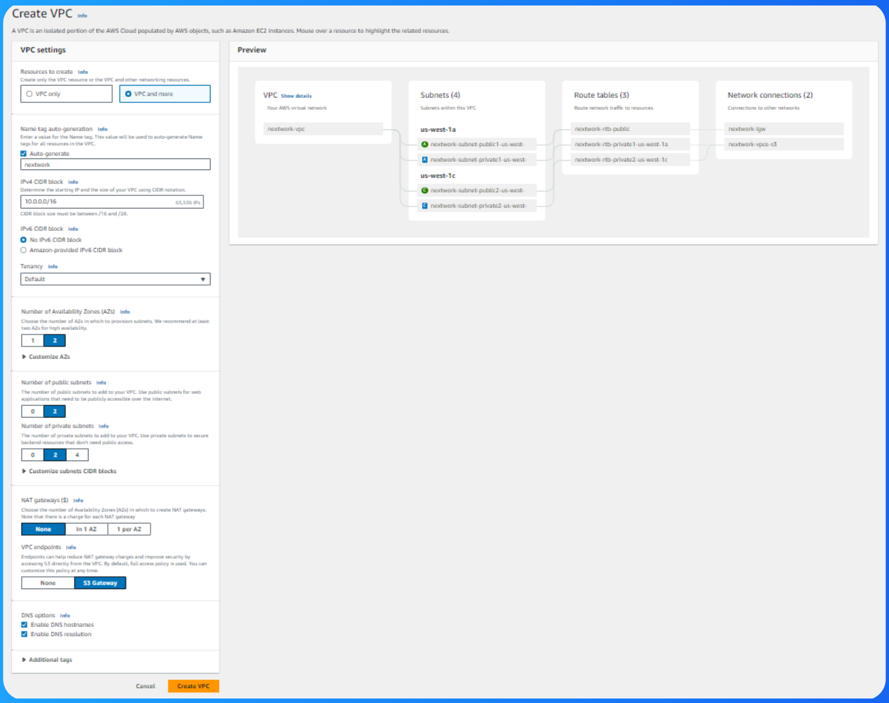
NextWork.org

Launching VPC Resources

mmoorejr24@gmail.com



Create VPC

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.

VPC settings

Resources to create
Create only the VPC resource or the VPC and other networking resources.
○ VPC only ● VPC and more

Name tag auto-generation
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.
☑ Auto-generate
nextwork

IPv4 CIDR block
Determine the starting IP and the size of your VPC using CIDR notation.
10.0.0.0/16 65,536 IPs
CIDR block size must be between /16 and /28.

IPv6 CIDR block
● No IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block

Tenancy
Default

Number of Availability Zones (AZs)
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.
1 [✓ 2]

▶ Customize AZs

Number of public subnets
The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.
0 [✓ 2]

Number of private subnets
The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.
0 [✓ 2] 4

▶ Customize subnets CIDR blocks

NAT gateways ($)
Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway
[✓ None] In 1 AZ 1 per AZ

VPC endpoints
Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.
None [✓ S3 Gateway]

DNS options
☑ Enable DNS hostnames
☑ Enable DNS resolution

▶ Additional tags

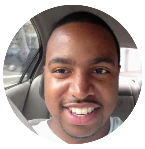
Preview

VPC
Your AWS virtual network
nextwork-vpc

Subnets (4)
Subnets within this VPC
us-west-1a
nextwork-subnet-public1-us-west-
nextwork-subnet-private1-us-west-
us-west-1c
nextwork-subnet-public2-us-west-
nextwork-subnet-private2-us-west-

Route tables (3)
Route network traffic to resources
nextwork-rtb-public
nextwork-rtb-private1-us-west-1a
nextwork-rtb-private2-us-west-1c

Network connections (2)
Connections to other networks
nextwork-igw
nextwork-vpce-s3



Introducing Today's Project!

What is Amazon VPC?

A VPC is a virtual network that closely resembles a traditional network that you'd operate in your own data center. Essentially, a VPC provisions logically isolated sections of a public cloud in order to provide a virtual private environment.

How I used Amazon VPC in this project

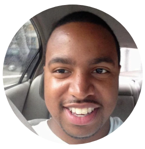
I used Amazon VPC to setup a public and private subnets with resources to securely communicate with each other.

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

I didn't expect the wealth of knowledge I would gain from configuring public and private resources and how they would communicate with each other securely.

This project took me...

This project took me about an 1 hour and 45 mins.



Setting Up Direct VM Access

Directly accessing a virtual machine means "logging into" the EC2 instance (instead of just managing it at a higher level with the AWS Management Console). This includes operations like installing software and changing EC2 instance's configurations.

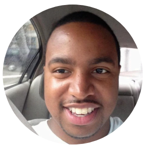
SSH is a key method for directly accessing a VM

SSH means Secure Shell, and it is both a protocol and a traffic type. It is the protocol that matches key pairs and direct VM access, and once a connection is set up, it is a traffic type that encrypts communication/data being transferred.

To enable direct access, I set up key pairs

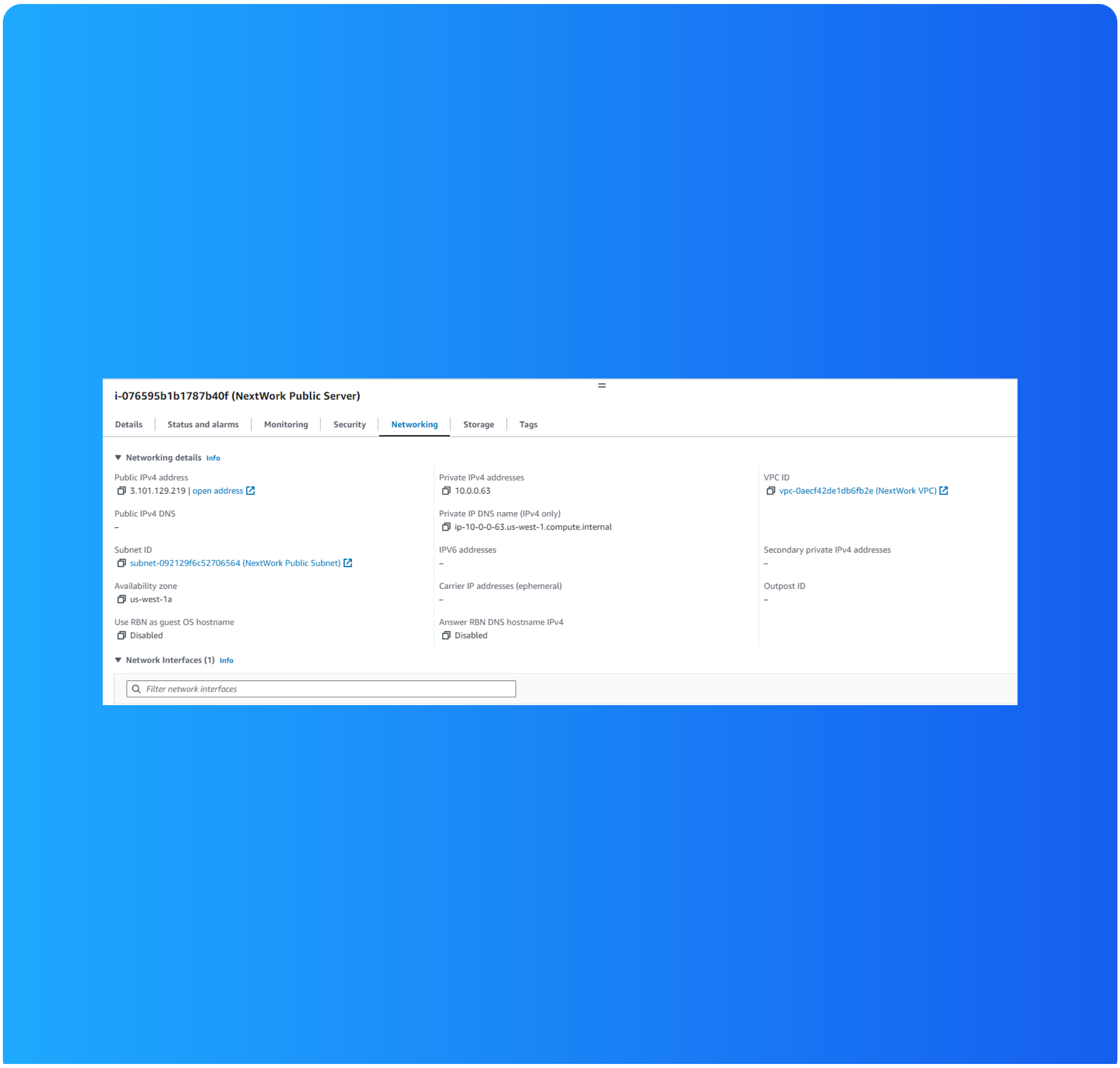
Key pairs are tools that help developers/engineers authenticate themselves when trying to get direct access to a virtual machine e.g. an EC2 instance.

A private key's file format means the file type that my key is stored in. My private key's file format was .pem, which is a widely accepted file format that most servers will be able to read/use.



Launching a public server

I had to change my EC2 instance's networking settings by changing the VPC and the Subnet my EC2 instance was going to be launched in! I updated both my NextWork VPC and Public Subnet. I also used my existing Public Security group.



i-076595b1b1787b40f (NextWork Public Server)

▼ Networking details Info

Public IPv4 address
3.101.129.219 | open address

Public IPv4 DNS
–

Subnet ID
subnet-092129f6c52706564 (NextWork Public Subnet)

Availability zone
us-west-1a

Use RBN as guest OS hostname
Disabled

Private IPv4 addresses
10.0.0.63

Private IP DNS name (IPv4 only)
ip-10-0-0-63.us-west-1.compute.internal

IPV6 addresses
–

Carrier IP addresses (ephemeral)
–

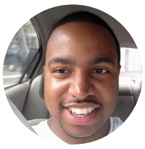
Answer RBN DNS hostname IPv4
Disabled

VPC ID
vpc-0aecf42de1db6fb2e (NextWork VPC)

Secondary private IPv4 addresses
–

Outpost ID
–

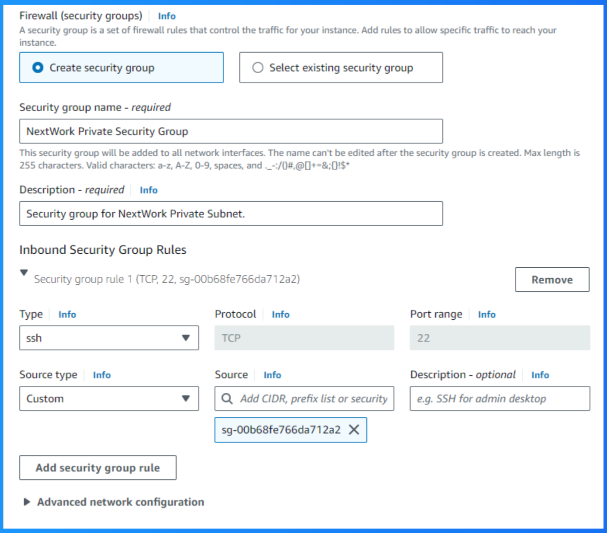
▼ Network Interfaces (1) Info



Launching a private server

My private server has its own dedicated security group because the NextWork public security group allows in All HTTP traffic - which would leave our private server much more vulnerable to security attacks/risks.

My private server's security group's source is my NextWork Public Security Group, which means only SSH traffic coming from resources associated with that security group would be allowed.



Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

Security group name - *required*

NextWork Private Security Group

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* Info

Security group for NextWork Private Subnet.

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, sg-00b68fe766da712a2) Remove

Type: ssh
Protocol: TCP
Port range: 22

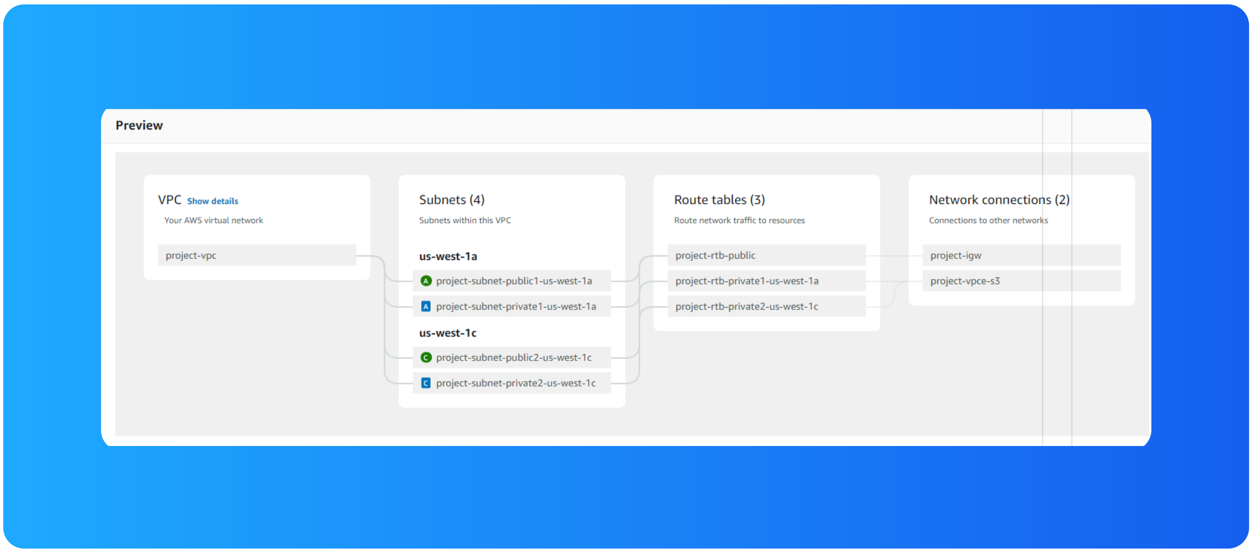
Source type: Custom
Source: *Add CIDR, prefix list or security*
sg-00b68fe766da712a2 ✕
Description - *optional*: *e.g. SSH for admin desktop*

Speeding up VPC creation

I used an alternative way to set up an Amazon VPC! This time, I used the 'VPC and more' option, which gives me a VPC resource map to use when creating the VPC and all of its components e.g. Security Groups, Route tables, and Internet Gateways.

A VPC resource map is a visual diagram that maps out my VPC components and the relationships/connects between them. A resource map is interactive i.e it will highlight the connections relevant to a resource that I highlight/hover over.

My new VPC has a CIDR block of 10.0.0.0/16. It is possible for my new VPC to have the same IPv4 CIDR block as my existing VPC because VPCs are already isolated from each other. Still, this is not best practice if we need VPC peering.

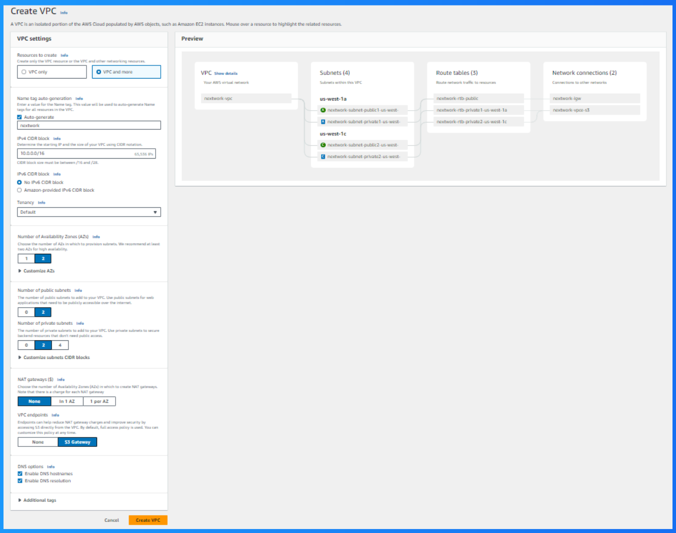

Preview
VPC Show details
Your AWS virtual network
project-vpc
Subnets (4)
Subnets within this VPC
us-west-1a
A project-subnet-public1-us-west-1a
A project-subnet-private1-us-west-1a
us-west-1c
C project-subnet-public2-us-west-1c
C project-subnet-private2-us-west-1c
Route tables (3)
Route network traffic to resources
project-rtb-public
project-rtb-private1-us-west-1a
project-rtb-private2-us-west-1c
Network connections (2)
Connections to other networks
project-igw
project-vpce-s3

Speeding up VPC creation

Tips for using the VPC resource map

When determining the number of public subnets in my VPC, I only had two options either none or one in each Availability zone for my VPC. This was because it is best practice (improves redundancy and high availability) to have at least one subnet/AZ.

The set up page also offered to create NAT gateways, which are connectors/gateways that will let resources in my private subnet get access to the internet (e.g. for security updates) while blocking off the incoming traffic from the internet.



Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.

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 auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.
☑ Auto-generate
nextwork

IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.
10.0.0.0/16 65,536 IPs
CIDR block size must be between /16 and /28.

IPv6 CIDR block Info
● No IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block

Tenancy Info
Default

Number of Availability Zones (AZs) Info
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.
1 [✓ 2]

Number of public subnets Info
The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.
0 [✓ 2]

Number of private subnets Info
The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.
0 [✓ 2] 4

NAT gateways ($) Info
Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway
[✓ None] In 1 AZ 1 per AZ

VPC endpoints Info
Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.
None [✓ S3 Gateway]

DNS options Info
☑ Enable DNS hostnames
☑ Enable DNS resolution

Preview

VPC Show details
Your AWS virtual network
nextwork-vpc

Subnets (4)
Subnets within this VPC
us-west-1a
nextwork-subnet-public1-us-west-
nextwork-subnet-private1-us-west-
us-west-1c
nextwork-subnet-public2-us-west-
nextwork-subnet-private2-us-west-

Route tables (3)
Route network traffic to resources
nextwork-rtb-public
nextwork-rtb-private1-us-west-1a
nextwork-rtb-private2-us-west-1c

Network connections (2)
Connections to other networks
nextwork-igw
nextwork-vpce-s3

Everyone should be in a job they love.

Check out nextwork.org for more projects