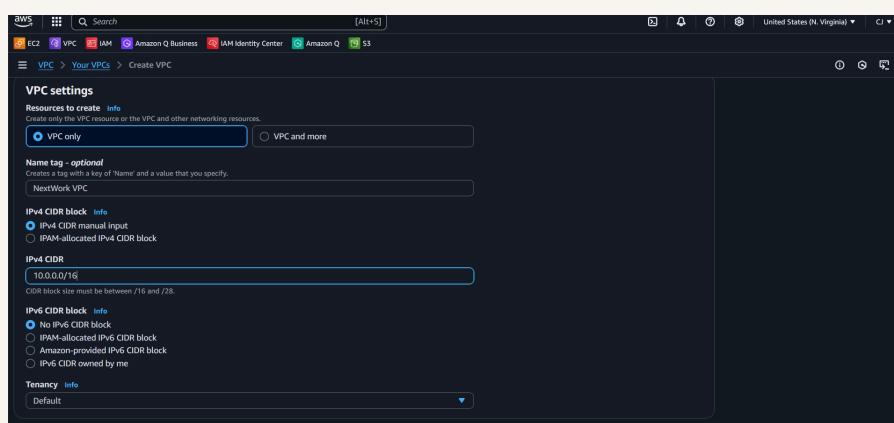


nextwork.org

Build a Virtual Private Cloud (VPC)



Chrispinus Jacob





Chrispinus Jacob
NextWork Student

nextwork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon 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



Virtual Private Clouds (VPCs)

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

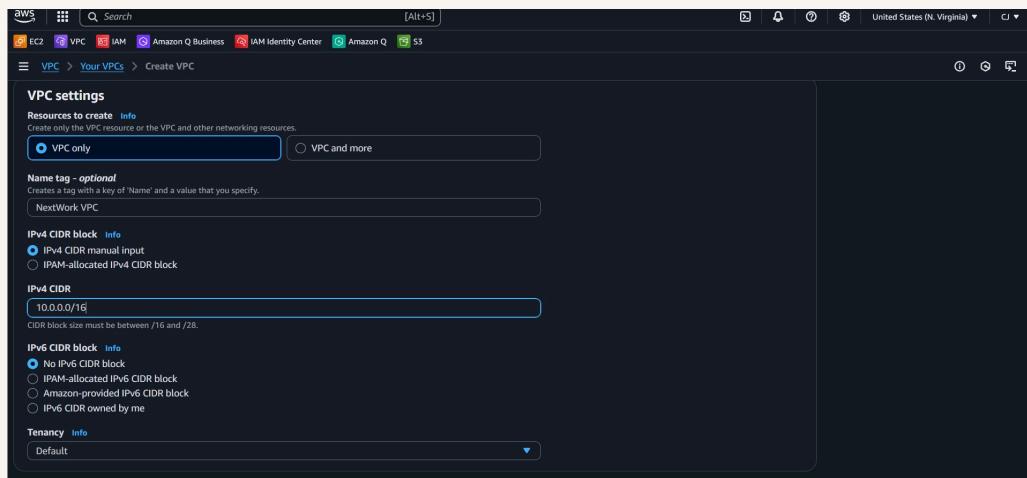
There was already a default VPC in my account ever since my AWS account was created. This is because AWS automatically provides a default VPC in each region to make it easier to launch resources like EC2 instances without having to set up networking from scratch.

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.



Chrispinus Jacob
NextWork Student

nextwork.org





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.

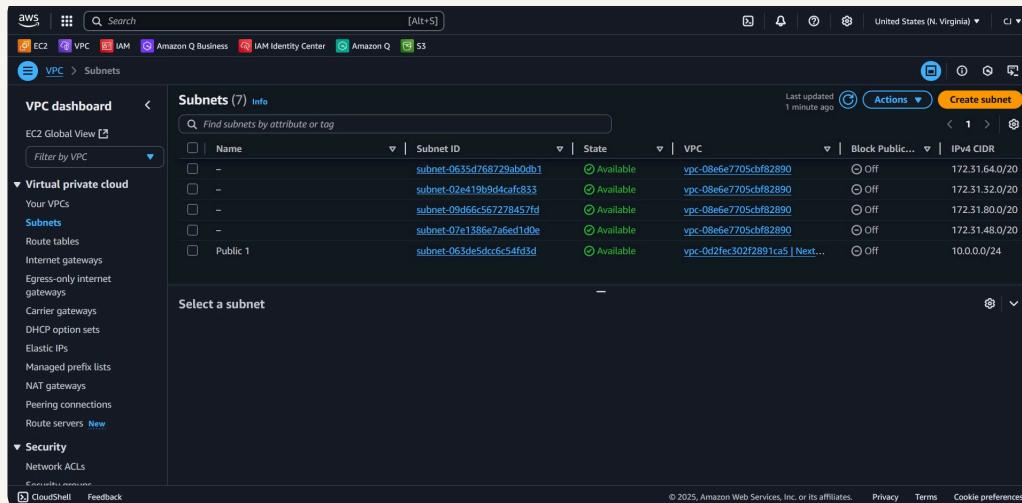
Once I created my subnet, I enabled auto-assign public IPv4 addresses. This setting makes sure that any new instance launched in that subnet automatically gets a public IP address, so that it can connect to the internet and be reached from outside if needed.

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

nextwork.org



The screenshot shows the AWS VPC Subnets page. The left sidebar is the VPC dashboard with sections for EC2 Global View, Virtual private cloud (Your VPCs, Subnets, Route tables, Internet gateways, Egress-only Internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, NAT gateways, Peering connections, Route servers), and Security (Network ACLs). The main content area is titled 'Subnets (7) Info' and shows a table of subnets. The table has columns for Name, Subnet ID, State, VPC, Block Public, and IPv4 CIDR. The subnets listed are:

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
-	subnet-0635d768729ab0db1	Available	vpc-08e5e7705cbf82890	Off	172.31.64.0/20
-	subnet-02e4199d4c4cf833	Available	vpc-08e5e7705cbf82890	Off	172.31.32.0/20
-	subnet-09d66c567278457fd	Available	vpc-08e5e7705cbf82890	Off	172.31.80.0/20
-	subnet-07e1386e7a6ed1d0e	Available	vpc-08e5e7705cbf82890	Off	172.31.48.0/20
Public 1	subnet-063de50cc6c54fd3d	Available	vpc-0d2fec302f2891ca5	Off	10.0.0.0/24

Below the table, a section titled 'Select a subnet' is visible. The bottom of the page includes a footer with links to CloudShell, Feedback, and copyright information: © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences.

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.

The screenshot shows the AWS VPC Internet Gateways page. The top navigation bar includes links for EC2, VPC, IAM, Amazon Q Business, IAM Identity Center, Amazon Q, and S3. The VPC dashboard is visible on the left, with a sidebar for the Virtual private cloud section. The Internet Gateways section is selected, showing a table with two entries:

Name	Internet gateway ID	State	VPC ID	Owner
-	igw-0e5bcf34bc1407e0c	Attached	vpc-08e6e7705cbf82890	464685491569
NextWork IG	igw-094235c8429c7f256	Attached	vpc-0d2fec302f2891ca5 NextWork VPC	464685491569

A green success message at the top right states: "Internet gateway igw-094235c8429c7f256 successfully attached to vpc-0d2fec302f2891ca5". The bottom of the page includes a footer with links for CloudShell, Feedback, and copyright information: "© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences".



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

nextwork.org

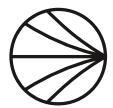
The screenshot shows the AWS VPC console. The top navigation bar includes 'VPC', 'Your VPCs (1/3) info', a search bar, and buttons for 'Actions' and 'Create VPC'. The main table lists three VPCs:

Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv6 CIDR	DHCP option set
NextWork VPC 2	vpc-0ce6fb235651533f	Available	Off	10.0.0.0/24	-	dopt-0dcbb6cf59292e4b9
-	vpc-08e6e7705cbf82890	Available	Off	172.31.0.0/16	-	dopt-0dcbb6cf59292e4b9
NextWork VPC	vpc-0d2fec302f2891ca5	Available	Off	10.0.0.0/16	-	dopt-0dcbb6cf59292e4b9

The 'NextWork VPC 2' row is selected. Below the table, a 'Resource map' is displayed for this VPC, showing four components:

- VPC** (Show details): Your AWS virtual network. Subnets within this VPC: us-east-1d (subnet-04087609ad809420d).
- Subnets (1)**: Subnets within this VPC.
- Route tables (1)**: Route network traffic to resources. Route table ID: rtb-0ca6d4ccb9438a43b.
- Network connections (1)**: Connections to other networks. Internet gateway ID: igw-075c14aa9835197b7.

At the bottom of the page are links for 'CloudShell', 'Feedback', and copyright information: '© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

