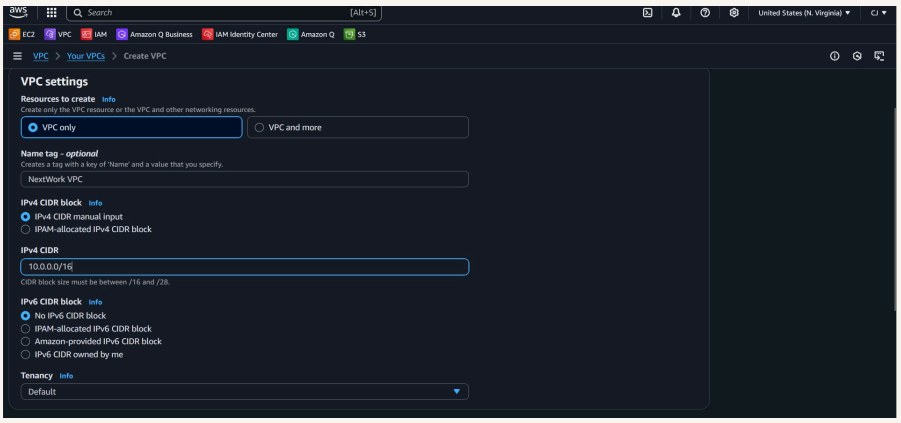
nextwork.org

Build a Virtual Private Cloud (VPC)

Chrispinus Jacob



Chrispinus Jacob
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

mazon VPC (Virtual Private Cloud) is a service that lets you create your own private network inside AWS — like having a personal, isolated data center in the cloud.

How I used Amazon VPC in this project

I used Amazon VPC in today’s project to set up a secure, custom network for my resources.

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

One thing I didn’t expect in this project was how easy it is to make a small mistake with CIDR blocks or command syntax and have it break the whole setup — like accidentally using brackets [] in commands, or trying to create a subnet with the same CIDR block as the entire VPC.

This project took me...

This project took me about 1 hour to complete

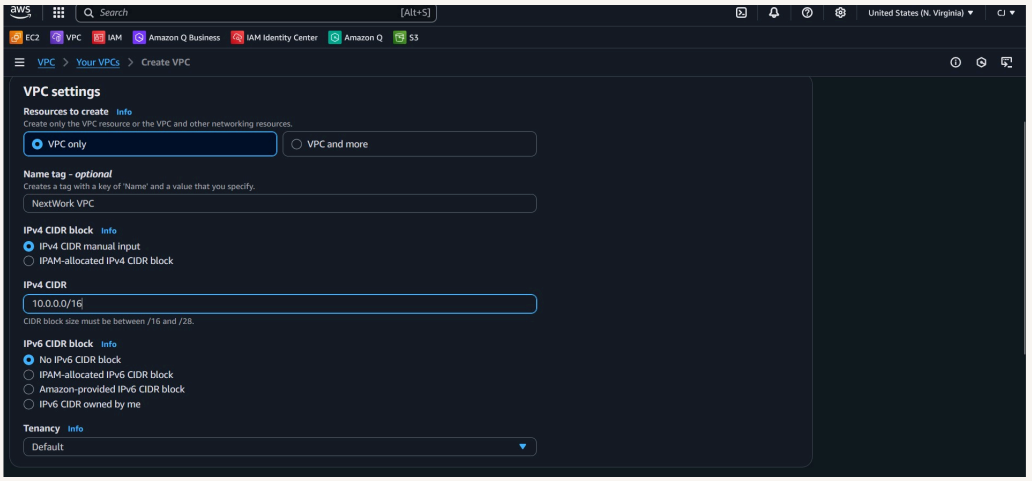
Chrispinus Jacob
NextWork Student

Virtual Private Clouds (VPCs)

VPCs are Virtual Private Clouds — they are private, isolated networks that you create inside a cloud provider like AWS.

There was already a default VPC in my account ever since my AWS account was created. This is because AWS automatically provides a default VPC in each region to make it easier to launch resources like EC2 instances without having to set up networking from scratch.

To set up my VPC, I had to define an IPv4 CIDR block, which is a range of private IP addresses that my resources inside the VPC will use — for example, 10.0.0.0/16. This block determines how big my network can be and how many subnets and IPs I can create within it.


aws
Search
[Alt+S]
United States (N. Virginia)
EC2
VPC
IAM
Amazon Q Business
IAM Identity Center
Amazon Q
S3
VPC > Your VPCs > Create VPC
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 - optional
Creates a tag with a key of 'Name' and a value that you specify.
NextWork VPC
IPv4 CIDR block Info
IPv4 CIDR manual input
IPAM-allocated IPv4 CIDR block
IPv4 CIDR
10.0.0.0/16
CIDR block size must be between /16 and /28.
IPv6 CIDR block Info
No IPv6 CIDR block
IPAM-allocated IPv6 CIDR block
Amazon-provided IPv6 CIDR block
IPv6 CIDR owned by me
Tenancy Info
Default

Chrispinus Jacob
NextWork Student

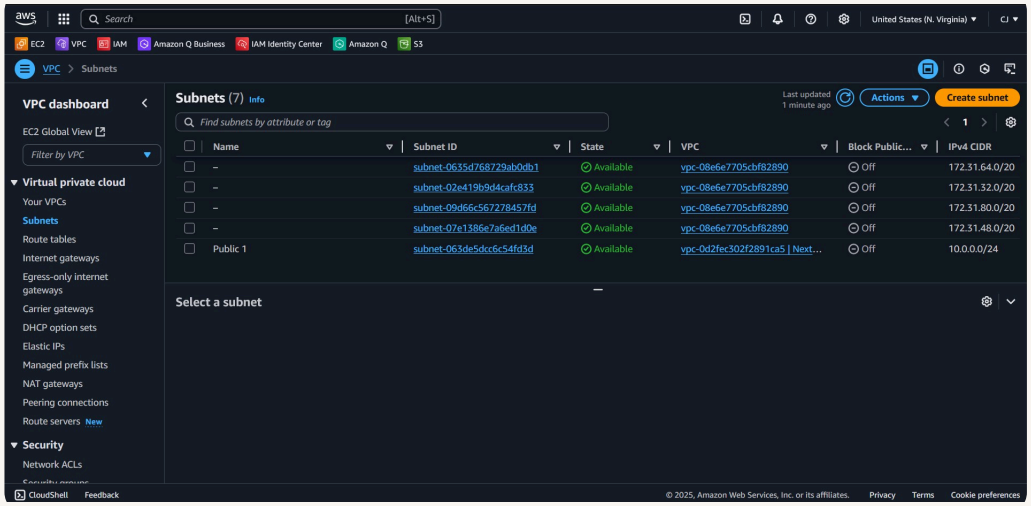
Subnets

Subnets are smaller sections of a VPC's IP address range — they divide the VPC into pieces to organize and control how resources are placed and connected. There are already subnets existing in my account, one for every Availability Zone in each region's default VPC.

Once I created my subnet, I enabled auto-assign public IPv4 addresses. This setting makes sure that any new instance launched in that subnet automatically gets a public IP address, so that it can connect to the internet and be reached from outside if needed.

The difference between public and private subnets are about whether resources inside can reach the internet directly or not. For a subnet to be considered public, it has to have a route to an Internet Gateway — this means instances in that subnet can send and receive traffic from the internet. A private subnet, on the other hand, does not have a direct route to an Internet Gateway. Resources in private subnets usually stay internal and access the internet only through things like a NAT Gateway or NAT instance, which lets them reach out (like to download updates) without being directly reachable from outside.

Chrispinus Jacob
NextWork Student

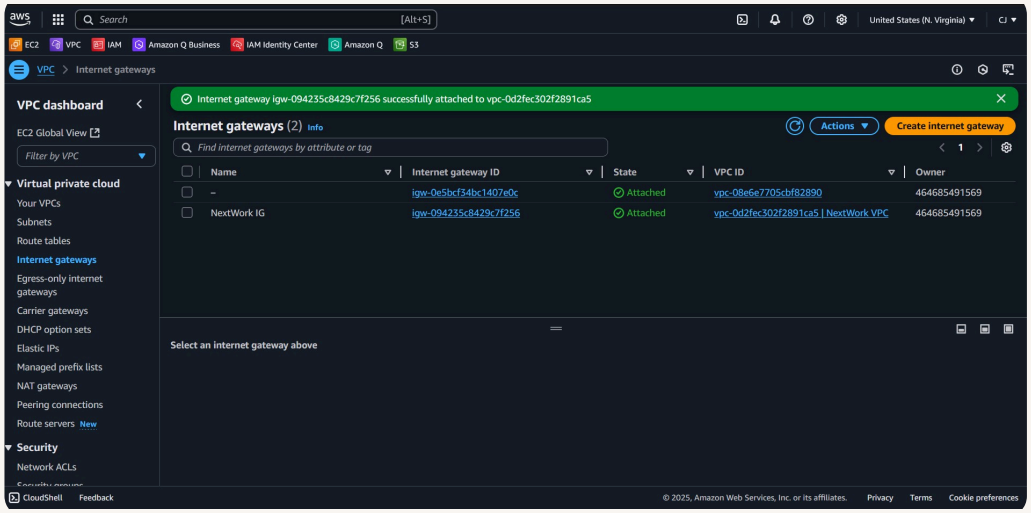


Chrispinus Jacob
NextWork Student

Internet gateways

ChatGPT said: Internet gateways are AWS resources that connect a VPC to the internet so that instances in public subnets can send and receive traffic outside AWS. An internet gateway handles the two-way communication between your private cloud network and the public internet.

Attaching an internet gateway to a VPC means connecting my private network to the internet, so that resources in public subnets can send and receive traffic outside AWS. If I missed this step, even if my instances have public IPs and a route table entry, they wouldn't be able to access the internet because there's no gateway to handle the traffic in and out of the VPC.



Chrispinus Jacob
NextWork Student

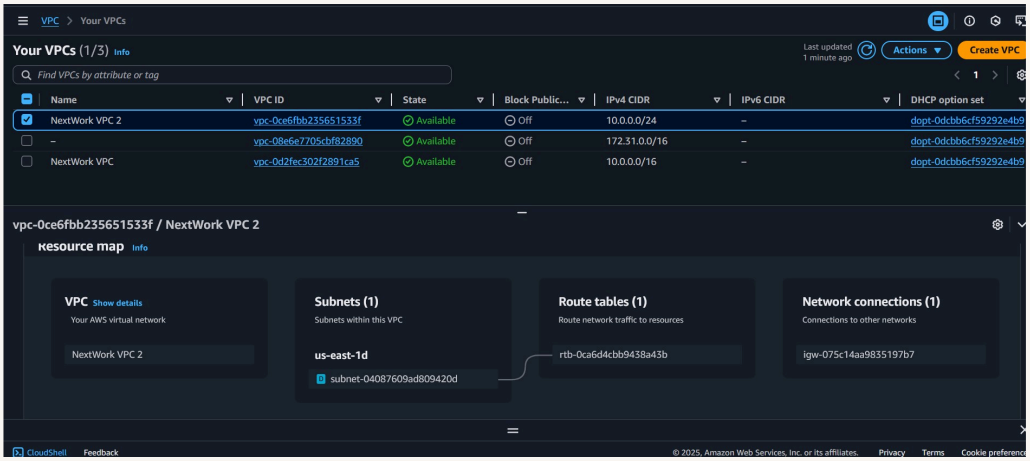
Using the AWS CLI

VPC resources could also be created with CloudShell, which is an online command-line environment provided by AWS right in the browser — it lets me run AWS CLI commands without installing anything on my computer. CLI is the Command Line Interface, a tool I can use to type commands to create, manage, and automate AWS resources, including VPCs, subnets, route tables, and more, instead of doing it manually through the console.

To set up a VPC or a subnet, you can use the command line with aws ec2 commands like create-vpc and create-subnet. Make sure to avoid errors by including all required parameters, like the --cidr-block for both the VPC and the subnet, and avoid using brackets [] in your actual commands — they're just placeholders in examples. Also, always check that your subnet's CIDR block is smaller than and fully inside your VPC's CIDR block, and if needed, specify an Availability Zone so you know exactly where your subnet will be created.

ChatGPT said: Compared to using the AWS Console, an advantage of using commands is that you can automate tasks, repeat them easily, and manage resources faster without clicking through many pages. An advantage of using the Console is that it's visual and beginner-friendly, so it's easier to see what's happening, spot mistakes, and understand how resources connect. Overall, I preferred using the Console at first to understand how VPC parts fit together, but using commands feels more powerful and efficient once I know what I'm doing

Chrispinus Jacob
NextWork Student



The place to learn & showcase your skills

Check out nextwork.org for more projects