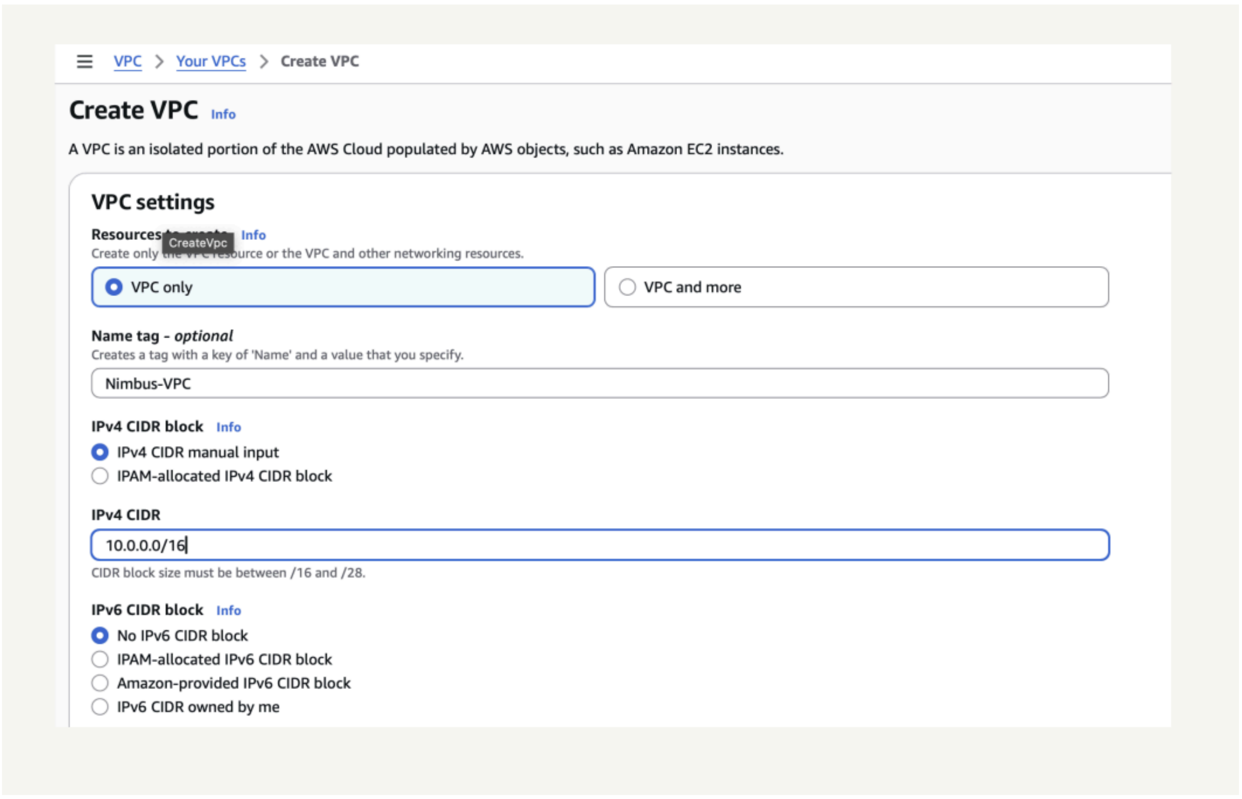
Build a Virtual Private Cloud (VPC)

Erik Gonzalez



VPC > Your VPCs > Create VPC

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.

Nimbus-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

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a service that lets you create your own private network environment inside AWS and it is useful because I can control who has access to what!

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create my own segmented network with its subnet, gateway etc..

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

One thing I didn't expect in this project was that AWS uses subnets.

This project took me...

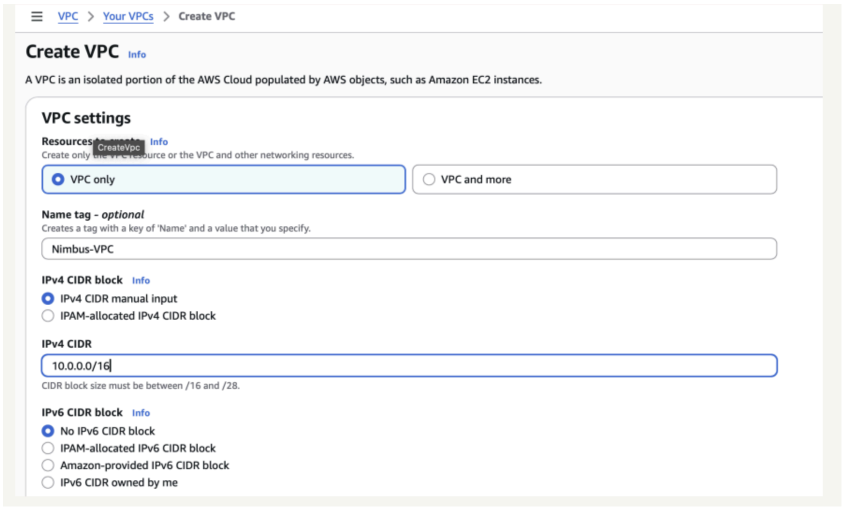
This project took me about an hour!

Virtual Private Clouds (VPCs)

VPCs are private network environments in the cloud where you can place servers, databases and applications while keeping them secured and isolated from other resources.

There was already a default VPC in my account ever since my AWS account was created. This is because AWS automatically sets up a default VPC for you! This default VPC is why you could launch resources (e.g. EC2 instances) and connect services together from Day 1 of using AWS. If it didn't exist, you would've had to learn how to create it before you can use some of the services that need VPCs to function.

To set up my VPC, I had to define an IPv4 CIDR block, which is an IP address range using a network address and a prefix length that determines how many IPs the block contains.



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
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.
Nimbus-VPC

IPv4 CIDR block
[✓ 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.

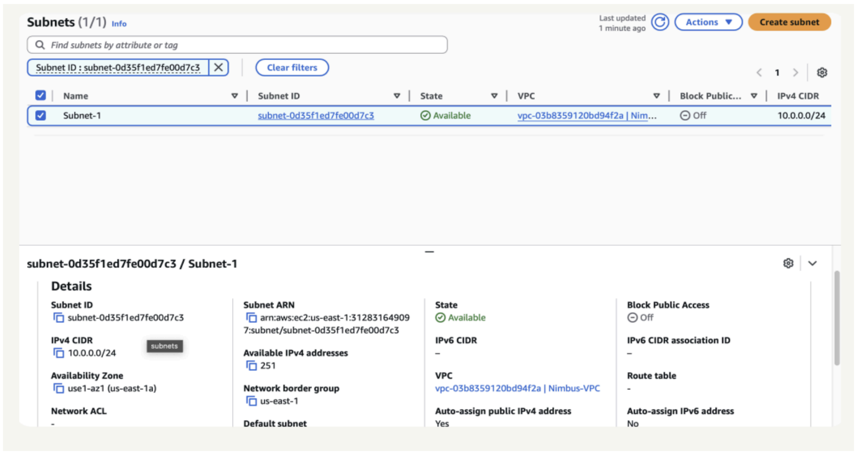
IPv6 CIDR block
[✓ No IPv6 CIDR block]
IPAM-allocated IPv6 CIDR block
Amazon-provided IPv6 CIDR block
IPv6 CIDR owned by me

Subnets

Subnets are a smaller, organized section of a larger network that divides and isolates resources for better control, security, and traffic management. There are already subnets existing in my account, one for every Availability Zone in my region (east-1)

Once I created my subnet, I enabled it. auto-assign public IPv4 address. This setting makes sure that any EC2 instance launched in the subnet will instantly get a public IP address so that I won't have to create one manually.

The difference between public and private subnets is that public subnets are resources that can communicate with external networks while private subnets are exclusively accessed by a specific user who created it. Holds internal resources.


Subnets (1/1) Info
Last updated 1 minute ago
Actions
Create subnet
Find subnets by attribute or tag
Subnet ID : subnet-0d35f1ed7fe00d7c3
Clear filters
1
subnets

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
Subnet-1	subnet-0d35f1ed7fe00d7c3	Available	vpc-03b8359120bd94f2a | Nim...	Off	10.0.0.0/24

subnet-0d35f1ed7fe00d7c3 / Subnet-1

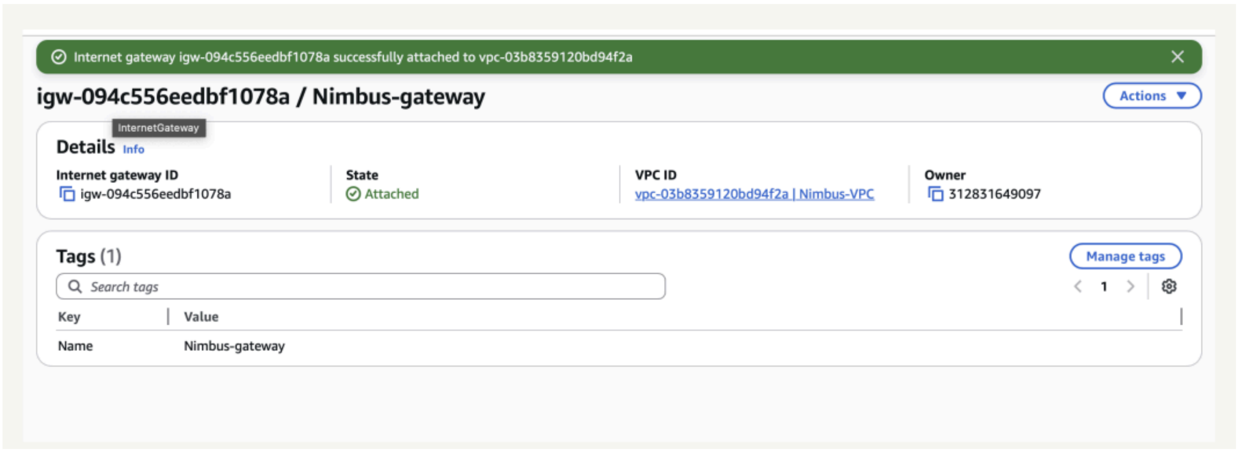
Details

Subnet ID subnet-0d35f1ed7fe00d7c3	**Subnet ARN** arn:aws:ec2:us-east-1:31283164909 7:subnet/subnet-0d35f1ed7fe00d7c3	**State** Available	**Block Public Access** Off
IPv4 CIDR 10.0.0.0/24	**Available IPv4 addresses** 251	**IPv6 CIDR** –	**IPv6 CIDR association ID** –
Availability Zone use1-az1 (us-east-1a)	**Network border group** us-east-1	**VPC** vpc-03b8359120bd94f2a | Nimbus-VPC	**Route table** -
Network ACL -	**Default subnet**	**Auto-assign public IPv4 address** Yes	**Auto-assign IPv6 address** No

Internet gateways

Internet gateways are components that allow resources inside a VPC (like EC2 instances) to send and receive traffic from the public internet.

Attaching an internet gateway to a VPC means the VPC can now access the internet. The EC2 instances with public IP addresses also become accessible to users, so my applications hosted on those servers become public too. If I missed this step the VPC would not be granted access to the internet.



Internet gateway igw-094c556eedbf1078a successfully attached to vpc-03b8359120bd94f2a

igw-094c556eedbf1078a / Nimbus-gateway

Details

Internet gateway ID	State	VPC ID	Owner
igw-094c556eedbf1078a	Attached	vpc-03b8359120bd94f2a | Nimbus-VPC	312831649097

Tags (1)

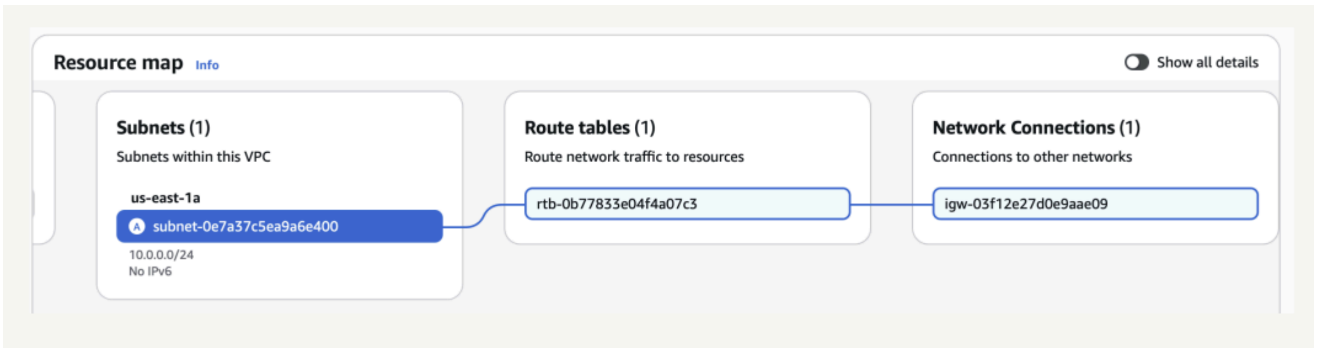
Key	Value
Name	Nimbus-gateway

Using the AWS CLI

VPC resources could also be created with CloudShell, which is a shell in your AWS Management Console to run code. CLI is a software that lets you create, delete and update AWS resources with commands instead of clicking through your console.

To set up a VPC or a subnet, you can use the command aws ec2 create-subnet -- *vpc-id* --*cidr-block* Make sure to avoid errors by typing the right number of dots, no overlapping, and no typos.

Compared to using the AWS Console, an advantage of using commands is that you can automate and repeat tasks easily by scripting them (saving commands, re-running them, and sharing them), instead of clicking through the console manually each time. An advantage of using the Console is that it provides a visual, point-and-click interface that's easier to learn. Overall, I preferred the console as I am more of a visual learner.


Resource map
Info
Show all details
Subnets (1)
Subnets within this VPC
us-east-1a
subnet-0e7a37c5ea9a6e400
10.0.0.0/24
No IPv6
Route tables (1)
Route network traffic to resources
rtb-0b77833e04f4a07c3
Network Connections (1)
Connections to other networks
igw-03f12e27d0e9aae09