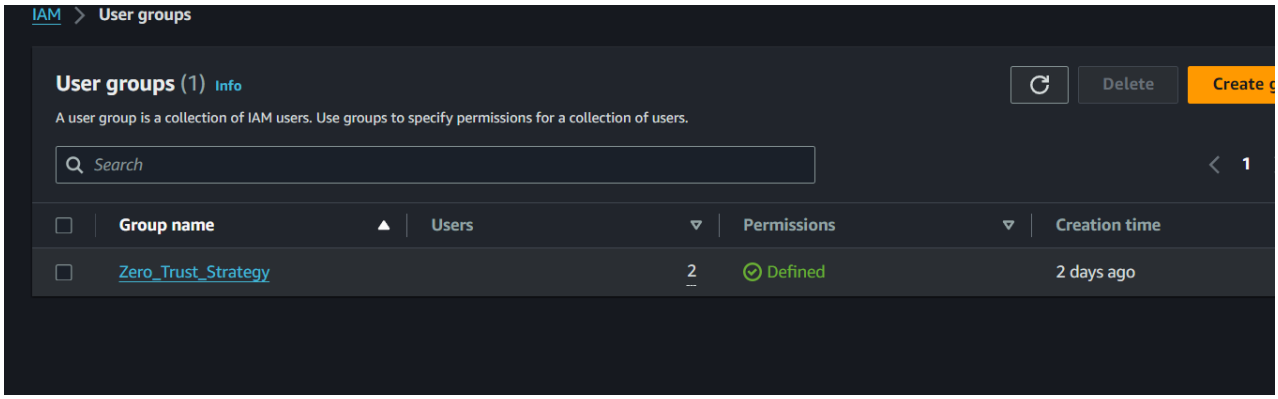
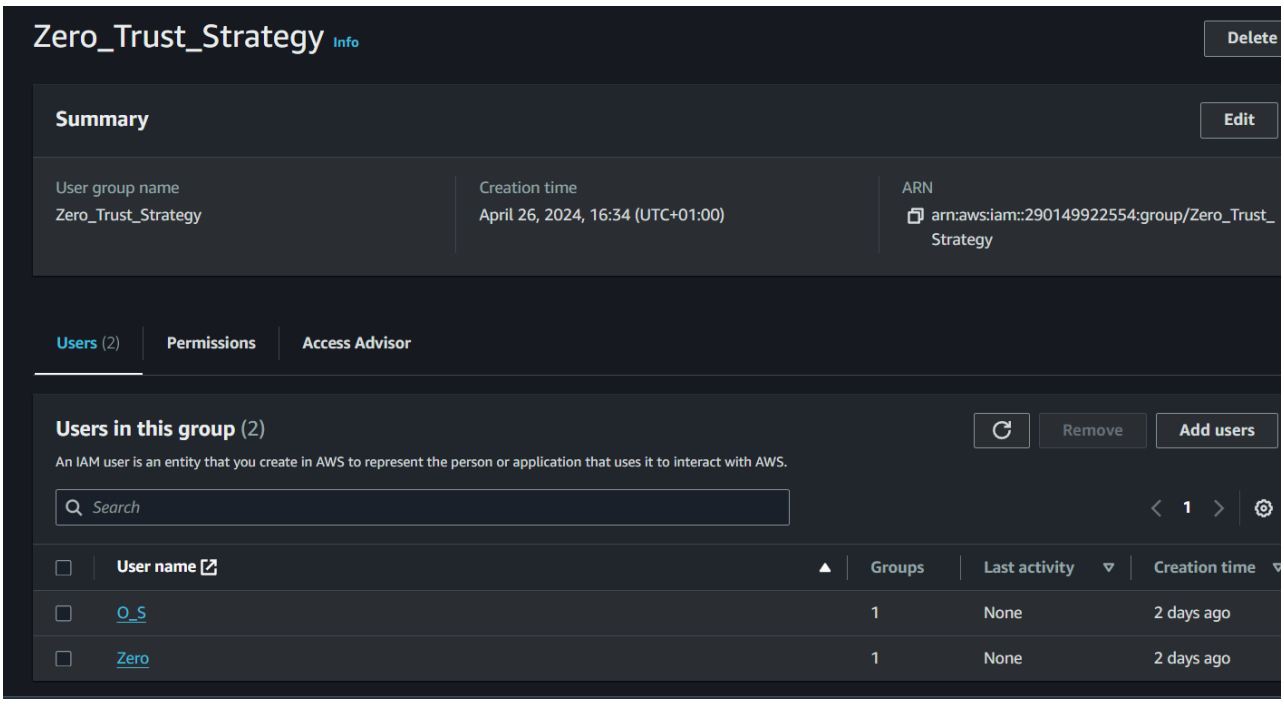
Zero Trust Strategy by Osman Hamza

In this project, I will create a zero-trust strategy using AWS environment. I will create a user group from IAM (Identity and Access Management) and assign them different permissions and policies. This is a best practice to ensure that users only have access to information essential them.

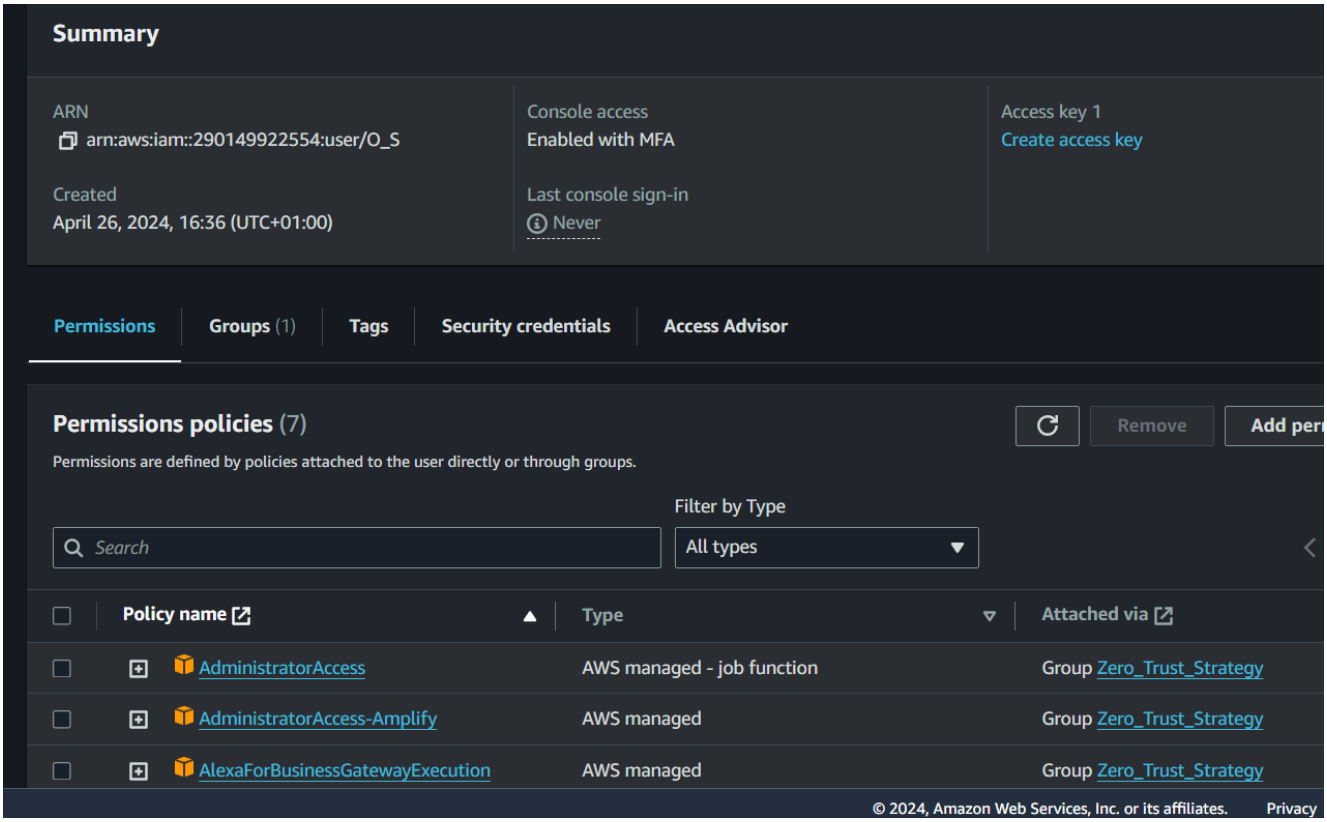
IAM



In the picture above, I have created a user group from IAM. The group is called Zero_Trust_Strategy

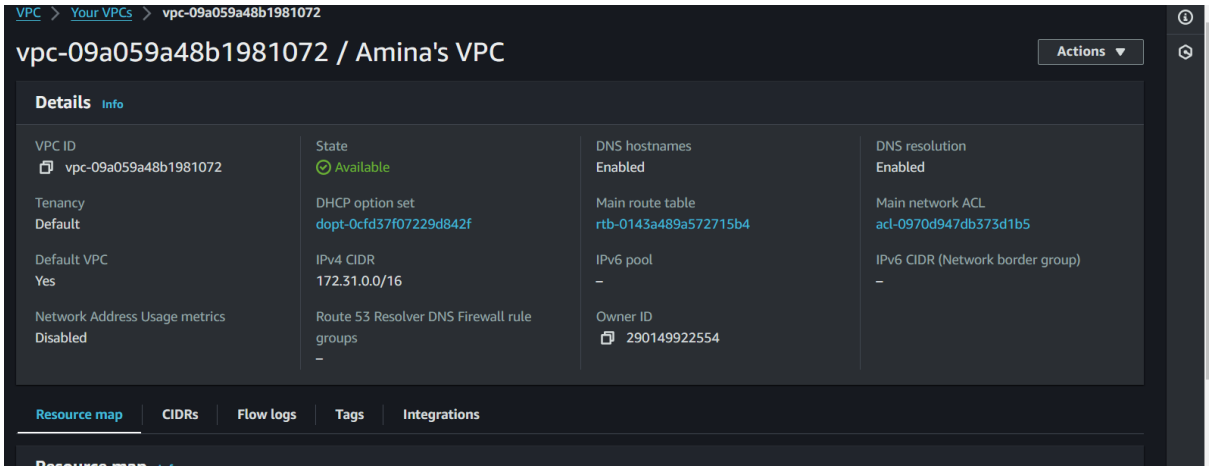


In the IAM dashboard, as it can be seen, I have created 2 users in the group and configured them with roles, policies, and trust relationships to ensure that access is granted strictly based on the necessity.

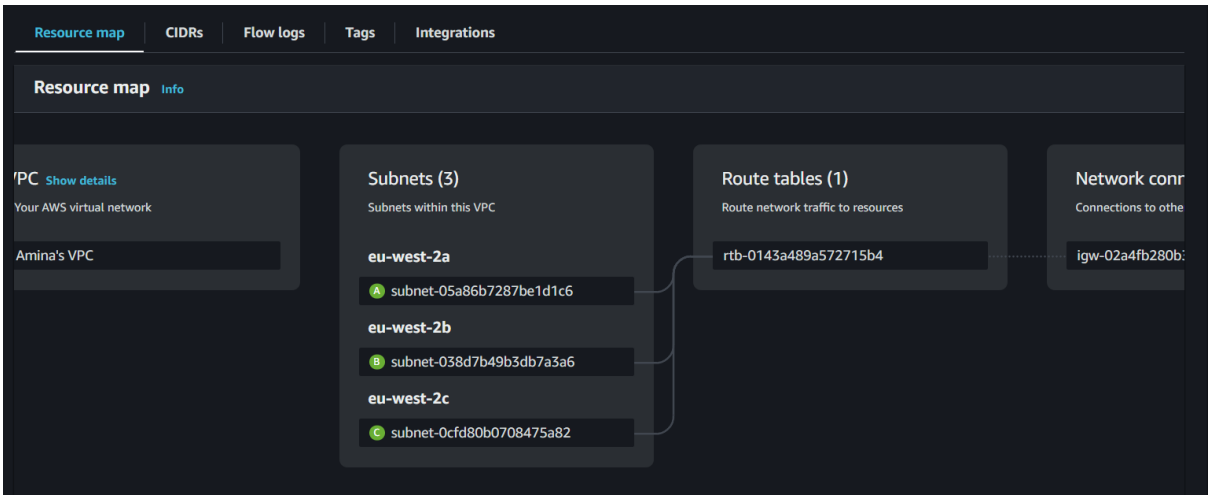


In the image above, I have configured the permissions to the users I have created. As it can be seen, I have given administrative access to O_S user which means he would have admin privileges to the systems. This went for the other user but unlike O_S User having the highest-level access, the user has the least level of access. This is to demonstrate how zero trust strategy would have an effect on a real-life scenario for an organisation.

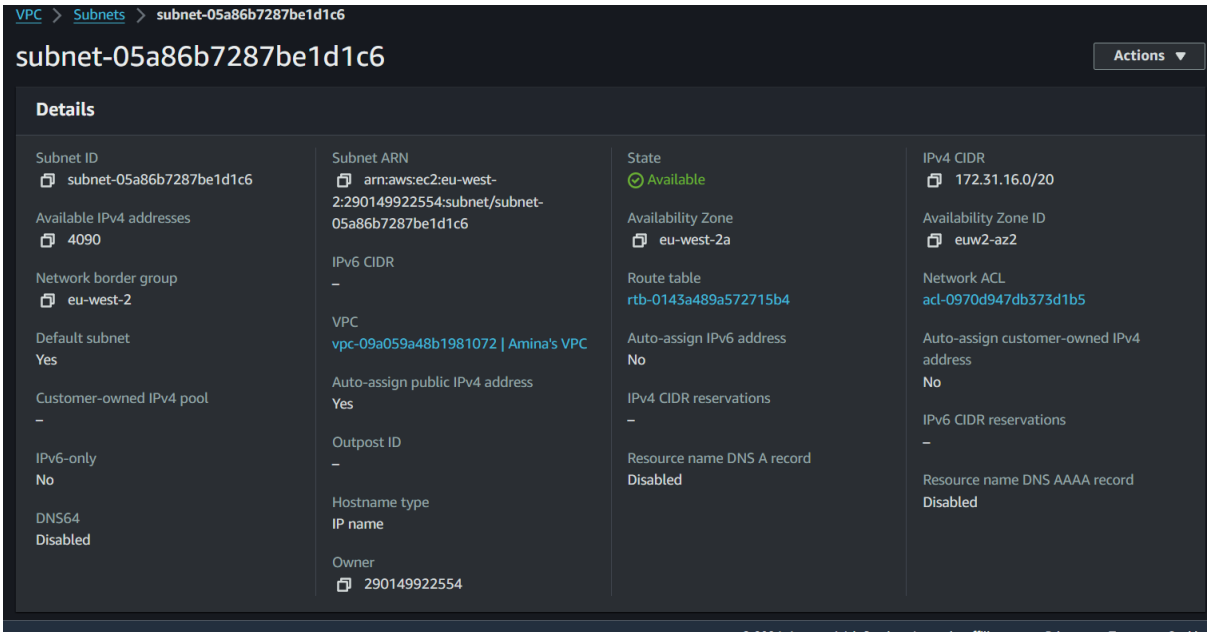
VPC configuration



In the image above, I have created a VPC, virtual private cloud. In this VPC, I will be configuring it with subnets and network segmentation and firewalls to ensure restrict and safe traffic.

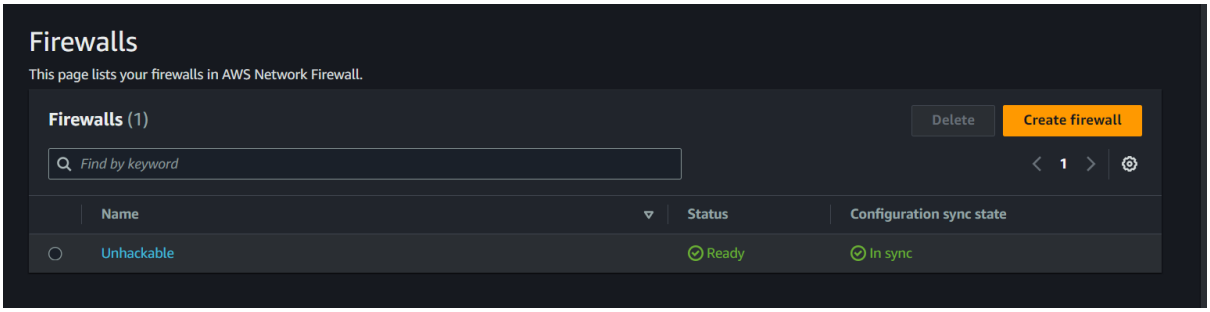


In here I have created 3 subnets for the VPC I created. This is one of the subnets I have created. This the resource map and as it can be seen, we have see the subnet property including route tables and network connections that I have configured.

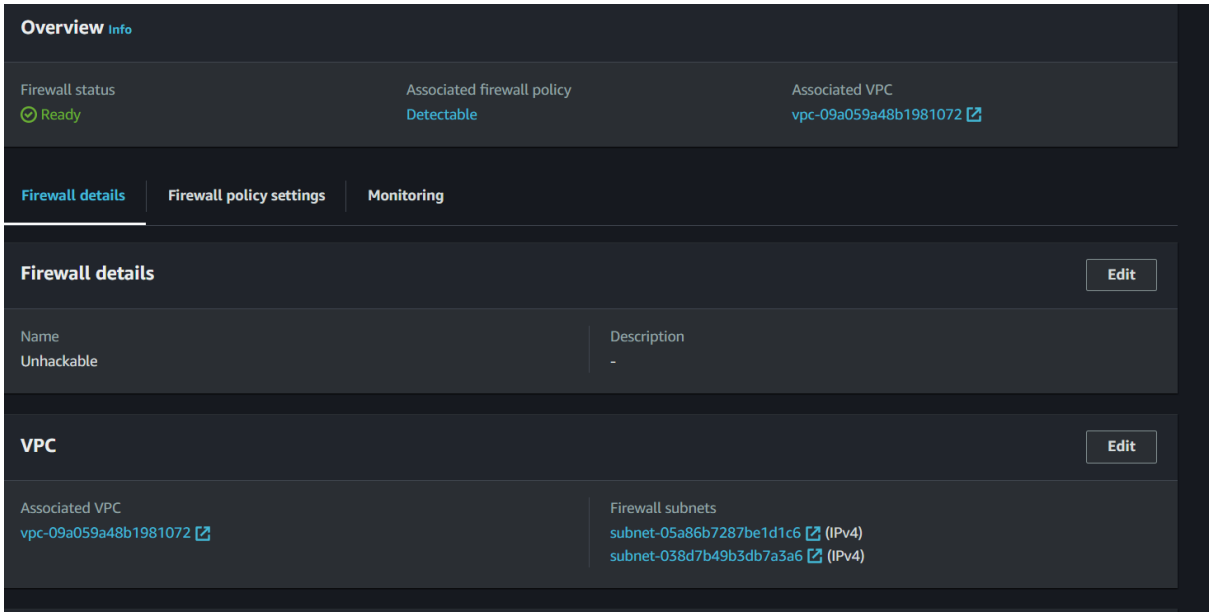


In this dashboard, we can view each subnet individually and see their critical information including subnet ID, border group, availability zone, ipv4 CIDR, the state of the subnet.

Firewall configuration



In this picture, I have created and configured a firewall for my VPC to protect and restrict the network traffic.



In here, this is the firewall dashboard and as it can be seen. I have configured it and connected it with my VPC, and the firewall status is ready and actively monitoring the network traffic.

What is zero-trust model and why I have used AWS to create a model?

Amazon Web Services, or AWS, offers a strong foundation for putting a zero-trust security approach into practice. With the help of AWS's many services and capabilities, businesses can set up strict access controls, keep an eye on and monitor user behaviour, encrypt data while it's in transit and at rest, and use multi-factor authentication (MFA). AWS Identity and Access Management (IAM) further enables enterprises to set up fine-grained policies and permissions to control who has access to AWS resources.

The zero-trust model is a security concept makes sure that there should never be any trust, not even on an internal network of a company. Traditionally, network security relied on the perimeter defense model, where access to resources within the network was granted based on the assumption that users and devices inside the network could be trusted.