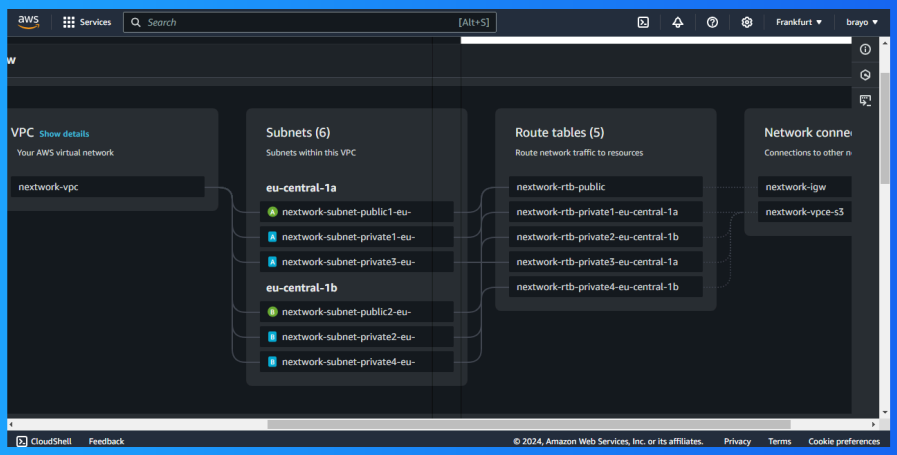
NextWork.org

Launching VPC Resources

Brian Kimemia N



Brian Kimemia N
NextWork Student

NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon Virtual Private Cloud enables users to create a logically isolated network in the AWS cloud, providing control over IP addressing, subnets, route tables, and security. It ensures secure, customizable network configurations for AWS resources.

How I used Amazon VPC in this project

I used Amazon VPC to design secure, isolated network environments for deploying AWS resources, configuring subnets, route tables, and security groups to control access and optimize data flow between instances and external services.

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

One thing I didn't expect in this project was the level of detail required to configure network ACLs and security groups and CIDR block allocations correctly to ensure proper isolation and security between subnets.

This project took me...

This project took me a few hours to complete, including setting up the VPC, configuring public and private subnets,CIDR block allocations , creating route tables, and establishing network ACLs to ensure proper security and traffic flow.

Brian Kimemia N
NextWork Student

NextWork.org

Setting Up Direct VM Access

Directly accessing a virtual machine means connecting to the EC2 instance via SSH (Linux) or RDP (Windows) to interact with the instance's operating system, manage files, and configure applications or services without using additional intermediaries.

SSH is a key method for directly accessing a VM

SSH traffic means Secure Shell traffic, a protocol used to securely connect to remote systems over a network, allowing users to manage servers and transfer files with encryption.

To enable direct access, I set up key pairs

Key pairs are a set of cryptographic keys used for secure SSH access to EC2 instances. They consist of a public key, stored on the instance, and a private key, which is kept securely by the user. The private key is used to authenticate the user.

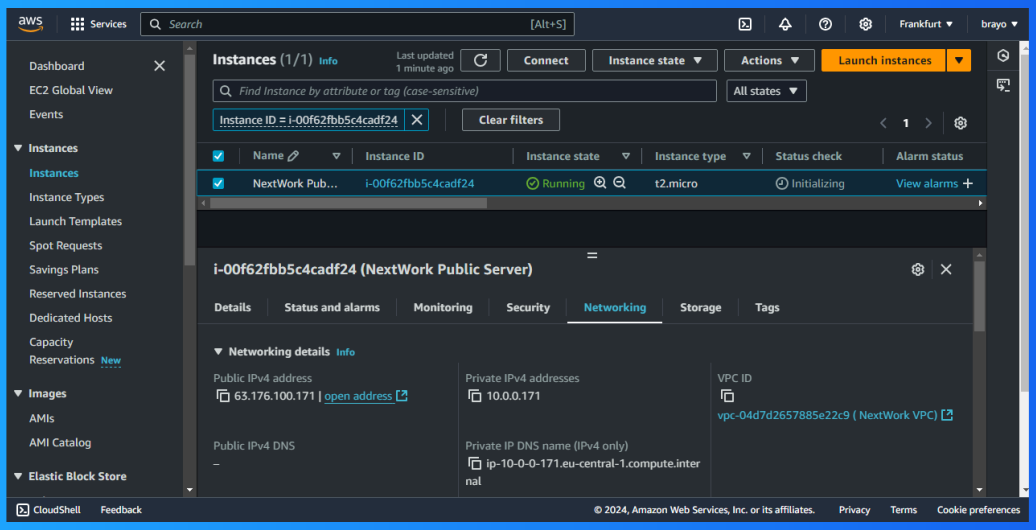
A private key's file format means the structure in which the key is saved, typically in PEM or PPK format. My private key's file format was PEM.

Brian Kimemia N
NextWork Student

NextWork.org

Launching a public server

I had to change my EC2 instance's networking settings by modifying the security groups, adjusting inbound and outbound rules, and updating the network interface configurations through the AWS Management Console.



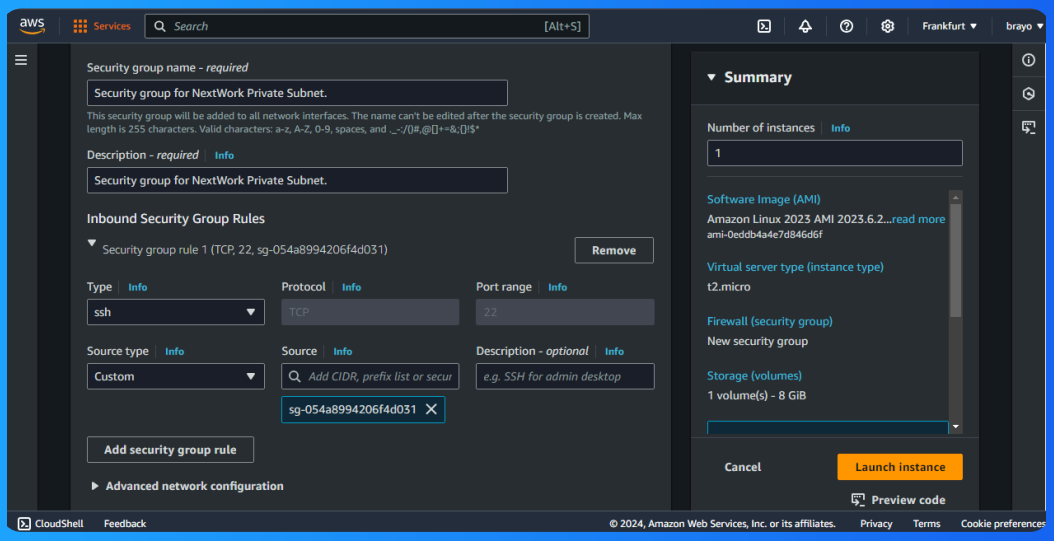
Brian Kimemia N
NextWork Student

NextWork.org

Launching a private server

My private server has its own dedicated security group because it requires different access controls than the public server, ensuring restricted access to sensitive resources while allowing the public server to be more accessible to external traffic.

My private server's security group's source is the security group of the public server, which means the private server allows traffic only from the public server, ensuring controlled and secure communication between the two.



Brian Kimemia N
NextWork Student

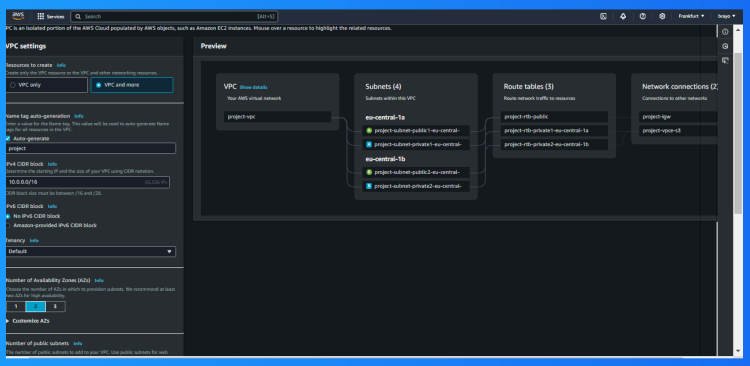
NextWork.org

Speeding up VPC creation

I used an alternative way to set up an Amazon VPC! This time, I manually created a VPC (CIDR block 10.0.0.0/16), added public & private subnets (CIDR blocks 10.0.0.0/24 & 10.0.1.0/24) configured a custom route table and network ACLs for security.

A VPC resource map is a visual representation of the resources within a Virtual Private Cloud (VPC), such as subnets, route tables, security groups, and network ACLs, helping to manage and understand the network architecture and their relationships.

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 they are separate, isolated networks,AWS allows multiple VPCs with same CIDR block in different regions or accounts.



Brian Kimemia N
NextWork Student

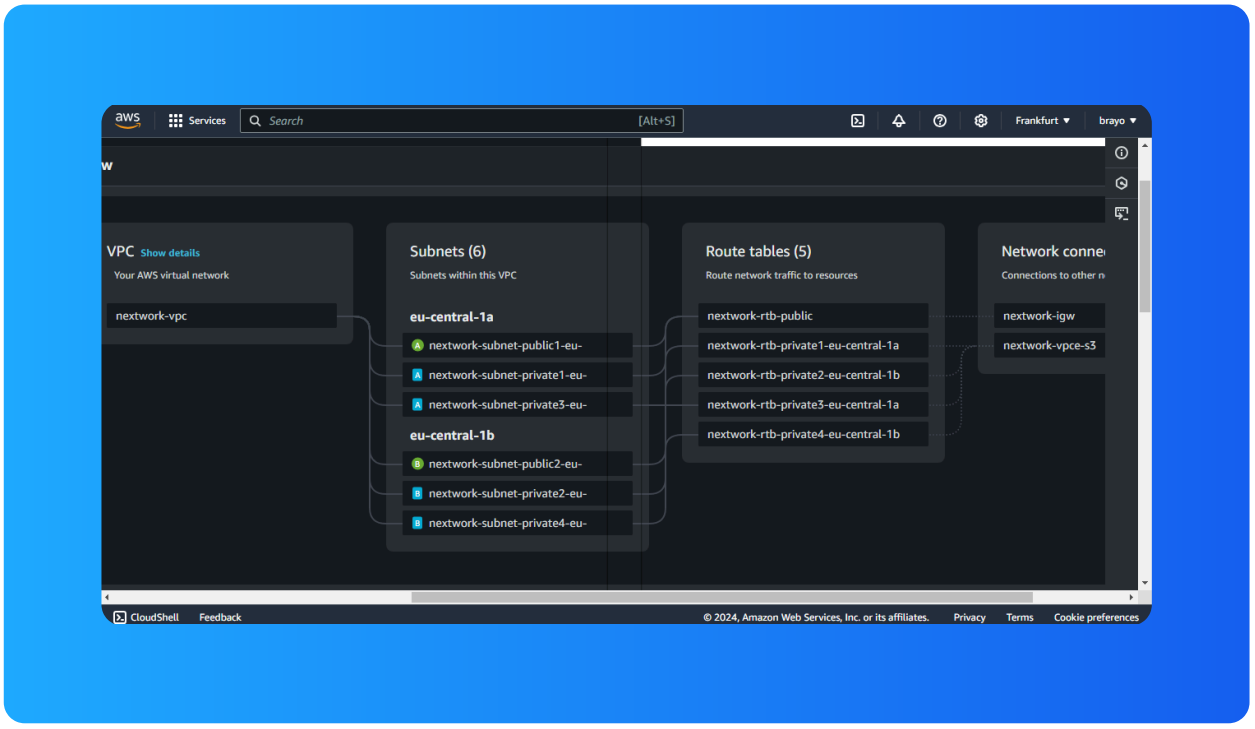
NextWork.org

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: one subnet in each availability zone. This was because I used a CIDR block of 10.0.0.0/16, can accommodate multiple subnets,but public subnets number is region dependent

The setup page also offered to create NAT gateways, which are managed services that allow instances in a private subnet to access the internet securely while preventing inbound internet traffic to those instances.



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects