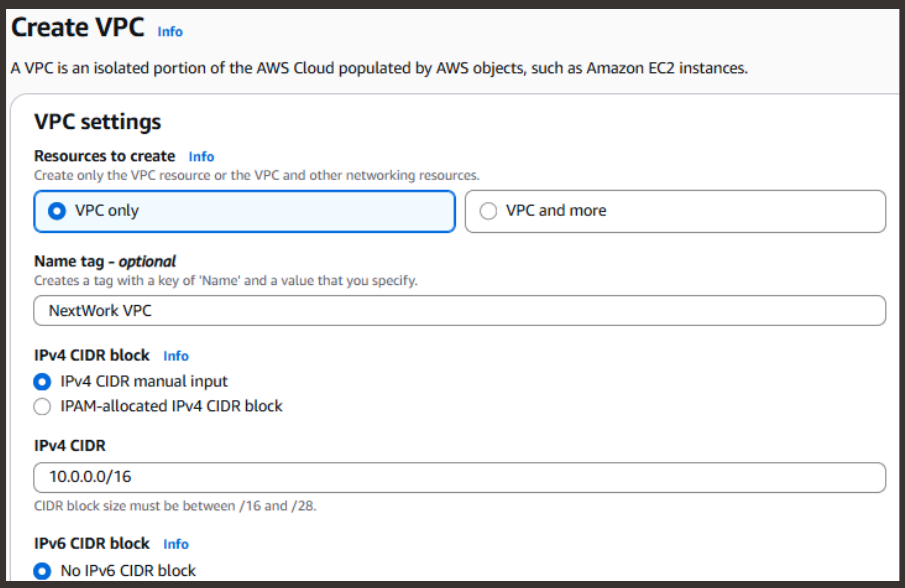
nextwork.org

Build a Virtual Private Cloud (VPC)

CH Arpita Chowdhury



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is your own private network inside AWS, and it’s useful because it gives you the flexibility, security, and connectivity you need to safely run applications in the cloud.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create my own VPC, subnet, internet gateway in Amazone VPC console and also another in cloudshell.

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

One thing I didn't expect in this project was using cloudshell which was new to me as I have used this for the first time.

This project took me...

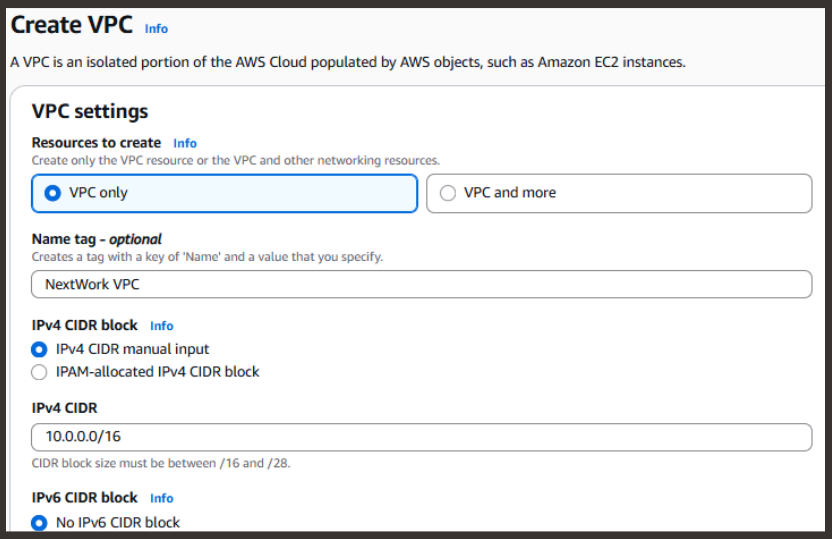
This project took me about 4 hours.

Virtual Private Clouds (VPCs)

VPCs (Virtual Private Cloud) are a private, isolated virtual network within a public cloud infrastructure, offering a controlled environment for launching resources like virtual servers and databases. It provides the control and security of a private data center but within the scalable and affordable framework of a public cloud, allowing organizations to manage their own IP address ranges, subnets, route tables, and security configurations.

There was already a default VPC in my account ever since my AWS account was created. This is because AWS automatically creates one in each region to make it easier to launch and use cloud resources without having to configure complex networking upfront.

To set up my VPC, I had to define an IPv4 CIDR block, which is 10.0.0.0/16. This gives my VPC a private IP address range with up to 65,536 IP addresses that I can divide across multiple subnets.


Create VPC Info
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.
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

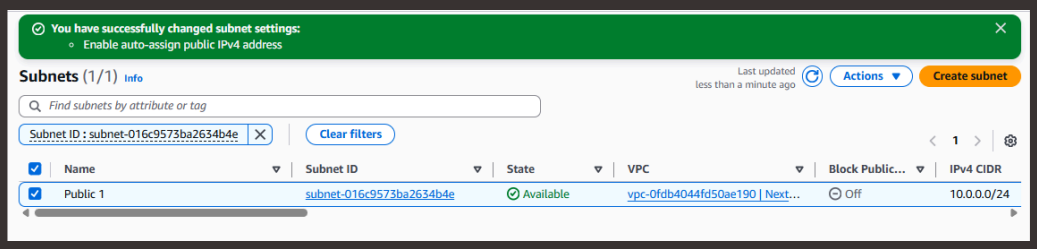
Subnets

Subnets are a segment within your Virtual Private Cloud (VPC) that defines a range of IP addresses for your resources, like EC2 instances. Subnets help organize and control your network by logically dividing your VPC into smaller, manageable parts, and can be either public (with internet access via an Internet Gateway) or private (without direct internet access). Each subnet must reside within a single Availability Zone (AZ) and has its own route table to manage traffic flow. There are already subnets existing in my account, one for every availability zone for the predfined VPC that exist there.

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 communicate directly with the internet through the internet gateway without me needing to manually attach an Elastic IP or configure one later.

The difference between public and private subnets is that public subnets can directly access the internet (and be accessed from it), while private subnets cannot. For a subnet to be considered public, it must have a route to an Internet Gateway and the VPC must have the IGW attached. Without this, the subnet is considered private

CH
Arpita Chowdhury
NextWork Student

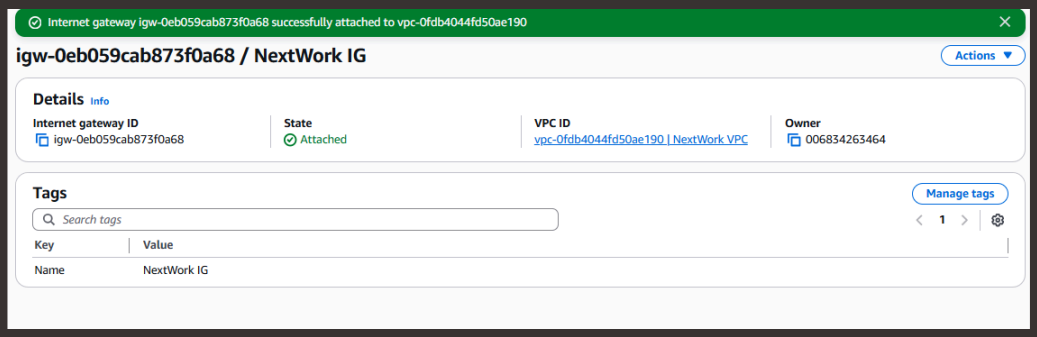


CH
Arpita Chowdhury
NextWork Student

Internet gateways

Internet Gateways are AWS-managed, horizontally scaled, redundant, and highly available components that connect a VPC to the public internet, enabling two-way communication for instances in public subnets that have public IPs and proper route/security configurations.

Attaching an internet gateway to a VPC gives the VPC a route to the public internet, enabling instances with public IPs in subnets that route 0.0.0.0/0 (or ::/0) to it to send and receive traffic; if you miss this step, your VPC stays isolated and no instances can access or be accessed from the internet (including NAT gateways).



CH
Arpita Chowdhury
NextWork Student

Using the AWS CLI

VPC resources could also be created with CloudShell, which is a browser-based shell environment in the AWS Management Console that gives you command-line access without local setup. The CLI (AWS Command Line Interface) is a tool you install and run locally (or in CloudShell/EC2) to manage AWS services through commands and scripts

To set up a VPC or a subnet, you can use the command VPC: {aws ec2 create-vpc --cidr-block 10.0.0.0/24 --query Vpc.VpcId --output text} Subnet: {aws ec2 create--subnet --vpc-id} . Make sure to avoid errors by including --cidr-block which defines a subnet's CIDR block range. Without this, the CLI cannot create the subnet because it doesn't know which IP addresses to allocate for it.

Compared to using the AWS Console, an advantage of using commands is what is being created can easily be monitored and handled. The deatailed step by step can be seen.An advantage of using the Console is it much faster and easier. Overall, I preferred console over cloudshell.

CH

Arpita Chowdhury
NextWork Student


```
An error occurred (Resource.AlreadyAssociated) when calling the AttachInternetGateway operation: resource igw-0eb059cab873f0a68 is already attached to network vpc-0fdb4044fd50ae190
~ $ aws ec2 attach-internet-gateway --vpc-id vpc-047294a352296aa6d --internet-gateway-id igw-08149fd88e2c21a48

An error occurred (Resource.AlreadyAssociated) when calling the AttachInternetGateway operation: resource igw-08149fd88e2c21a48 is already attached to network vpc-047294a352296aa6d
~ $ aws ec2 delete-vpc --vpc-id vpc-047294a352296aa6d

An error occurred (DependencyViolation) when calling the DeleteVpc operation: The vpc 'vpc-047294a352296aa6d' has dependencies and cannot be deleted.
~ $ cls
bash: cls: command not found
~ $ clear
~ $ aws ec2 create-vpc --cidr-block 10.0.0.0/24 --query Vpc.VpcId --output text
An error occurred (MissingParameter) when calling the CreateSubnet operation: The request must contain at least one of these parameters: cidrBlock or ipv6CidrBlock or ipv4IpamPoolId or ipv6IpamPoolId.
~ $ aws ec2 create-subnet --vpc-id VPC-ID --cidr-block 10.0.0.0/24

An error occurred (InvalidVpcID.NotFound) when calling the CreateSubnet operation: The vpc ID 'VPC-ID' does not exist
~ $ aws ec2 create-subnet --vpc-id VPC-047294a352296aa6d --cidr-block 10.0.0.0/24
~ $ --query Vpc.VpcId --output text
bash: --query: command not found
~ $ aws ec2 create-internet-gateway --query InternetGateway.InternetGatewayId --output text
~ $ aws ec2 create-internet-gateway --query InternetGateway.InternetGatewayId --output text
~ $ aws ec2 attach-internet-gateway --vpc-id vpc-0fdb4044fd50ae190 --internet-gateway-id igw-0eb059cab873f0a68

An error occurred (Resource.AlreadyAssociated) when calling the AttachInternetGateway operation: resource igw-0eb059cab873f0a68 is already attached to network vpc-0fdb4044fd50ae190
~ $ aws ec2 attach-internet-gateway --vpc-id vpc-047294a352296aa6d --internet-gateway-id igw-0eb059cab873f0a68

An error occurred (Resource.AlreadyAssociated) when calling the AttachInternetGateway operation: resource igw-0eb059cab873f0a68 is already attached to network vpc-0fdb4044fd50ae190
~ $ aws ec2 attach-internet-gateway --vpc-id vpc-047294a352296aa6d --internet-gateway-id igw-08149fd88e2c21a48
```

nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects