



Build a Virtual Private Cloud (VPC)

K

Katleo Rantle

☰ [VPC](#) > [Your VPCs](#) > Create VPC

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

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.

IPv4 CIDR block [Info](#)
 IPv4 CIDR manual input IPAM-allocated IPv4 CIDR block

IPv4 CIDR

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](#)

VPC encryption control (\$ - new) [Info](#)
Monitor mode provides visibility into encryption status without blocking traffic. Enforce mode prevents unencrypted traffic. Additional charges apply [Learn more](#)

None Monitor mode
See which resources in your VPC are unencrypted but allow the creation of unencrypted resources.

Enforce mode
Requires all resources, except exclusions, in your VPC to be encryption-capable and blocks creation of unencrypted resources.



Katleo Rantle

NextWork Student

nextwork.org

Introducing Today's Project!

In this project, I will demonstrate building & configuring an AWS VPC from scratch: subnets route tables, internet gateways & security groups for secure, scalable networks . I'm doing this project to learn VPC isolation/connection for app deployments

What is Amazon VPC?

Amazon VPC is a logical network boundary and it is useful because it helps keep resources isolated and private on the cloud

In today's project, I used Amazon VPC to build private network with a subnet and allowed resources in the vpc to connect to external networks

Personal reflection

This project took me 2.5 hours



K

Katleo Rantle

NextWork Student

nextwork.org

One thing I didn't expect in this project was the amount of configuration on the resources to get things to work we have to explicitly turn things on. which i learnt is good for security

Virtual Private Clouds (VPCs)

What I did in this step

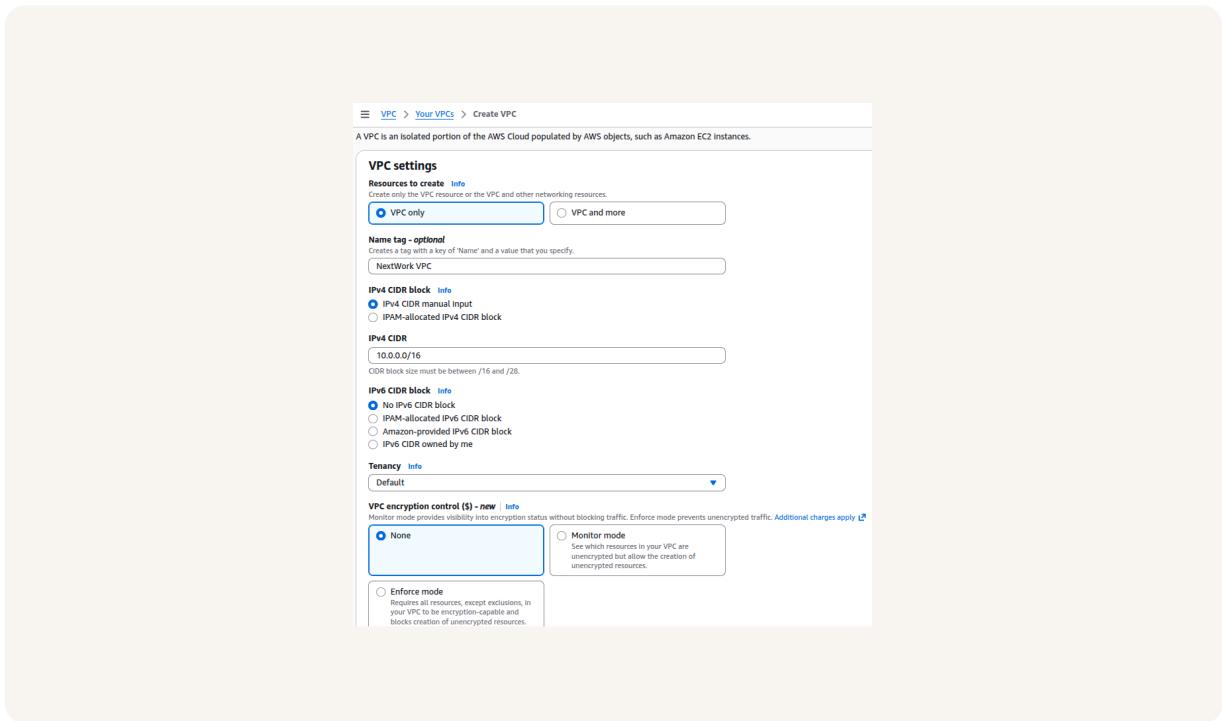
In this step, I will be creating a VPC because it establishes the isolated network environment that we need in this project to securely connect and scale all our cloud resources

How VPCs work

VPCs are logical network boundaries that help keep resources isolated secure and private on the cloud ensuring protection from unauthorized access this is achieved by defining IP ranges, subnets and routing rules

Why there is a default VPC in AWS accounts

There was already a default VPC in my account ever since my AWS account was created. This is because many AWS services cannot run without a VPC although we can configure our own VPC on AWS it is more convenient to have it for beginners to AWS



Defining IPv4 CIDR blocks

To set up my VPC, I had to define an IPv4 CIDR block, which is a way to define a portion of IP addresses for a network that cloud resources can use without overlapping others and preventing IP conflicts

Subnets

What I did in this step

In this step I will create subnets because they divide the VPC's IP address range into logical segments i.e public ones for internet-facing resources and private ones for secure internal access enabling granular control & better organization & security

Creating and configuring subnets

Subnets are subdivisions of the VPC IP address range, where we can launch AWS resources. There are already subnets existing in my account, one for every availability zone

Public vs private subnets

The difference between public and private subnets are internet access (public) to external networks and no direct internet access (private) for internal resource communication. For a subnet to be considered public, it has to deliberately be attached to an Internet Gateway.



Auto-assigning public IPv4 addresses

Once I created my subnet, I enabled auto assign public IPv4 addresses. This setting makes sure any Ec2 instance launched in this subnet will instantly receive a public ip address so that we don't have to create one manually.

Internet gateways

What I did in this step

In this step, I will be attaching an internet gateway and updating the route table associated with the subnet to include a route pointing to the internet gateway because it is the essential component that allows our VPC to communicate with the public internet.

Setting up internet gateways

Internet gateways are a managed AWS service or VPC component that serves as a bridge between VPC and public internet. It enables two-way communication so that resources inside the VPC such as EC2 instances (inside public subnets) can reach the internet, and devices on the internet can initiate connections with those devices.

Attaching an internet gateway to a VPC means resources within the VPC can now access the internet. If I missed this step, resources like EC2 instances will not be able to initiate a connection to external networks such as the internet.



Katleo Rantle

NextWork Student

nextwork.org

The screenshot shows the AWS VPC Internet Gateways page. The left sidebar has 'VPC dashboard' selected under 'Virtual private cloud'. The main content area shows a table of internet gateways:

Name	Internet gateway ID	Status	VPC ID	Owner
aws	ipn-022e615d4c264c9	Attached	vpc-063a1c7dd60f11x6	D99612844607
NextWork IG	ipn-0270b01504c264c9	Attached	vpc-07842490b0011c11	NextWork VPC

A notification at the top states: "Internet gateway ipn-022e615d4c264c9 successfully attached to vpc-01f472460db0f1e78".



Katleo Rantle

NextWork Student

nextwork.org

Using the AWS CLI

What I'm doing in this extension

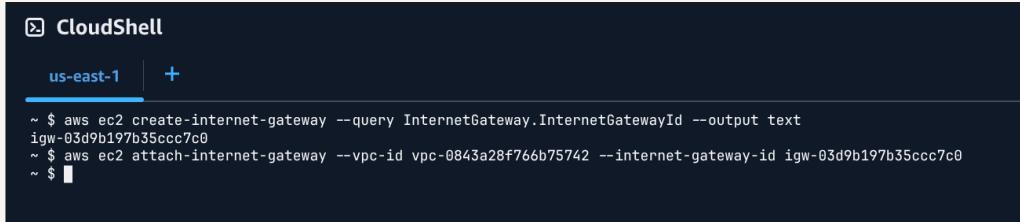
In this project extension, I will be using the AWS cli to launch VPC resources to determine if it will be faster and more efficient than the aws console

Exploring CloudShell and CLI

VPC resources could also be created with CloudShell, which is a management console that provides space or terminal to run code. CLI is utility software that allows us to execute commands such as create, update and delete on AWS resources.

Debugging my setup

To set up a VPC or a subnet, you can use the command `--cidr-block`. Make sure to avoid errors by including a subnet CIDR block range that is within the VPC's CIDR block.



The screenshot shows the AWS CloudShell interface. At the top, it says "CloudShell" with a "us-east-1" dropdown menu and a "+" button. Below that is a terminal window with the following command history:

```
~ $ aws ec2 create-internet-gateway --query InternetGateway.InternetGatewayId --output text
igw-03d9b197b35ccc7c0
~ $ aws ec2 attach-internet-gateway --vpc-id vpc-0843a28f766b75742 --internet-gateway-id igw-03d9b197b35ccc7c0
~ $
```

Comparing CloudShell vs AWS Console

Compared to using the AWS Console, an advantage of using commands is its much quicker and easier to check for errors An advantage of using the Console its visual and on syntax to remeber Overall, I preferred the cli as you could just run one command instead of clicking thoungh many pages and i found it less intimidating



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

