SIEM REGIME AWS COMPREHENSIVE BREAKDOWN

SIEM REGIME has created roles, users, groups, policies, and permissions for each organization to utilize and control.

An IAM role is a set of permissions that can be assumed by an entity, such as a user, application, or service. Roles are not users, but rather a set of permissions that can be granted to a user or service. Roles are used to grant access to AWS resources without sharing the user's credentials.

An IAM user is a unique identity within your AWS account. Users are used to authenticate with AWS services and can be granted access to specific resources. Each user has a unique username and password and can be associated with one or more roles.

An IAM group is a collection of IAM users that you can manage as a single unit. Groups can be used to simplify access management and make it easier to manage permissions for multiple users.

An IAM policy is a set of permissions that define what actions can be performed on specific resources. Policies can be attached to IAM users, groups, or roles, and can be used to grant or deny access to specific AWS resources.

Permissions are the specific actions that can be performed on AWS resources. There are two types of permissions:

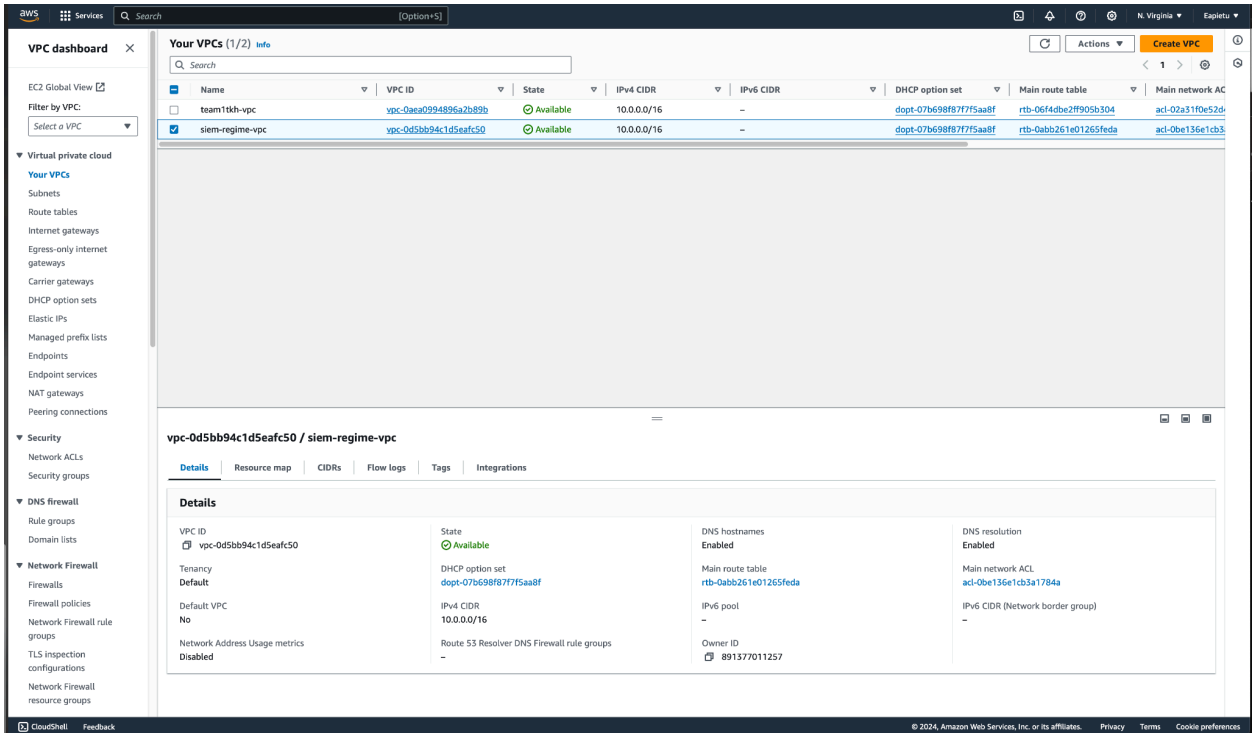
1. Actions: Specific actions that can be performed on an AWS resource, such as "S3: List Buckets" or "EC2: Describe Instances".
2. Resources: The specific AWS resources that the actions can be performed on, such as a specific S3 bucket or an EC2 instance.

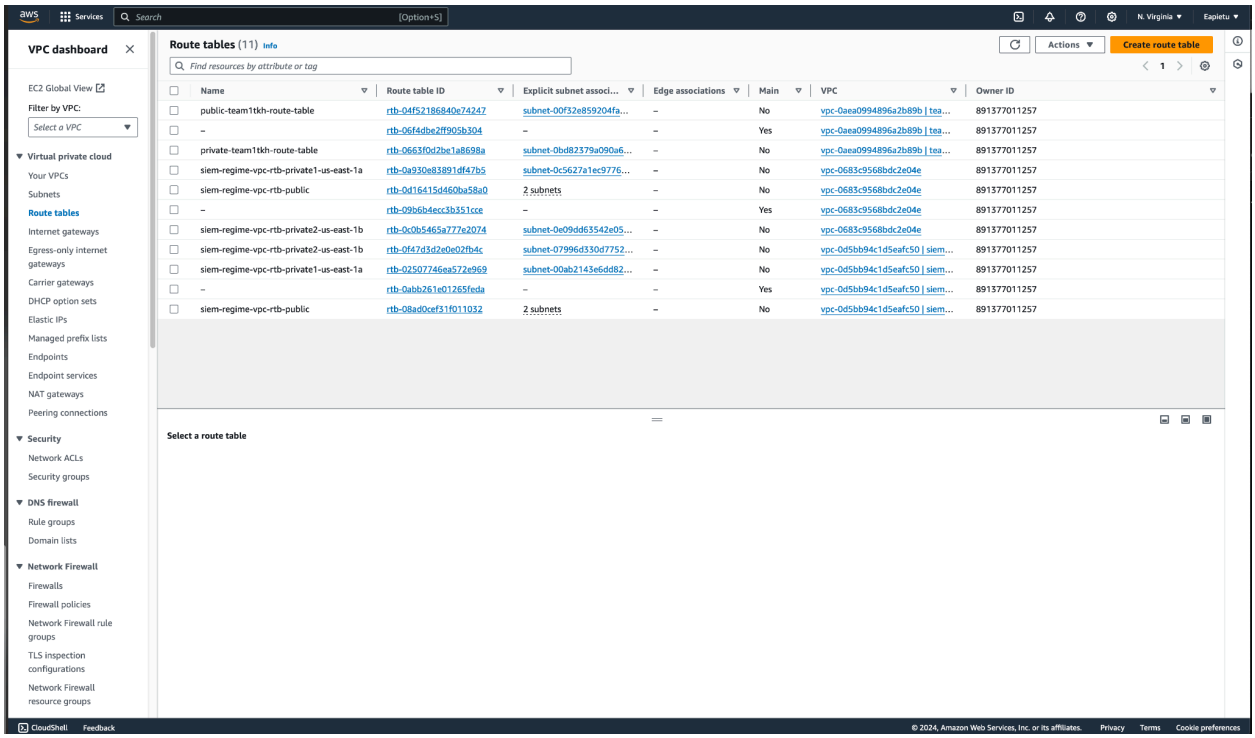
SIEM functionalities and secure virtual network architecture within the cloud platform is used to segregate SIEM components and manage data access for AWS. The following will be considered as components:

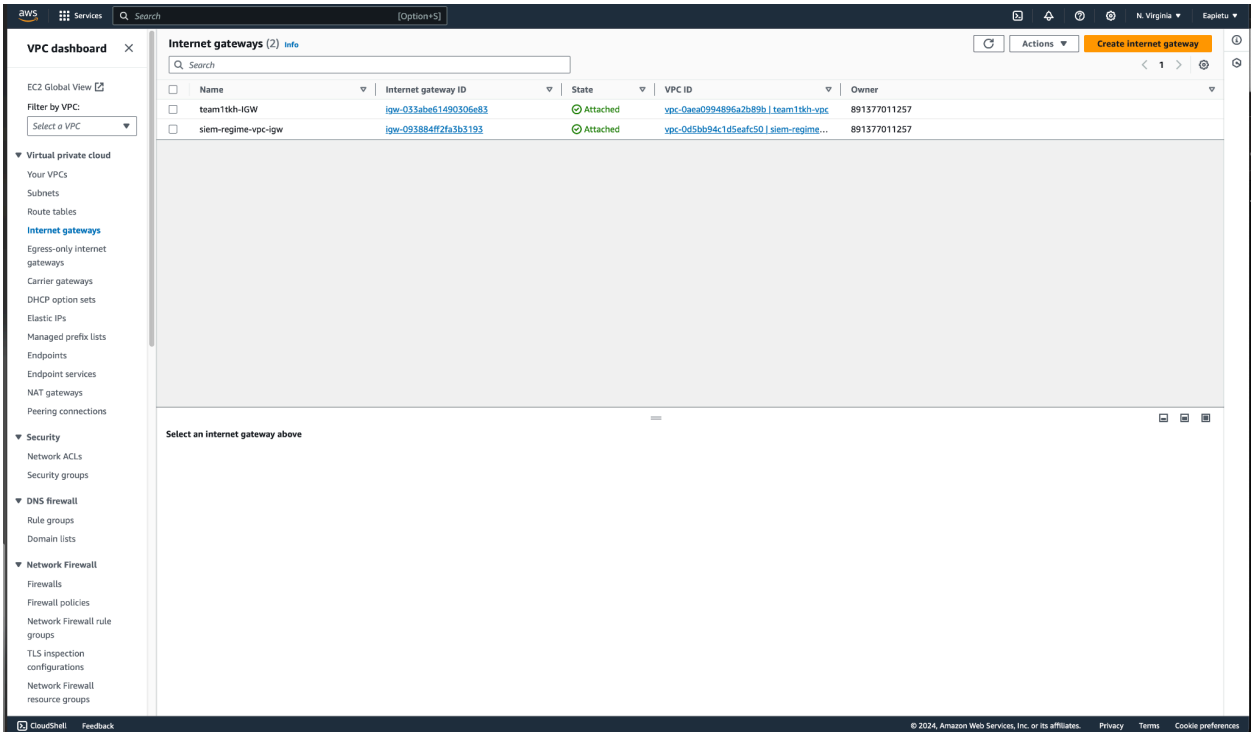
Network Segmentation:

Create multiple virtual private clouds (VPCs) to segregate SIEM components, each with its own security group and network ACLs. This will help prevent lateral movement in case of a breach.

Attached below are photos from our AWS to display VPCs setup.


VPC dashboard
Your VPCs (1/2) Info
Actions
Create VPC
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
DHCP option set
Main route table
team1tkh-vpc
vpc-0aea099489 6a2b89b
Available
10.0.0.0/16
dopt-07b698f87f7f5aa8f
rtb-06f4dbe2ff905b304
siem-regime-vpc
vpc-0d5bb94c1d5eafc50
Available
10.0.0.0/16
dopt-07b698f87f7f5aa8f
rtb-0abb261e01265feda
vpc-0d5bb94c1d5eafc50 / siem-regime-vpc
Details
Resource map
CIDRs
Flow logs
Tags
Integrations
VPC ID
vpc-0d5bb94c1d5eafc50
State
Available
DNS hostnames
Enabled
DNS resolution
Enabled
Tenancy
Default
DHCP option set
dopt-07b698f87f7f5aa8f
Main route table
rtb-0abb261e01265feda
Main network ACL
acl-0be136e1cb3a1784a
Default VPC
No
IPv4 CIDR
10.0.0.0/16
IPv6 pool
–
IPv6 CIDR (Network border group)
–
Network Address Usage metrics
Disabled
Route 53 Resolver DNS Firewall rule groups
–
Owner ID
891377011257


VPC dashboard
Route tables (11) Info
Actions
Create route table
Name
Route table ID
Explicit subnet associ...
Edge associations
Main
VPC
Owner ID
public-team1tkh-route-table
rtb-04f52186840e74247
subnet-00f32e859204fa...
–
No
vpc-0aea0994896a2b89b | tea...
891377011257
–
rtb-06f4dbe2ff905b304
–
–
Yes
vpc-0aea0994896a2b89b | tea...
891377011257
private-team1tkh-route-table
rtb-0663f0d2be1a8698a
subnet-0bd82379a090a6...
–
No
vpc-0aea0994896a2b89b | tea...
891377011257
siem-regime-vpc-rtb-private1-us-east-1a
rtb-0a930e83891df47b5
subnet-0c5627a1ec9776...
–
No
vpc-0683c9568bdc2e04e
891377011257
siem-regime-vpc-rtb-public
rtb-0d16415d460ba58a0
2 subnets
–
No
vpc-0683c9568bdc2e04e
891377011257
–
rtb-09b6b4ecc3b351cce
–
–
Yes
vpc-0683c9568bdc2e04e
891377011257
siem-regime-vpc-rtb-private2-us-east-1b
rtb-0c0b5465a777e2074
subnet-0e09dd63542e05...
–
No
vpc-0683c9568bdc2e04e
891377011257
siem-regime-vpc-rtb-private2-us-east-1b
rtb-0f47d3d2e0e02fb4c
subnet-07996d330d7752...
–
No
vpc-0d5bb94c1d5eafc50 | siem...
891377011257
siem-regime-vpc-rtb-private1-us-east-1a
rtb-02507746ea572e969
subnet-00ab2143e6dd82...
–
No
vpc-0d5bb94c1d5eafc50 | siem...
891377011257
–
rtb-0abb261e01265feda
–
–
Yes
vpc-0d5bb94c1d5eafc50 | siem...
891377011257
siem-regime-vpc-rtb-public
rtb-08ad0cef31f011032
2 subnets
–
No
vpc-0d5bb94c1d5eafc50 | siem...
891377011257
Select a route table



Subnets:

Create separate subnets for each SIEM component, such as:

- Log collection (e.g., CloudWatch logs, AWS Config logs)
- Log analysis and correlation
- Alerting and notification
- Data storage and retention

Attached below is our AWS account subnets from the VPC.

IAM Roles:

Assign specific IAM roles to each SIEM component to control access to resources and services.

For example:

- A log collection role with read-only access to CloudWatch logs

- A log analysis role with read-only access to S3 buckets containing log data
- An alerting role with write access to SNS topics for notifications

Role-Based Access Control (RBAC) for SIEM (Security Information and Event Management) is a critical component of securing and managing access to sensitive security-related data.

RBAC Examples:

- Security Analyst Role: This role has permissions to view logs, configure alerts, and access sensitive data.
- Network Administrator Role: This role has permissions to manage network devices, configure network settings, and access sensitive data.
- Compliance Officer Role: This role has permissions to view logs, configure alerts, and access sensitive data for compliance purposes.

By implementing RBAC in a SIEM system, organizations can improve security, simplify management, and ensure compliance with regulatory requirements.

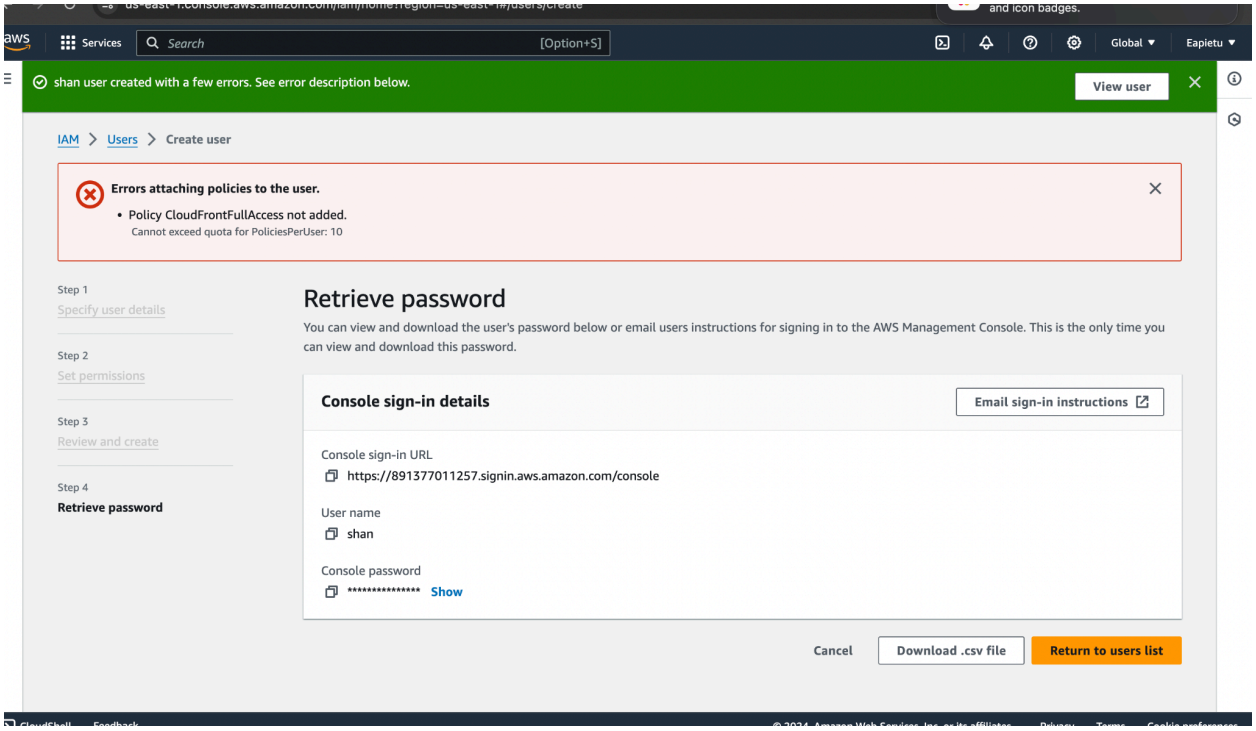
IAM Policies:

Create IAM policies to define the permissions for each SIEM component.

For example:

- A policy that allows a log collection role to read CloudWatch logs
- A policy that allows a log analysis role to read S3 buckets containing log data
- A policy that allows an alerting role to write to SNS topics

Attached is a photo from our AWS account showing a user with limited permissions.



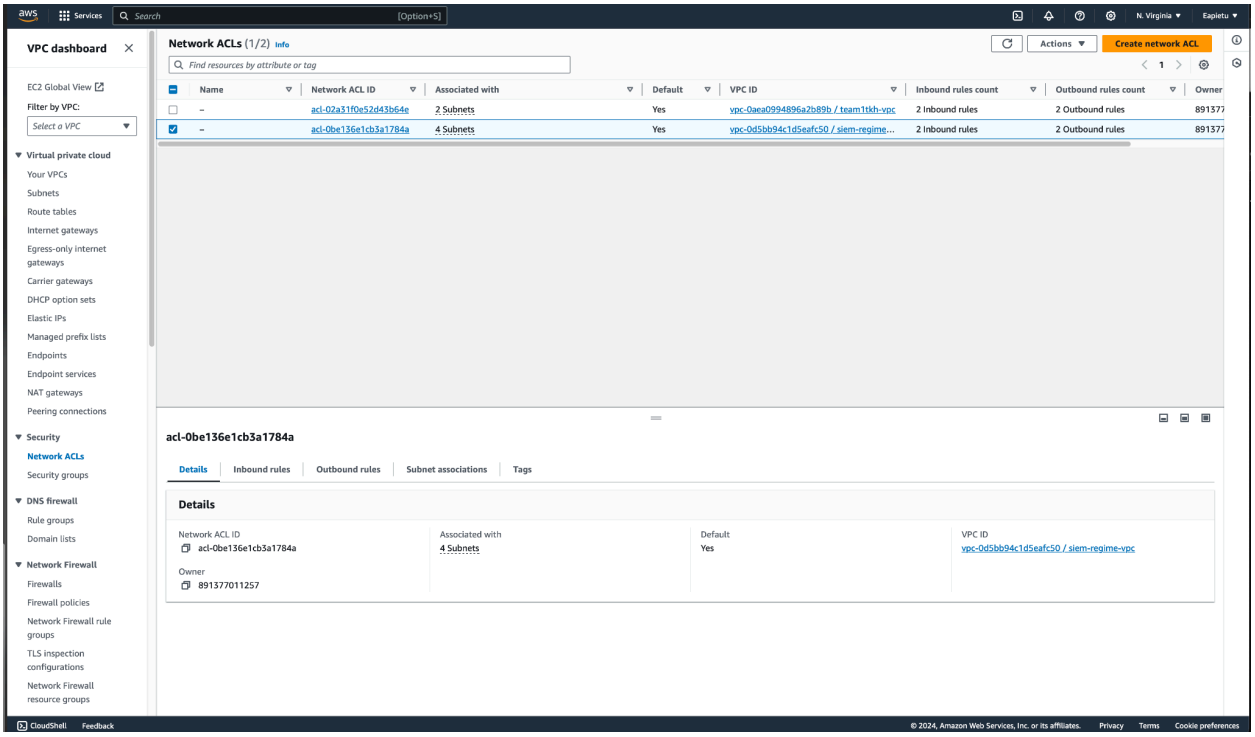
Network Access Control Lists (ACLs):

Configure network ACLs to control incoming and outgoing traffic between subnets and VPCs.

For example:

- Allow incoming traffic from the internet to the log collection subnet
- Allow outgoing traffic from the log analysis subnet to the data storage subnet
- Deny all incoming traffic from the internet to the data storage subnet

Attached below is a photo from our AWS account to display the NACLs.



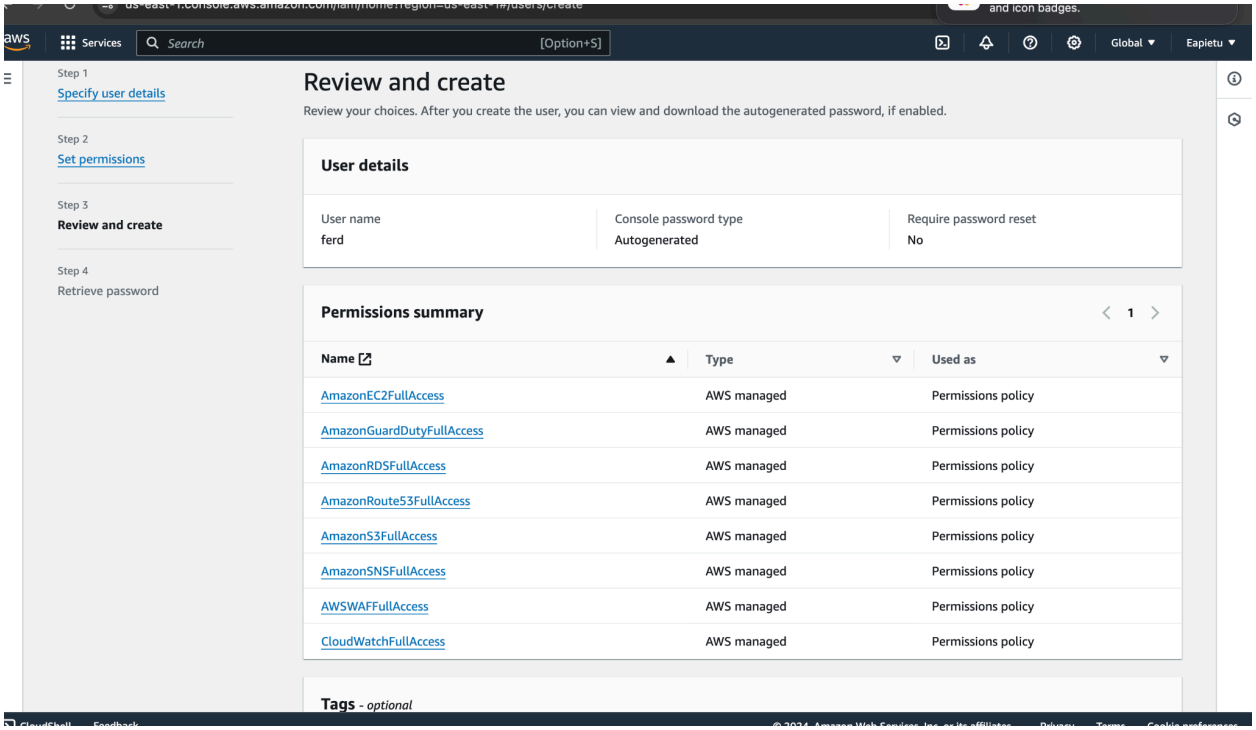
Security Groups:

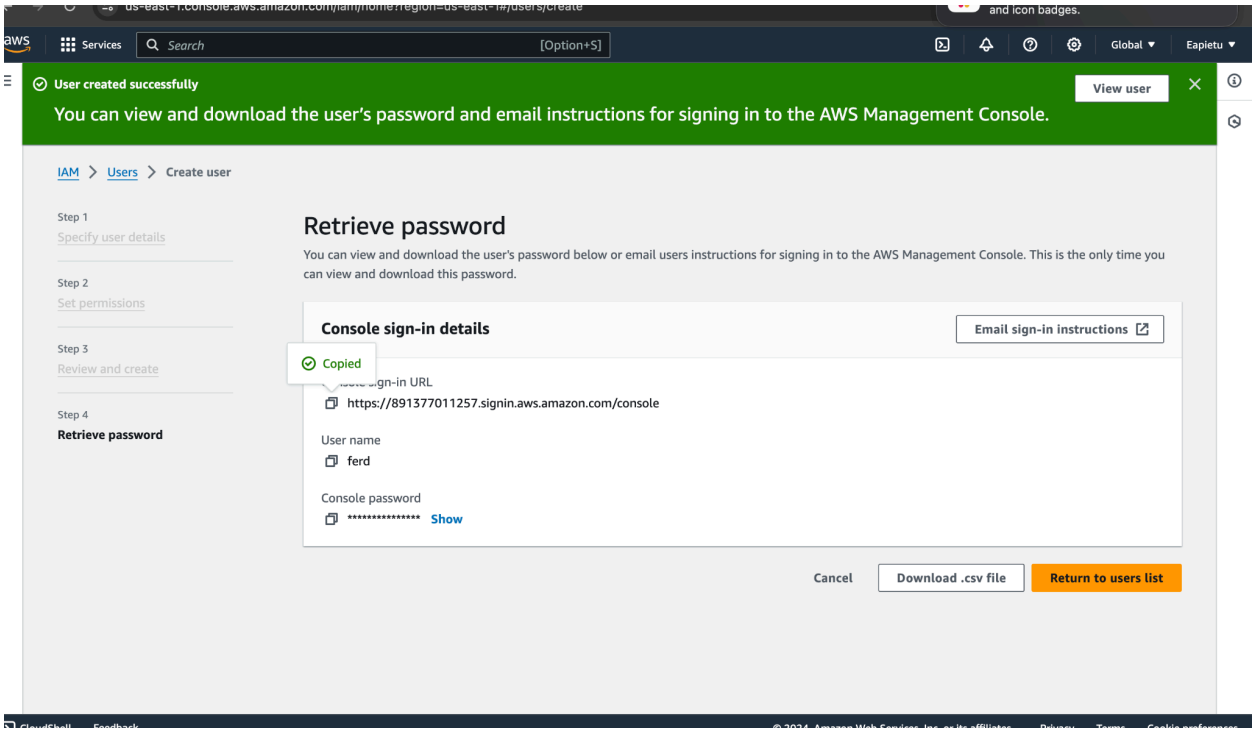
Configure security groups for each subnet to control incoming and outgoing traffic.

For example:

- Allow incoming traffic from trusted IP addresses or AWS services to the log collection subnet
- Allow outgoing traffic from the log analysis subnet to the data storage subnet
- Deny all incoming traffic from the internet to the data storage subnet

Attached below is a photo from our AWS account for users with permissions.


Services
Search
[Option+S]
Global
Eapietu
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
ferd
Console password type
Autogenerated
Require password reset
No
Permissions summary
Name
Type
Used as
AmazonEC2FullAccess
AWS managed
Permissions policy
AmazonGuardDutyFullAccess
AWS managed
Permissions policy
AmazonRDSFullAccess
AWS managed
Permissions policy
AmazonRoute53FullAccess
AWS managed
Permissions policy
AmazonS3FullAccess
AWS managed
Permissions policy
AmazonSNSFullAccess
AWS managed
Permissions policy
AWSWAFFullAccess
AWS managed
Permissions policy
CloudWatchFullAccess
AWS managed
Permissions policy
Tags - optional


Services
Search
[Option+S]
Global
Eapietu
User created successfully
View user
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
IAM
Users
Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Retrieve password
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.
Console sign-in details
Email sign-in instructions
Copied
https://891377011257.signin.aws.amazon.com/console
User name
ferd
Console password
Show
Cancel
Download .csv file
Return to users list

Data Encryption:

Encrypt all data in transit and at rest using AWS Key Management Service (KMS) keys. This includes encrypting log data, configuration data, and any other sensitive data such as multi-factor authentication.

Monitoring and Logging:

Monitor and log all network traffic, including security group and network ACL changes, using AWS CloudWatch logs and CloudTrail. Amazon S3 is a popular choice for storing logs because it provides a scalable, durable, and secure storage solution. Amazon CloudWatch Logs is a fully managed log service that collects, monitors, and stores logs from AWS services, including EC2 instances, AWS Lambda functions, and more.

With this architecture, you can ensure a secure and compliant virtual network architecture for your SIEM components in AWS.