to authenticate my SSH connection.

A private key's file format defines how the key is encoded and stored for use in authentication. Common formats include PEM (.pem) and PPK (.ppk). My private key's file format was PEM, which is the standard format for AWS EC2 SSH connections.



# Launching a public server

I had to change my EC2 instance's networking settings by confirming it used my custom VPC (not default) and placing it in the correct subnet for this project only!

The screenshot shows the AWS CloudWatch Metrics interface for an EC2 instance named 'i-0ca323ced29b1cf84'. The 'Networking' tab is selected. Key details shown include:

- VPC ID:** vpc-076d0c5b71f4a54eb (louismoyo VPC)
- Subnet ID:** subnet-0c5adb416fd4e5a4 (louismoyo public subnet)
- Availability zone:** eu-west-2a
- IP addresses:** Public IPv4 address: 3.8.143.11; Private IPv4 addresses: 10.0.0.246.
- Hostname and DNS:** Public DNS: ip-10-0-0-246.eu-west-2.compute.internal; Private IP DNS name (IPv4 only): ip-10-0-0-246.eu-west-2.compute.internal



# Launching a private server

My private server has its own dedicated security group because it requires specific inbound and outbound rules that differ from the public server, helping to enforce stricter access control and separate network traffic for security purposes.

My private server's security group's source is another security group, which means only resources within that group, such as my public server, can initiate connections to it. This setup allows controlled, private communication between instances.

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, sg-0b25b3bd5ae1122d1) Remove

Type   <a href="#">Info</a> ssh	Protocol   <a href="#">Info</a> TCP	Port range   <a href="#">Info</a> 22
Source type   <a href="#">Info</a> Custom	Source   <a href="#">Info</a> <input type="text" value="Add CIDR, prefix list or security group"/> <span style="border: 1px solid #ccc; padding: 2px;">sg-0b25b3bd5ae1122d1 </span>	Description - optional   <a href="#">Info</a> e.g. SSH for admin desktop

[Add security group rule](#)

► Advanced network configuration

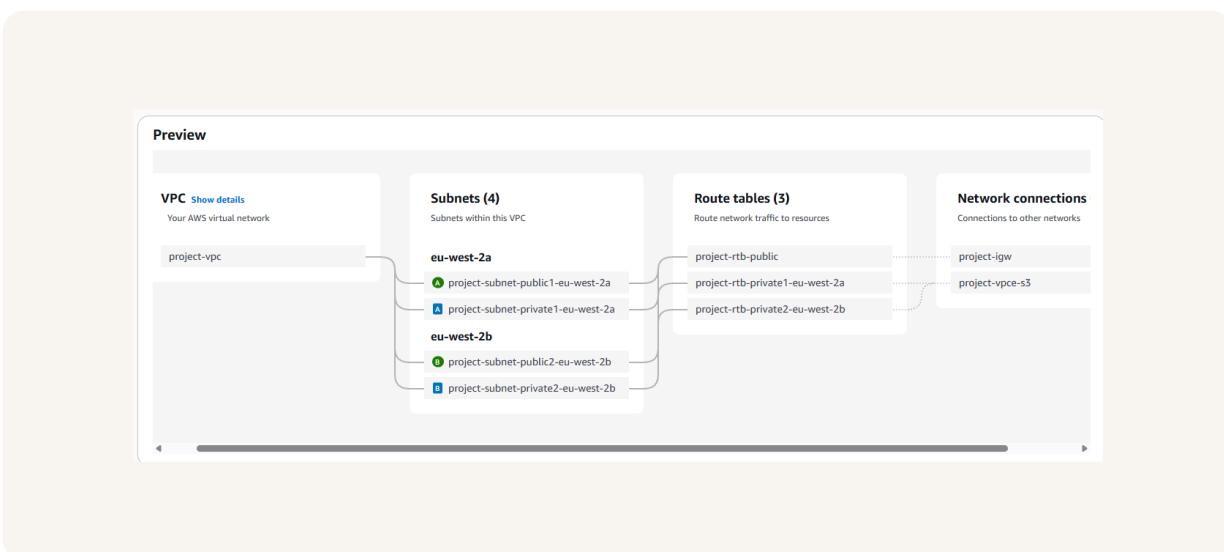


# Speeding up VPC creation

I used an alternative way to set up an Amazon VPC! This time, I created it using the “VPC and more” option, which automatically provisioned subnets, route tables, gateways, and other networking components for a complete, ready-to-use setup.

A VPC resource map is a visual diagram in AWS that shows all networking components within a VPC, including subnets, route tables, gateways, and security groups, helping you understand how resources are connected and interact in your architecture.

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 separate networks and do not communicate unless explicitly peered.

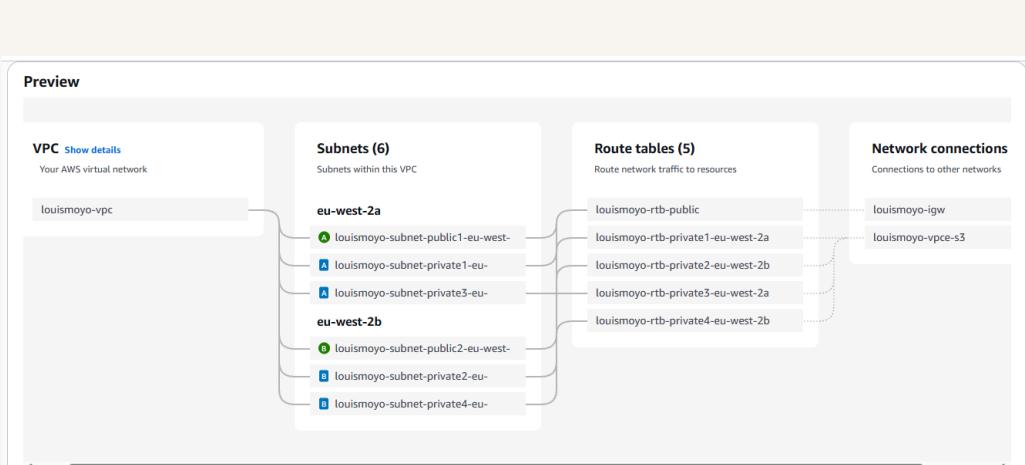


# Speeding up VPC creation

## 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 my chosen configuration automatically created subnets in different availability zones to ensure redundancy and high availability.

The set up page also offered to create NAT gateways, which are managed AWS services that allow private subnet resources to initiate outbound internet connections while preventing inbound traffic from the internet for enhanced security.





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

# The place to learn & showcase your skills

Check out [nextwork.org](https://nextwork.org) for more projects

