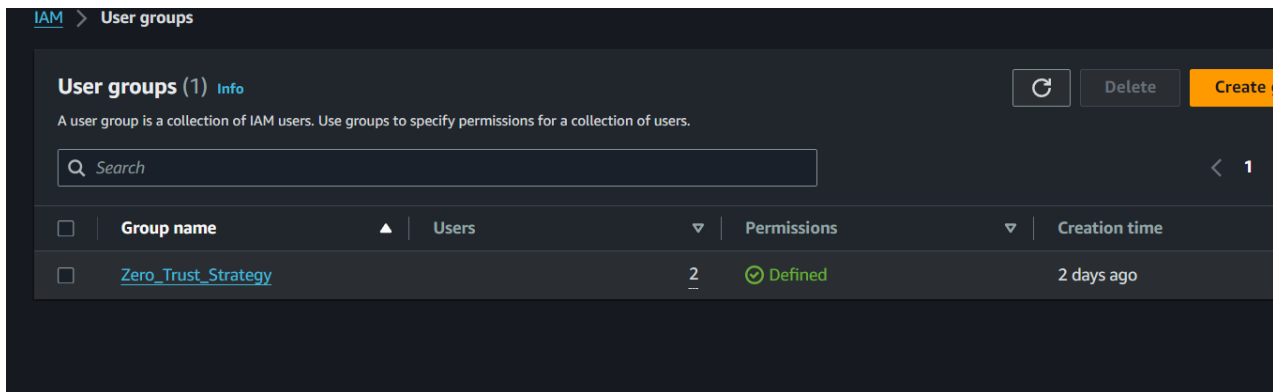


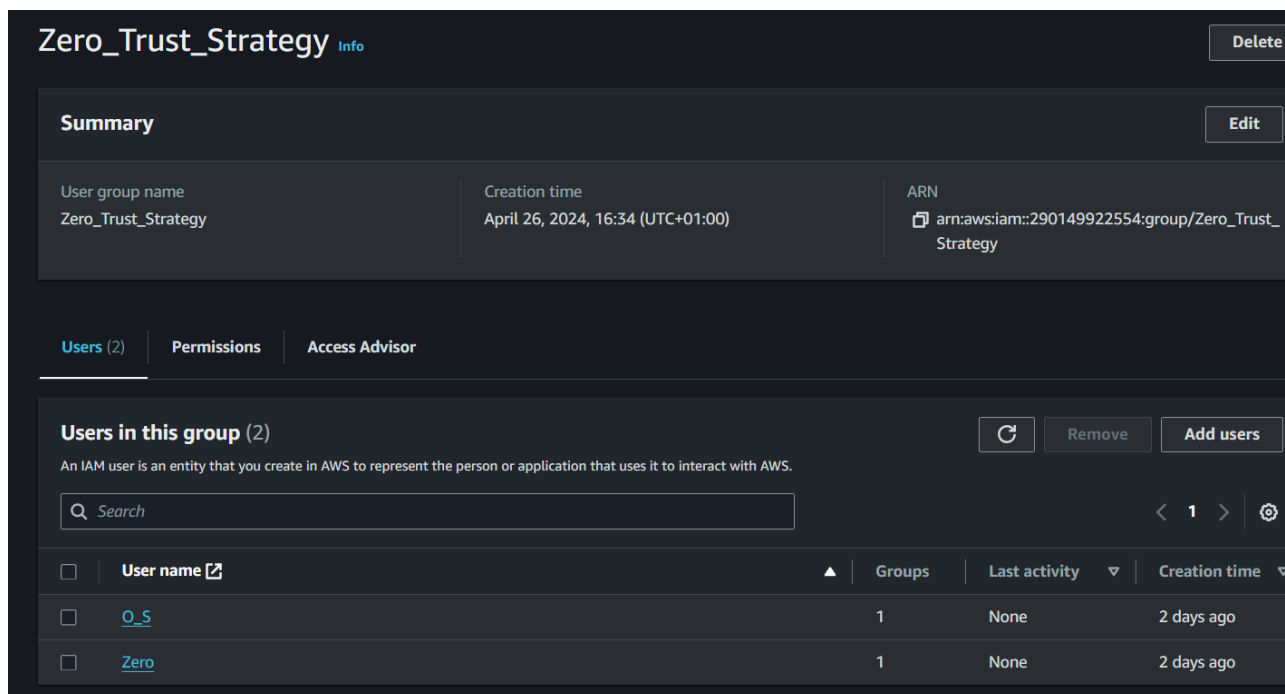
Zero Trust Strategy by Osman Hamza

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.

Summary

ARN

arn:aws:iam::290149922554:user/O_S

Created

April 26, 2024, 16:36 (UTC+01:00)

Console access

Enabled with MFA

Last console sign-in

Never

Access key 1

Create access key

Permissions

Groups (1)

Tags

Security credentials

Access Advisor

Permissions policies (7)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type

All types

	Policy name	Type	Attached via
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function	Group Zero_Trust_Strategy
<input type="checkbox"/>	AdministratorAccess-Amplify	AWS managed	Group Zero_Trust_Strategy
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	AWS managed	Group Zero_Trust_Strategy

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy

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

VPC > Your VPCs > vpc-09a059a48b1981072

vpc-09a059a48b1981072 / Amina's VPC

Details

Info

VPC ID vpc-09a059a48b1981072	State Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-0cfd37f07229d842f	Main route table rtb-0143a489a572715b4	Main network ACL acl-0970d947db373d1b5
Default VPC Yes	IPv4 CIDR 172.31.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 290149922554	

Resource map

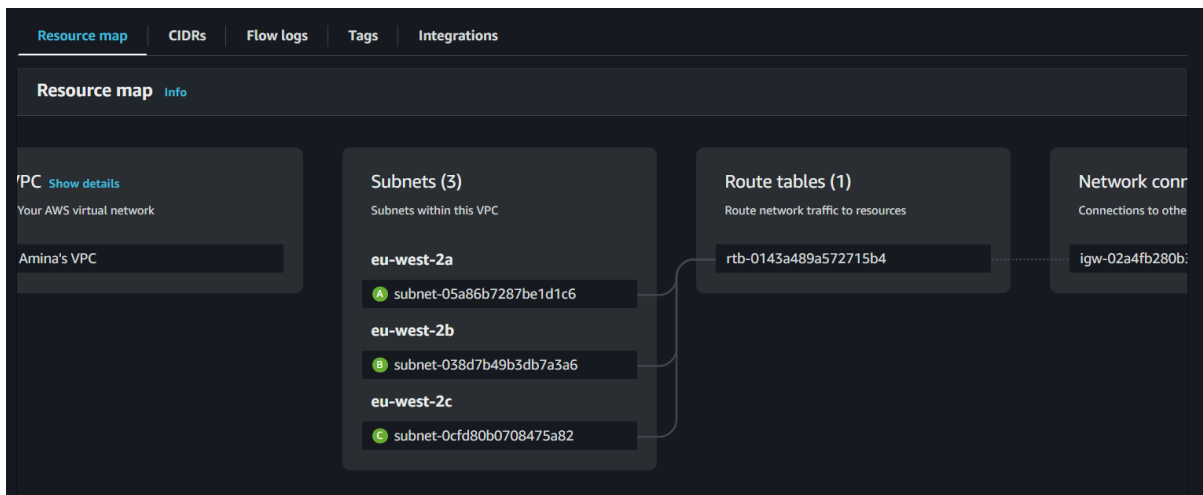
CIDRs

Flow logs

Tags

Integrations

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.

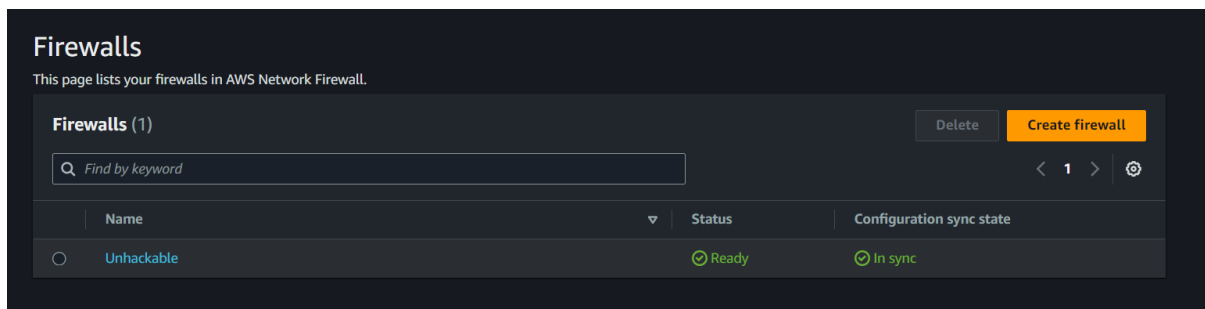


In here I have created 3 subnets for the VPC I created. This is one of the subnets I have created. This the resource map and as it can be seen, we have see the subnet property including route tables and network connections that I have configured.

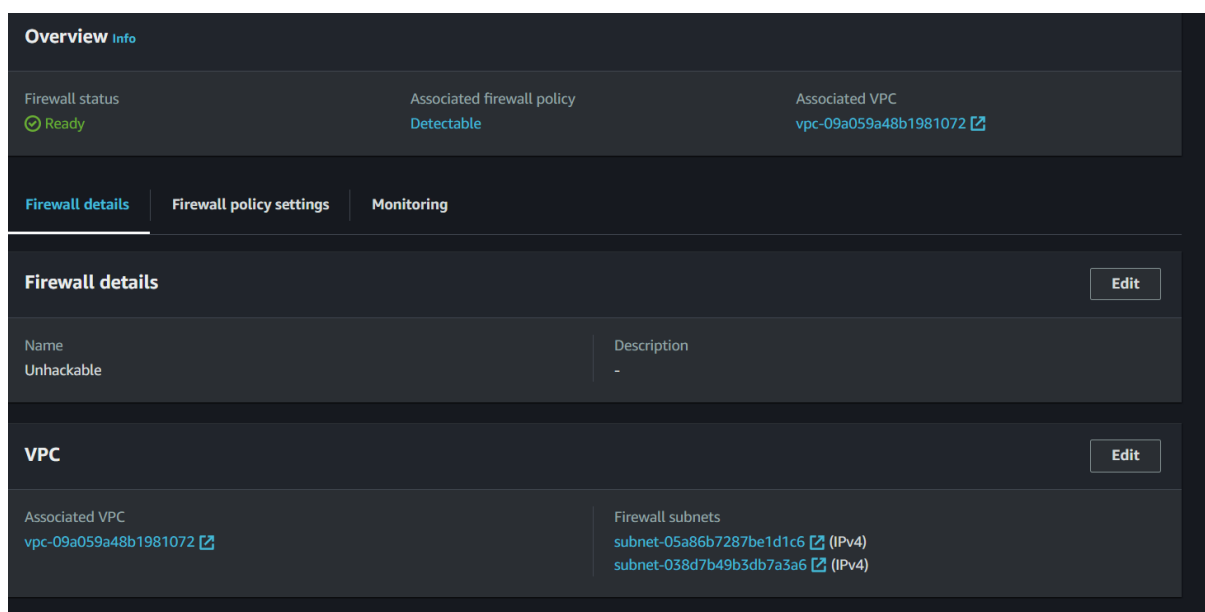
VPC > Subnets > subnet-05a86b7287be1d1c6			
subnet-05a86b7287be1d1c6			
Details			
Subnet ID subnet-05a86b7287be1d1c6	Subnet ARN arn:aws:ec2:eu-west-2:290149922554:subnet/subnet-05a86b7287be1d1c6	State Available	IPv4 CIDR 172.31.16.0/20
Available IPv4 addresses 4090	IPv6 CIDR -	Availability Zone eu-west-2a	Availability Zone ID euw2-az2
Network border group eu-west-2	VPC vpc-09a059a48b1981072 Amina's VPC	Route table rtb-0143a489a572715b4	Network ACL acl-0970d947db373d1b5
Default subnet Yes	Auto-assign public IPv4 address Yes	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No
Customer-owned IPv4 pool -	Outpost ID -	IPv4 CIDR reservations -	IPv6 CIDR reservations -
IPv6-only No	Hostname type IP name	Resource name DNS A record Disabled	Resource name DNS AAAA record Disabled
DNS64 Disabled	Owner 290149922554		

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.