Name:AbdelRahman Moustafa Mohamed Abdallah

Groub name: AWS Cloud Specialist (ALX1_SWD8_M1e)

Student ID: 1110242719

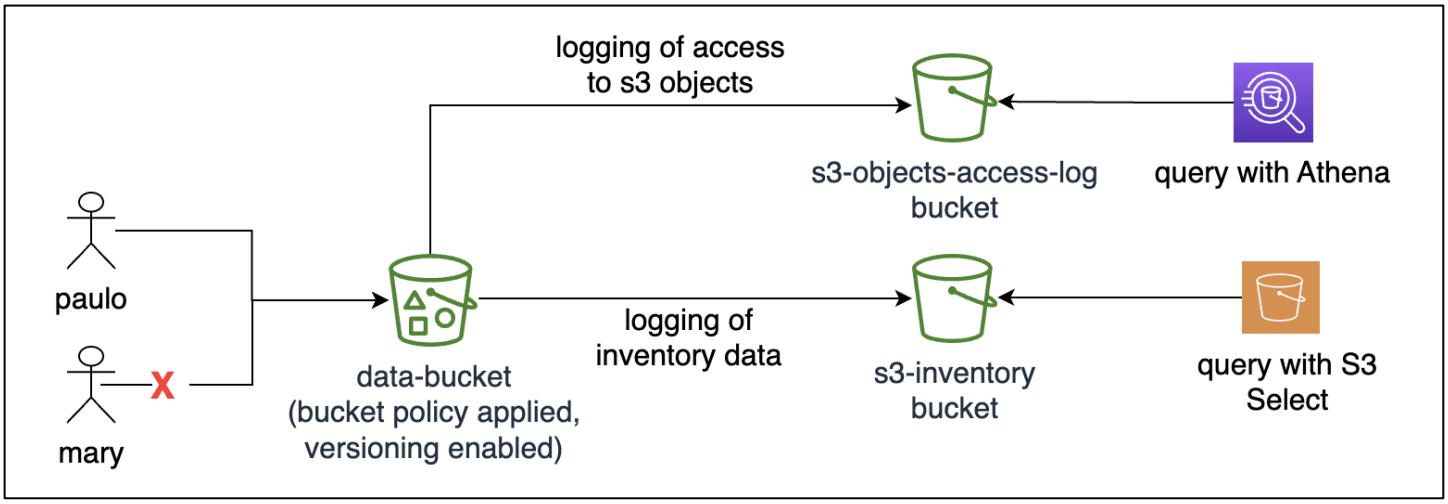
AWS Academy Cloud Security Foundations

Securing and Monitoring Resources with AWS

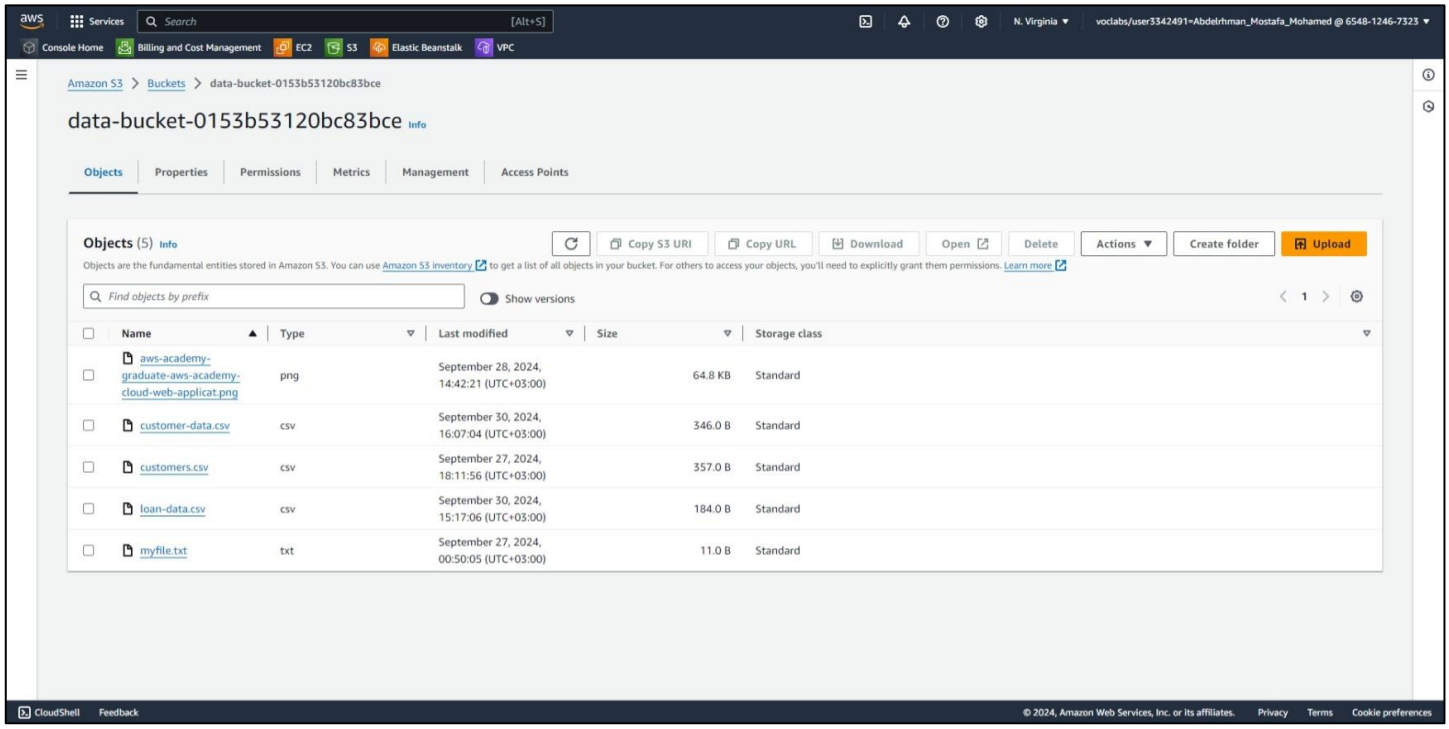
Supervise by: Eng. Merhan Adel

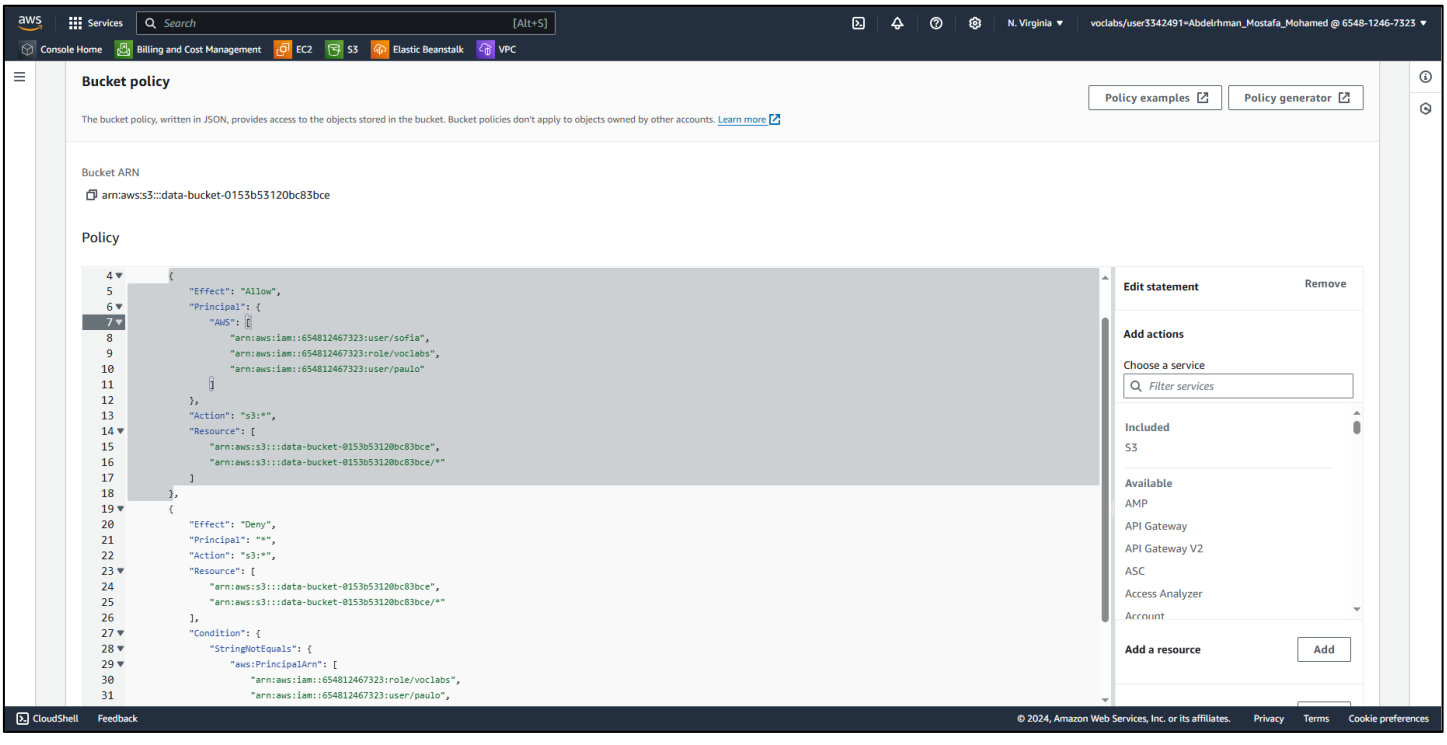
Badge Link

Phase 1: Securing data in Amazon S3

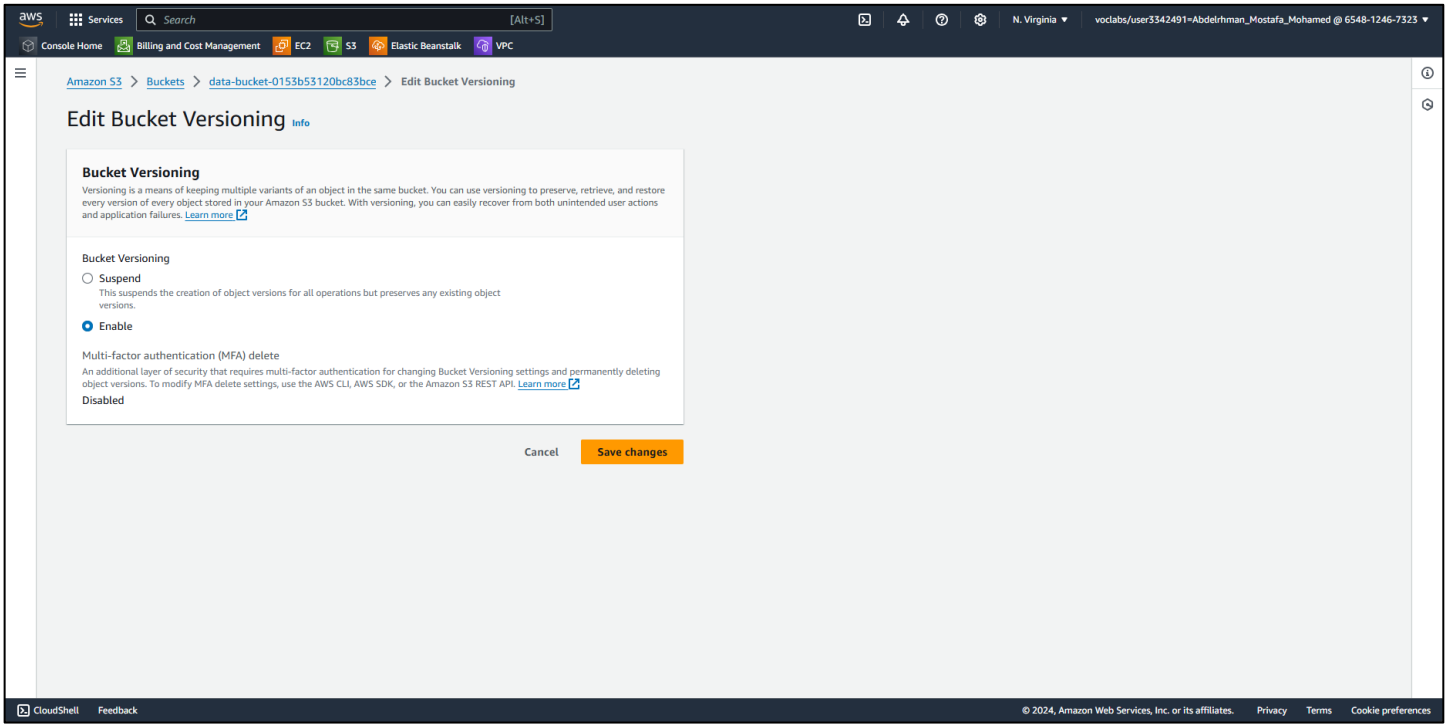


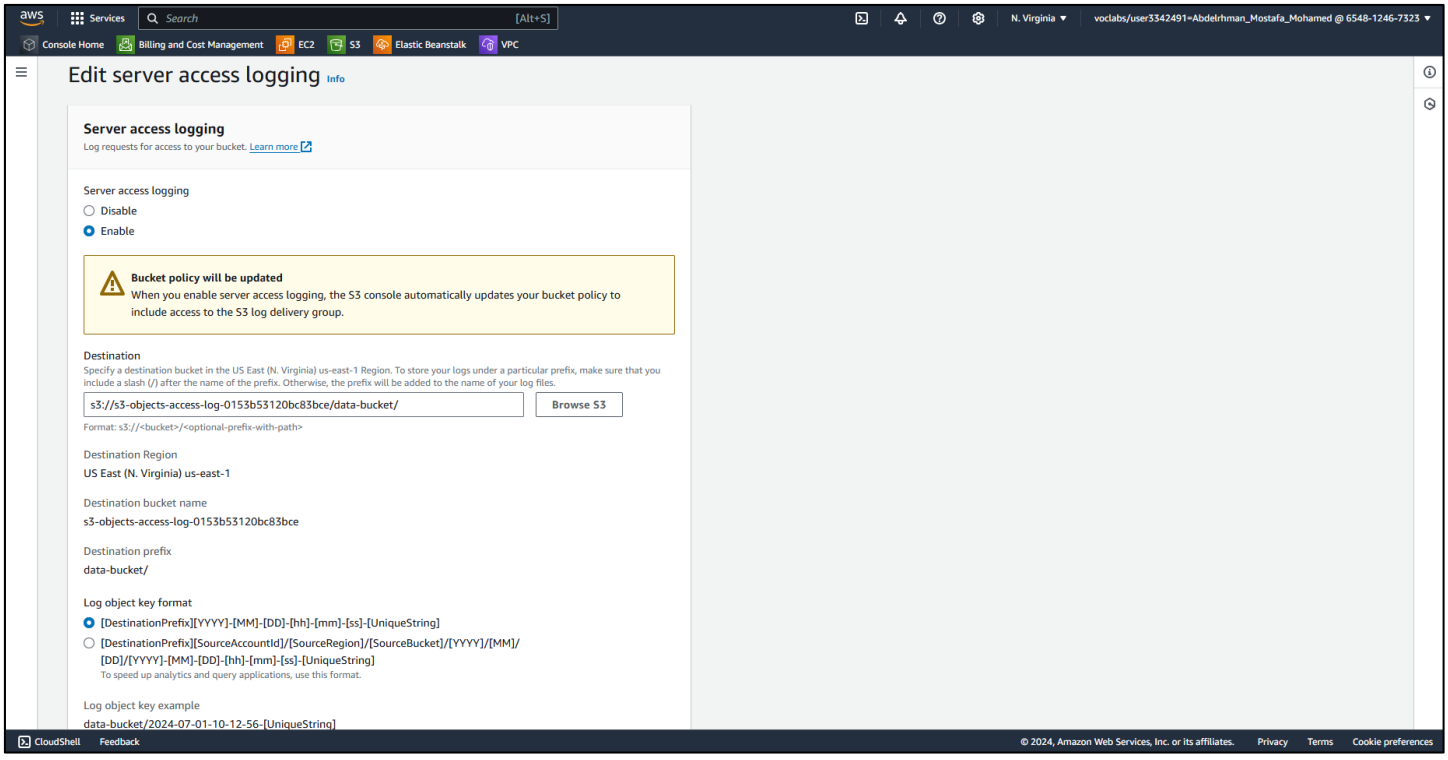
Task 1.1: Create a bucket, apply a bucket policy, and test access



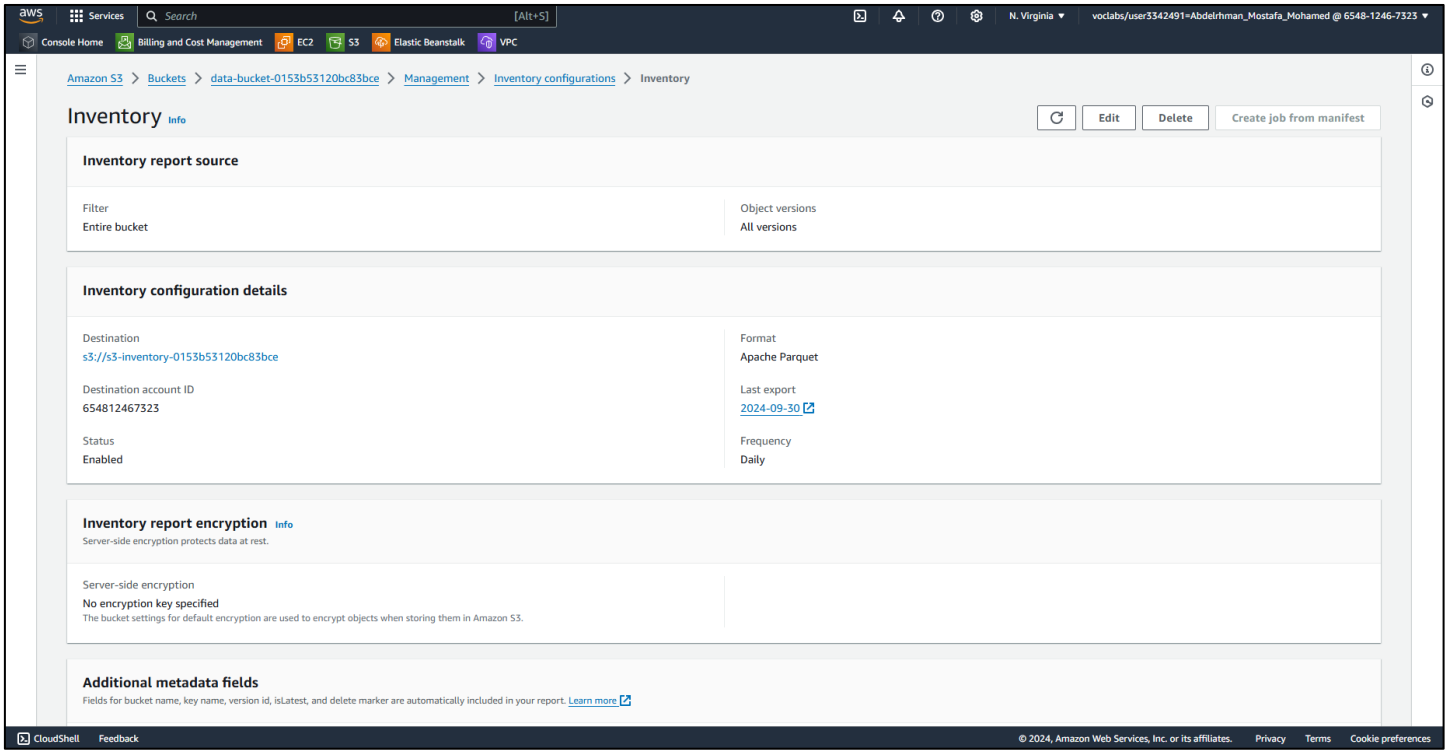


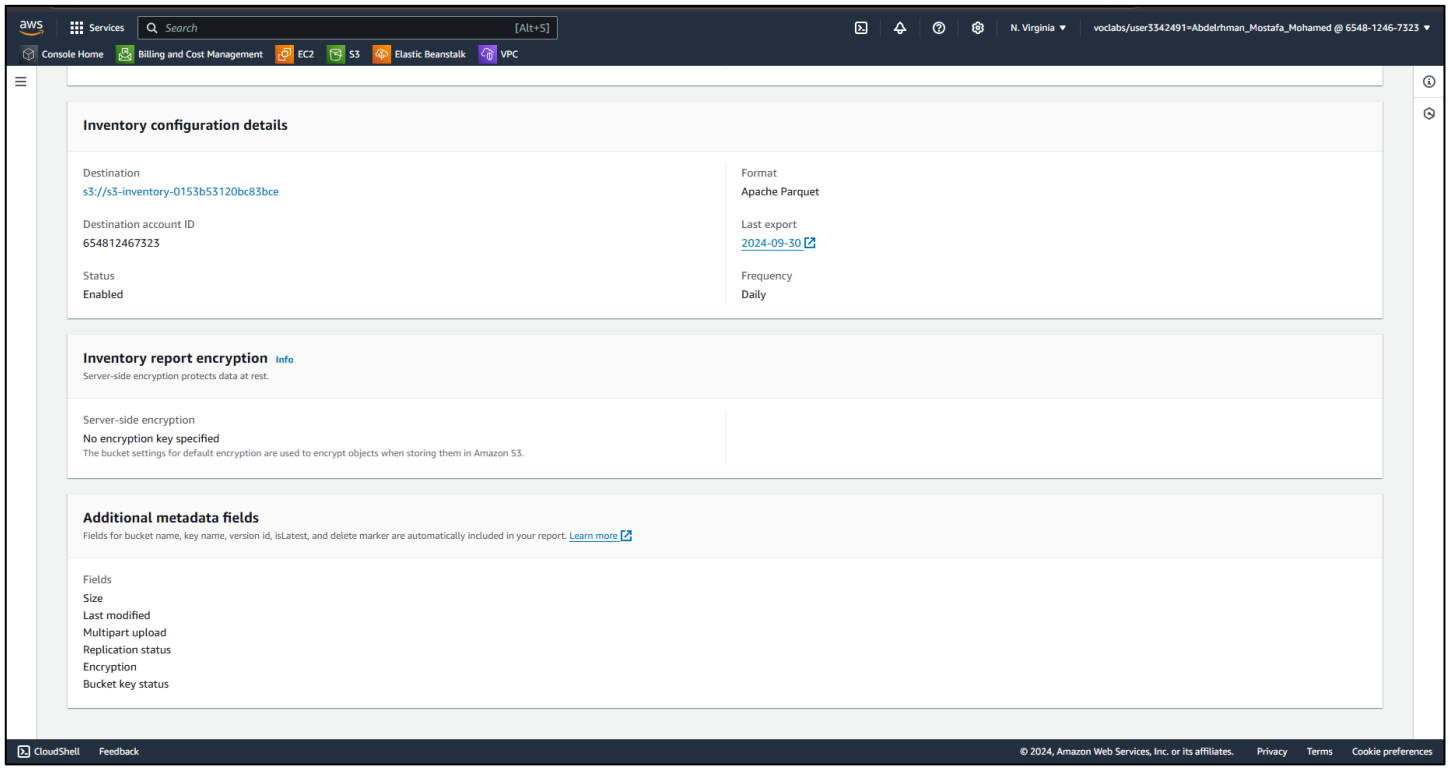
Task 1.2: Enable versioning and object-level logging on a bucket



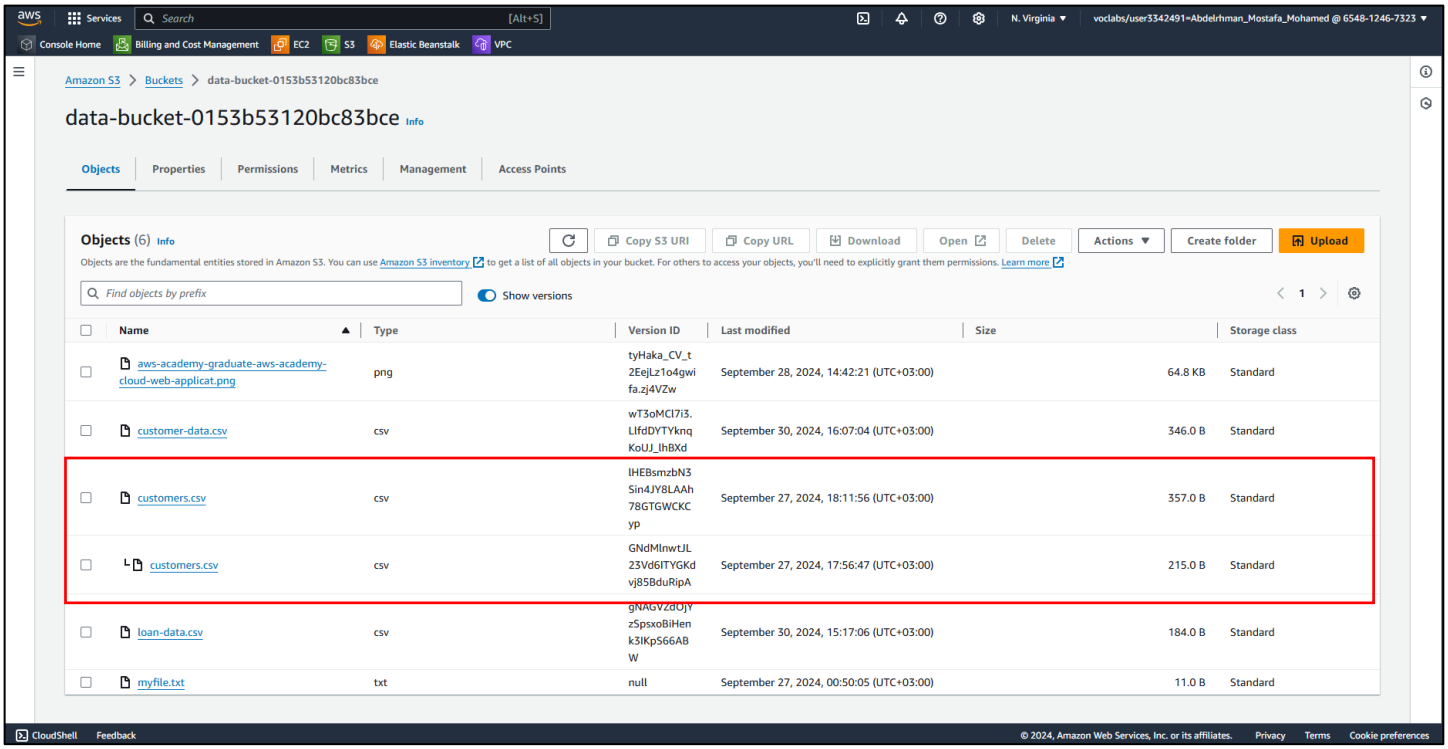


Task 1.3: Implement the S3 Inventory feature on a bucket

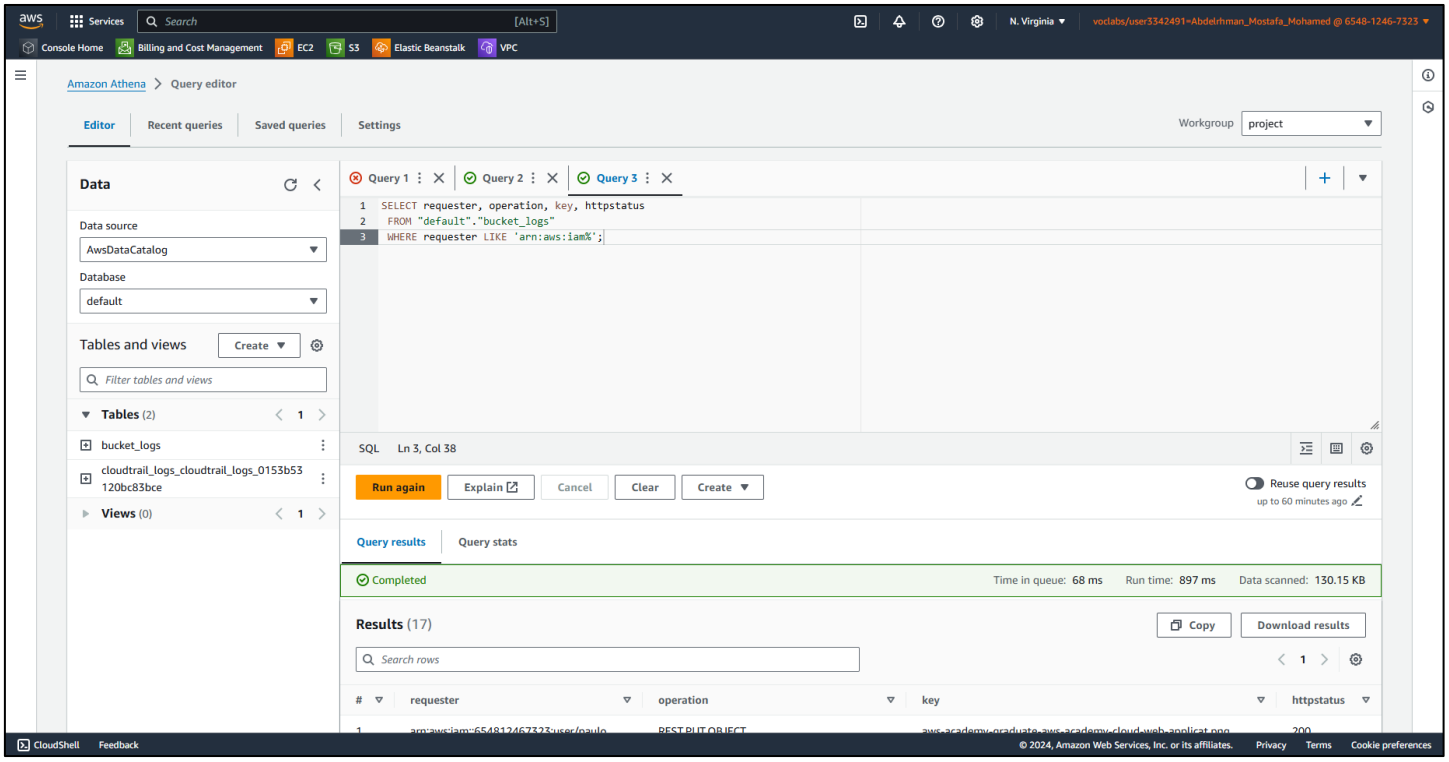


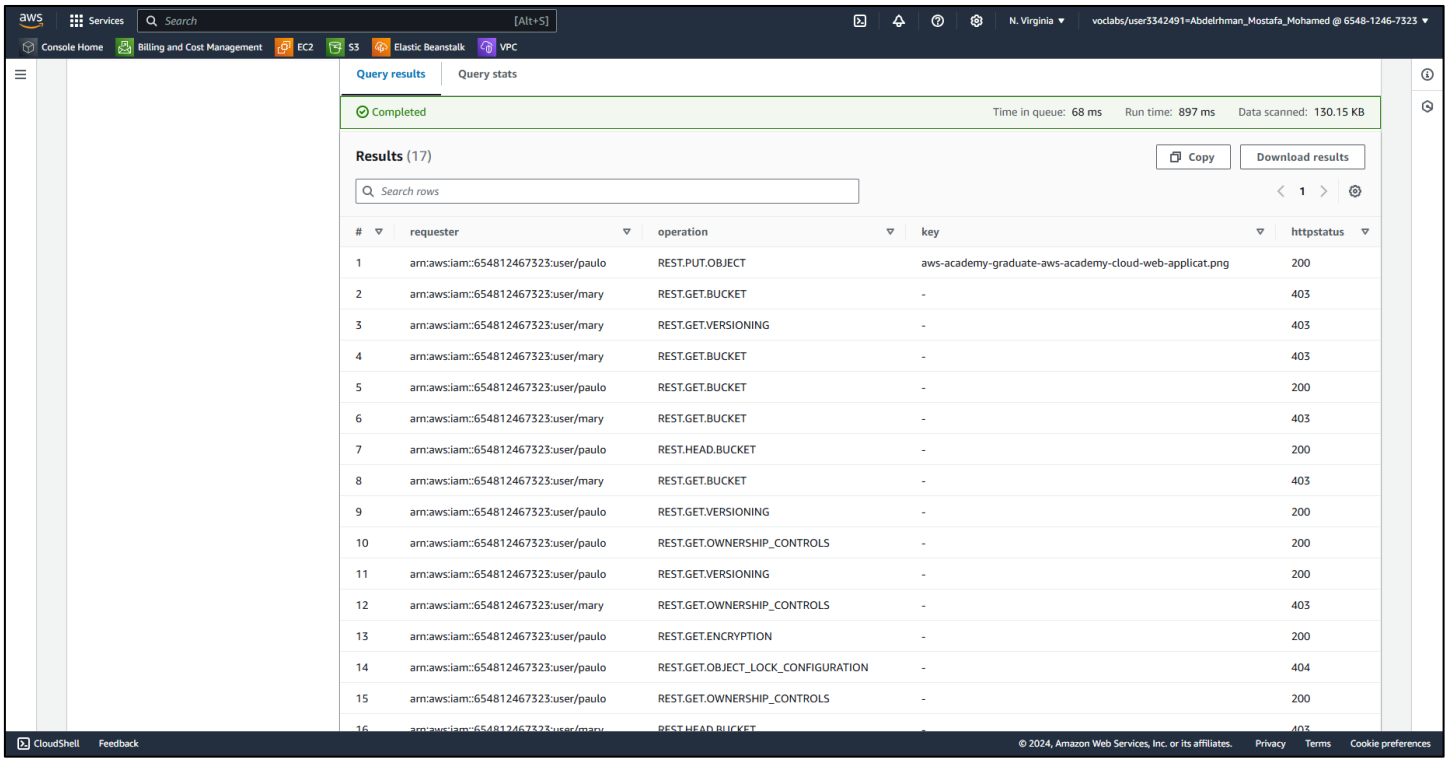


Task 1.4: Confirm that versioning works as intended



Task 1.5: Confirm object-level logging and query the access logs by using Athena



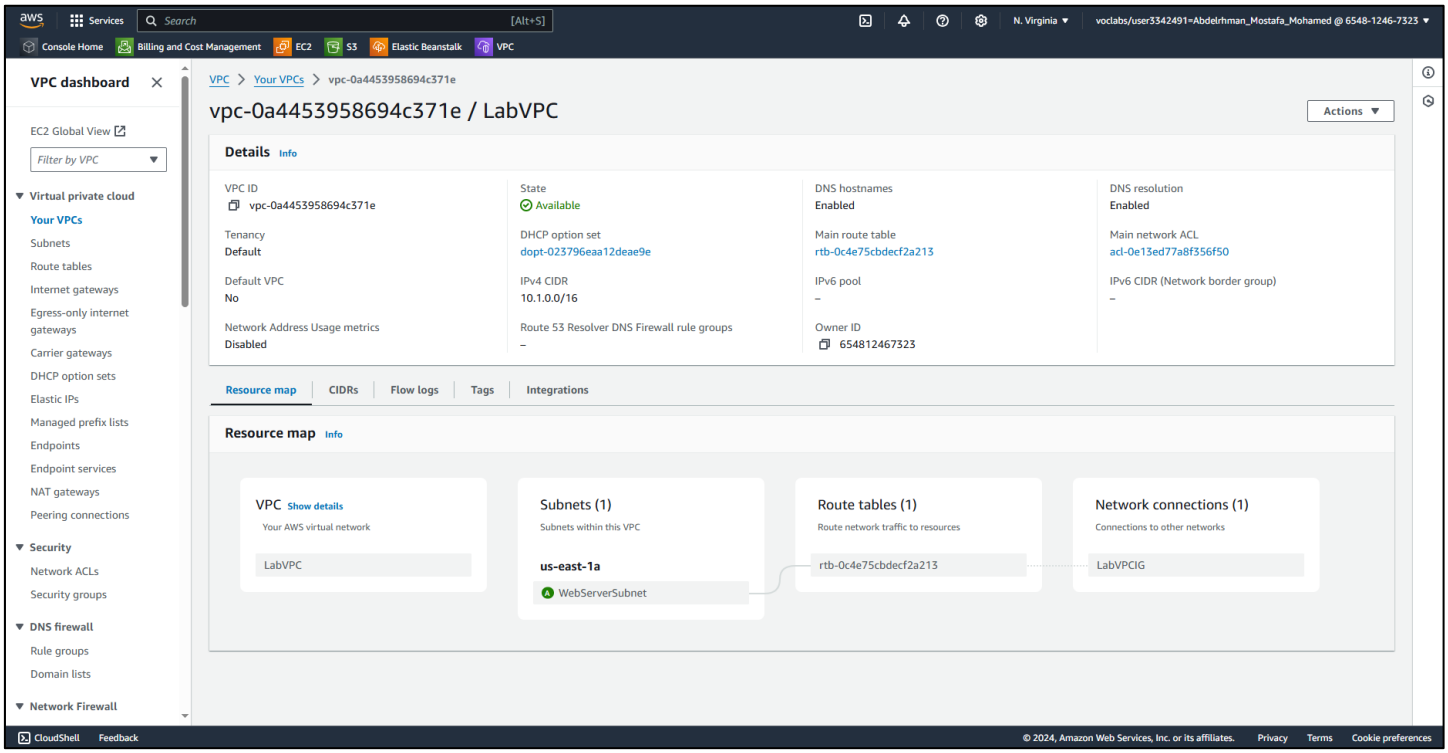


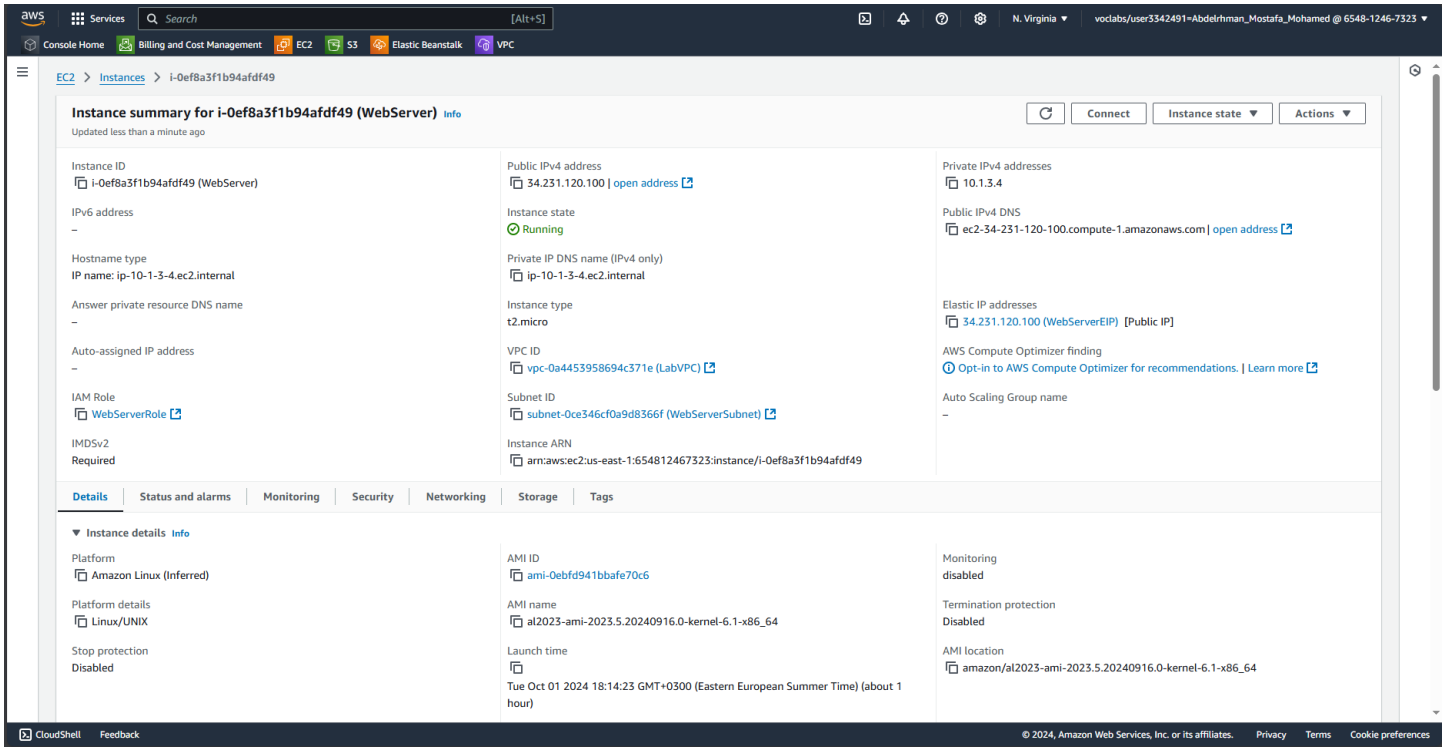
Cost assessment to secure Amazon S3

Estimate Cost CSV File

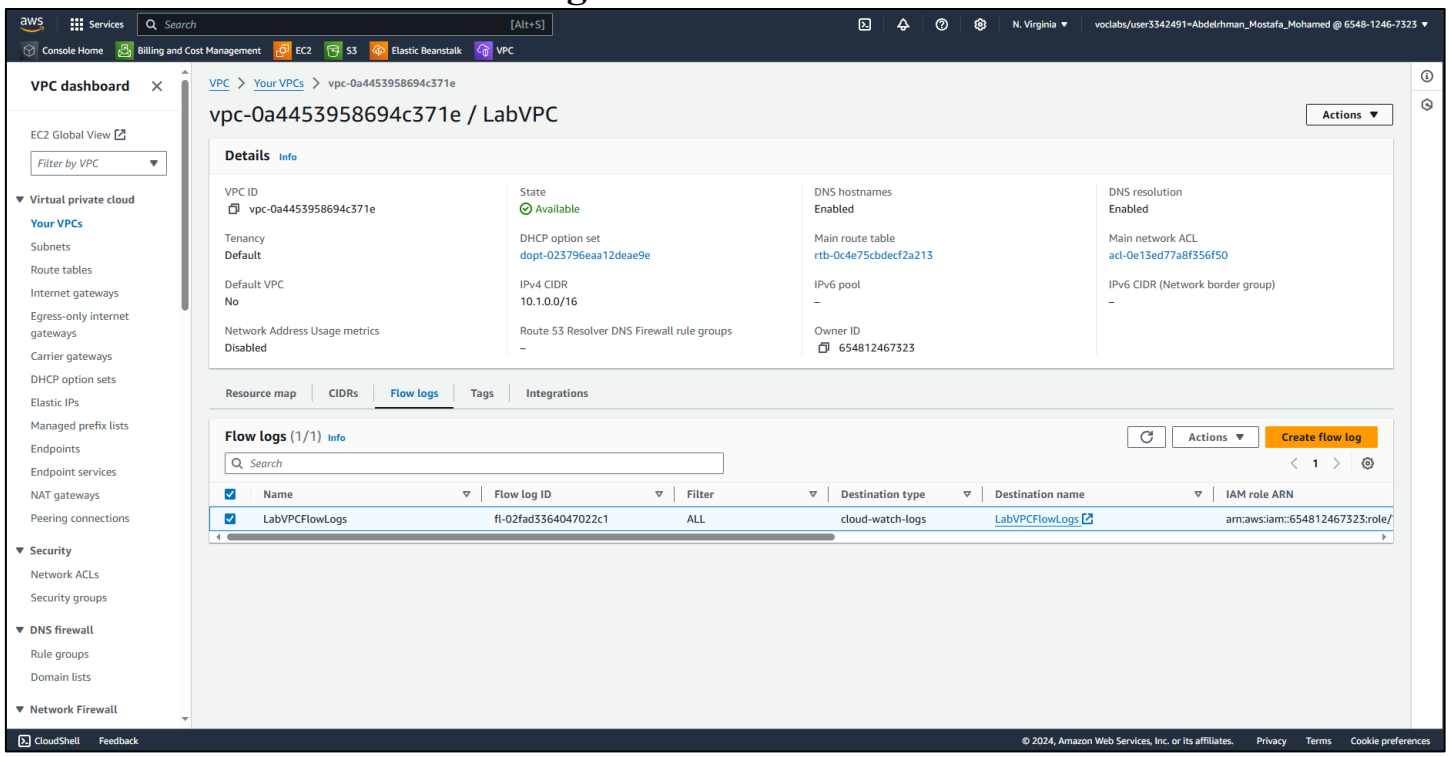
Phase 2: Securing VPCs

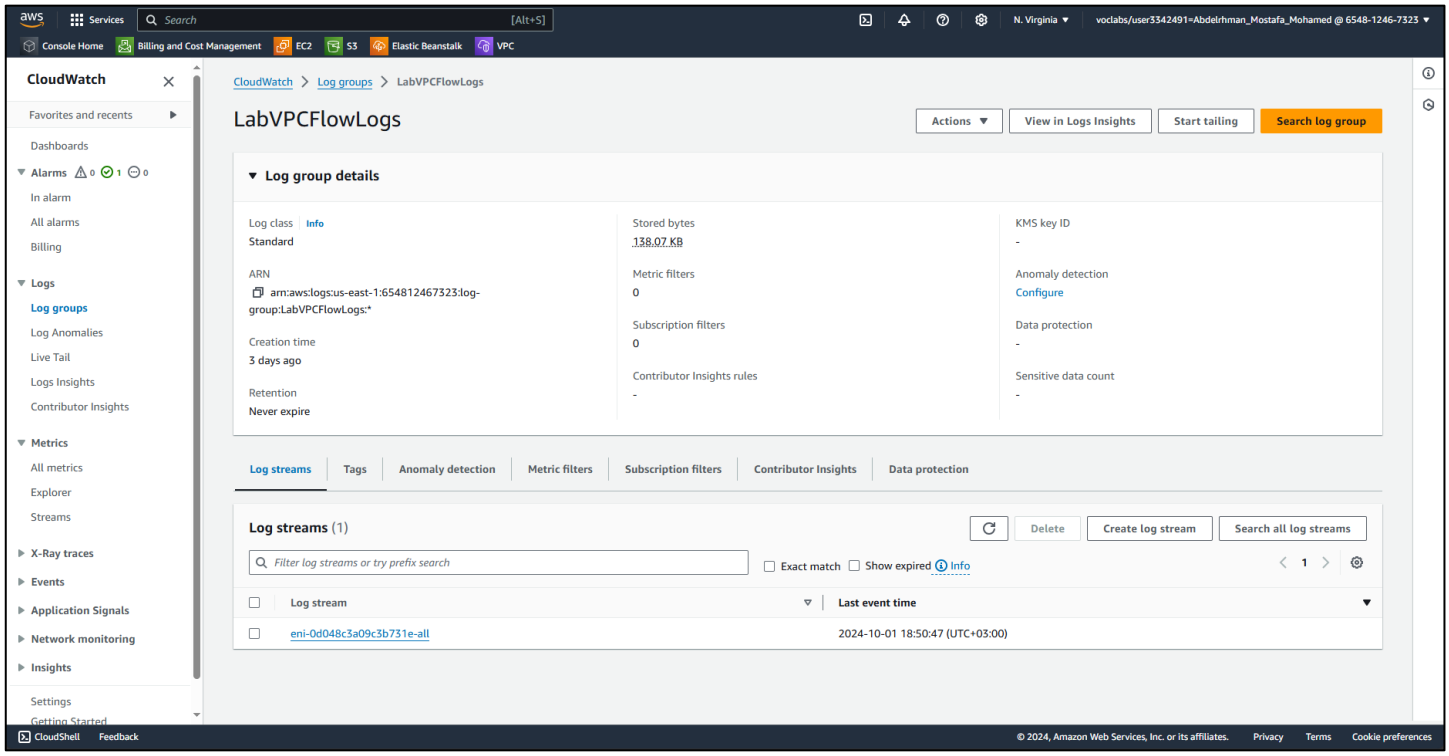
Task 2.1: Review LabVPC and its associated resources



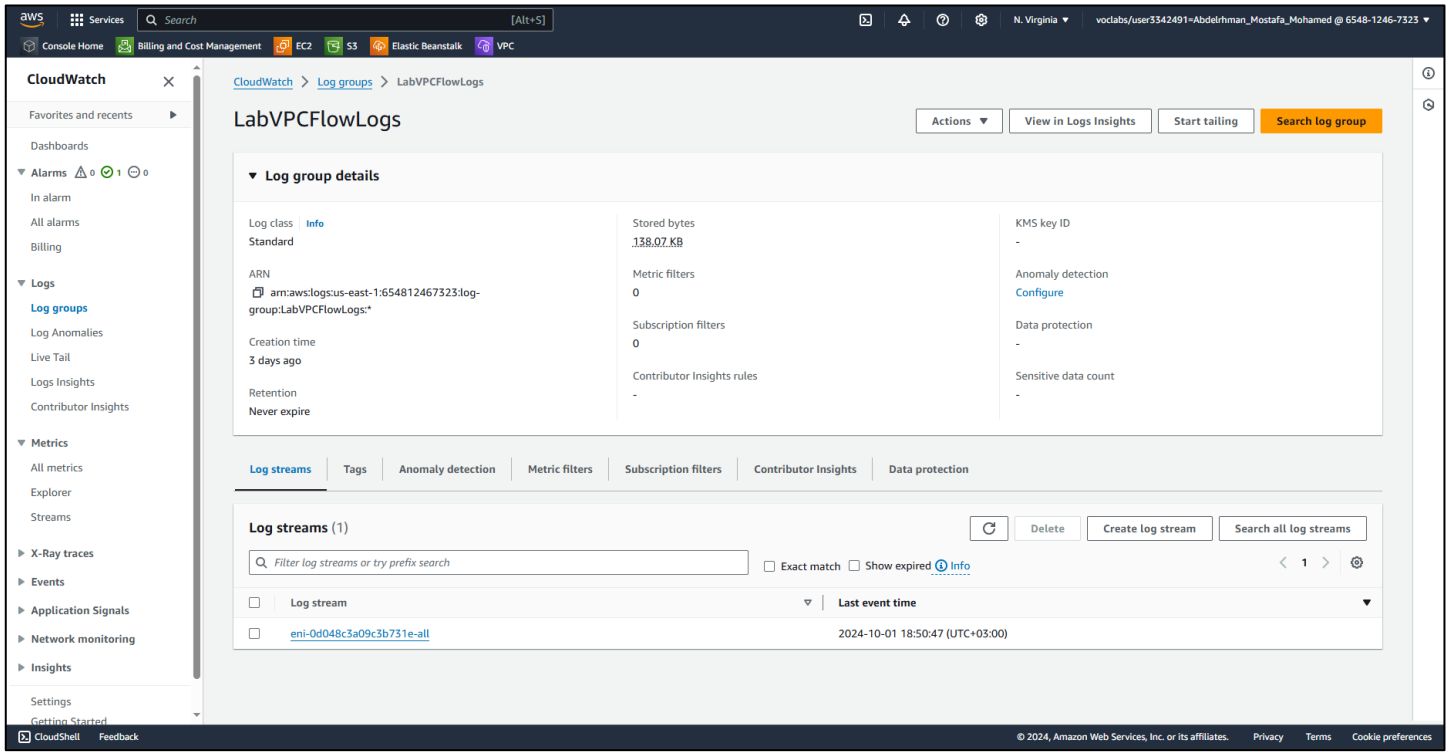


Task 2.2: Create a VPC flow log

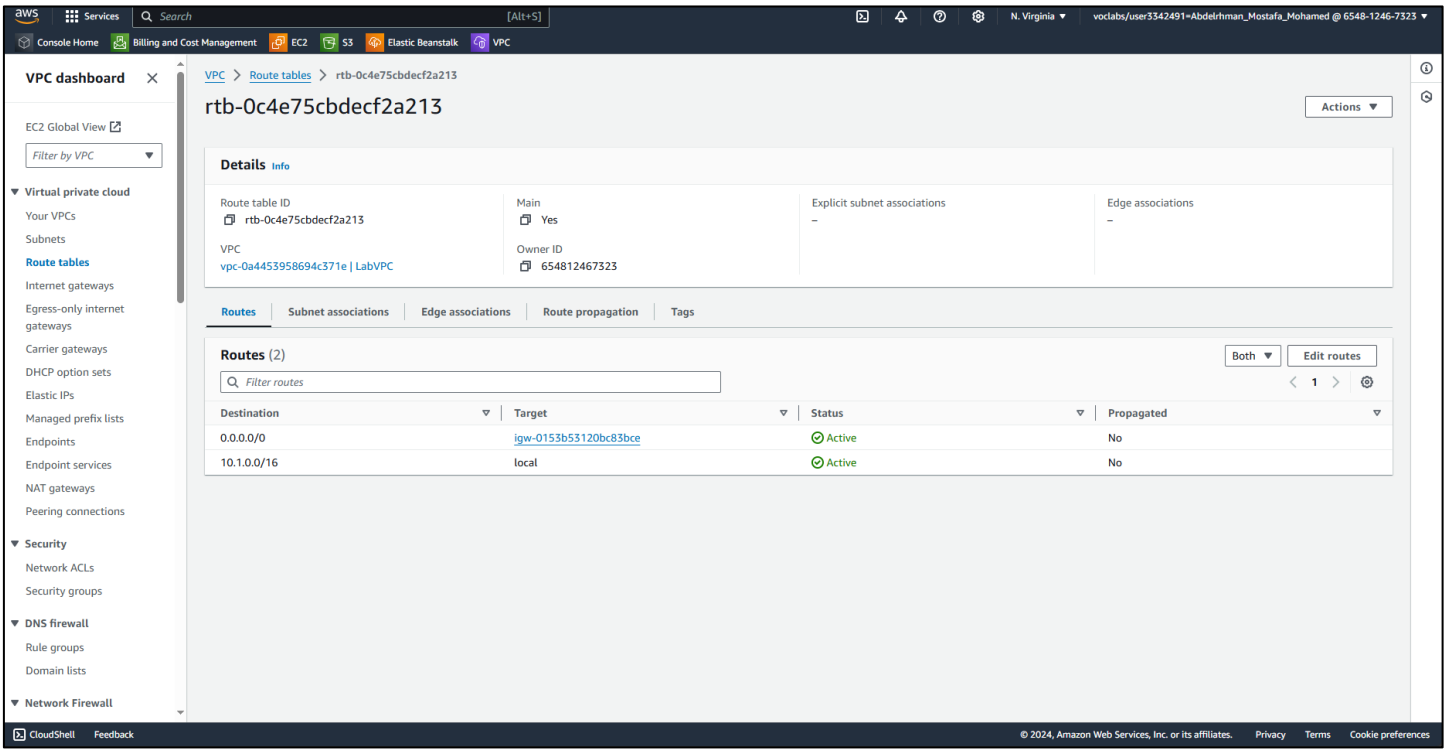


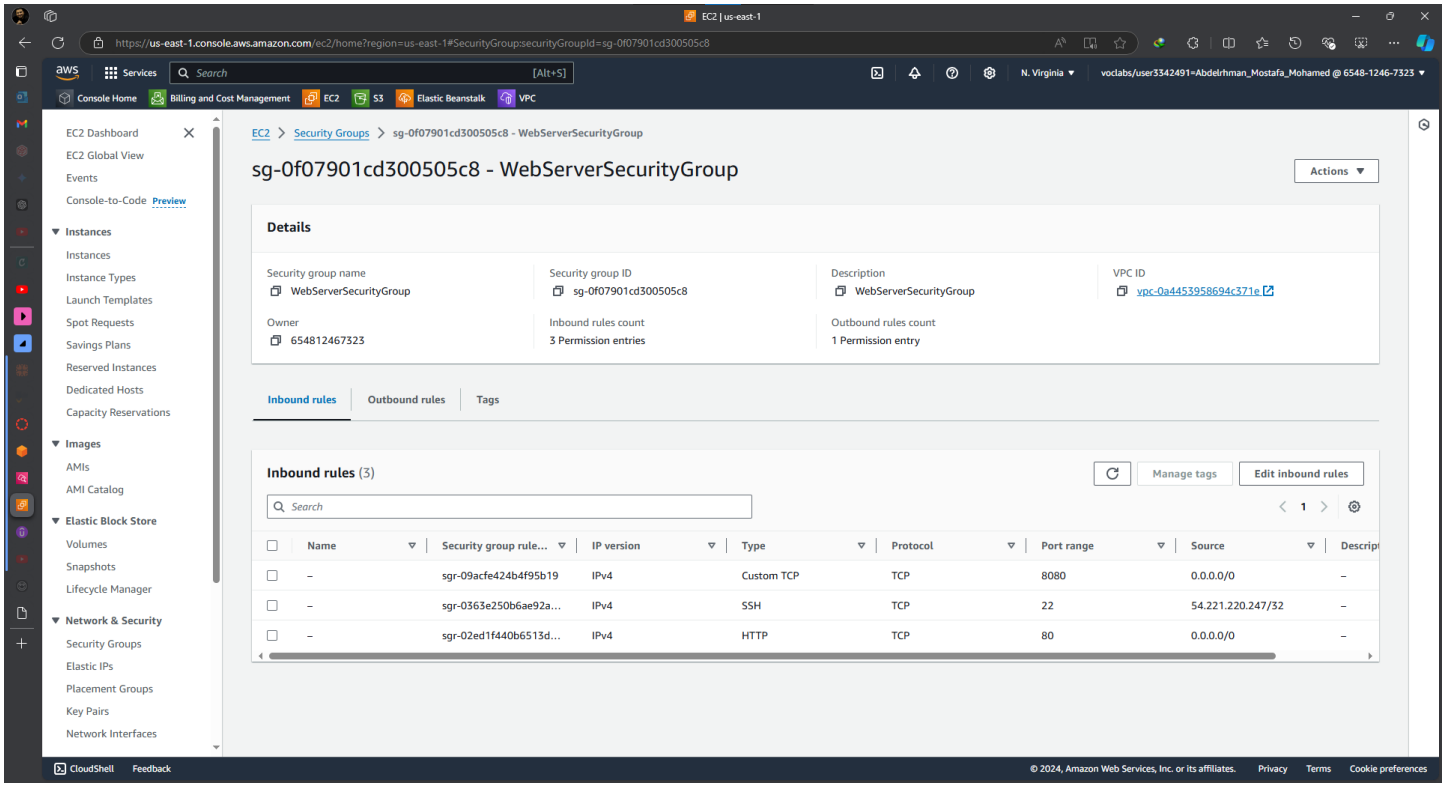


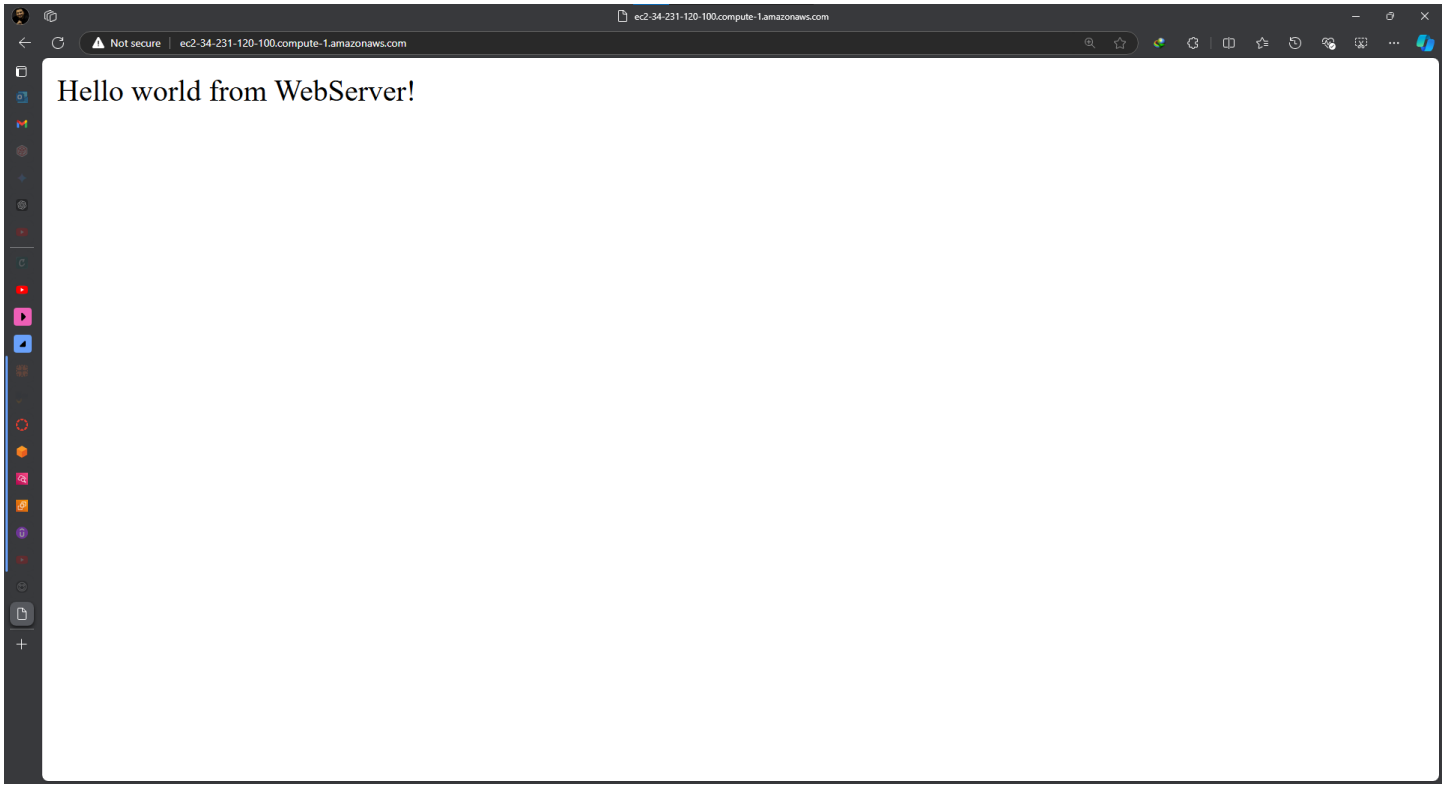
Task 2.3: Access the WebServer instance from the internet and review VPC flow logs in CloudWatch



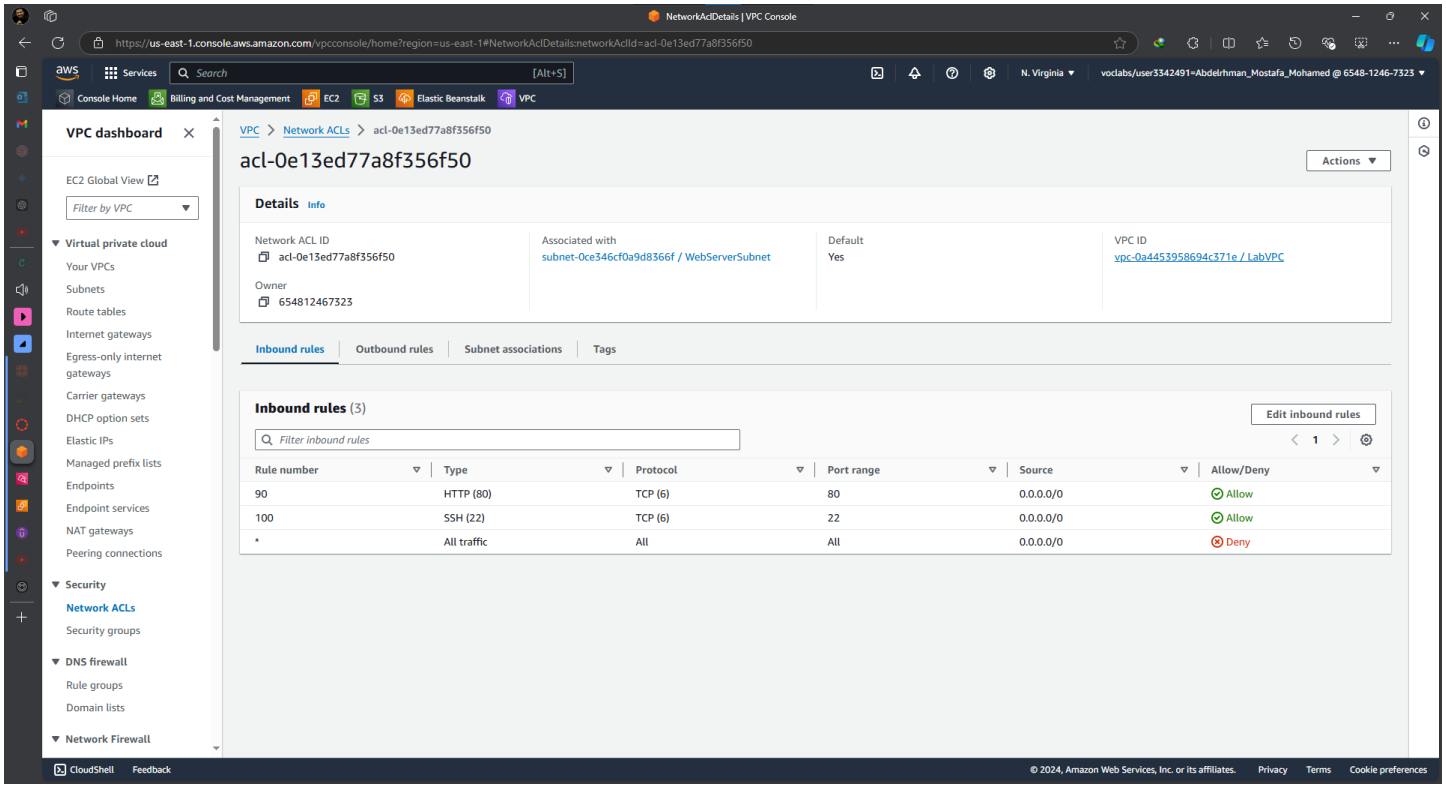
Task 2.4: Configure route table and security group settings

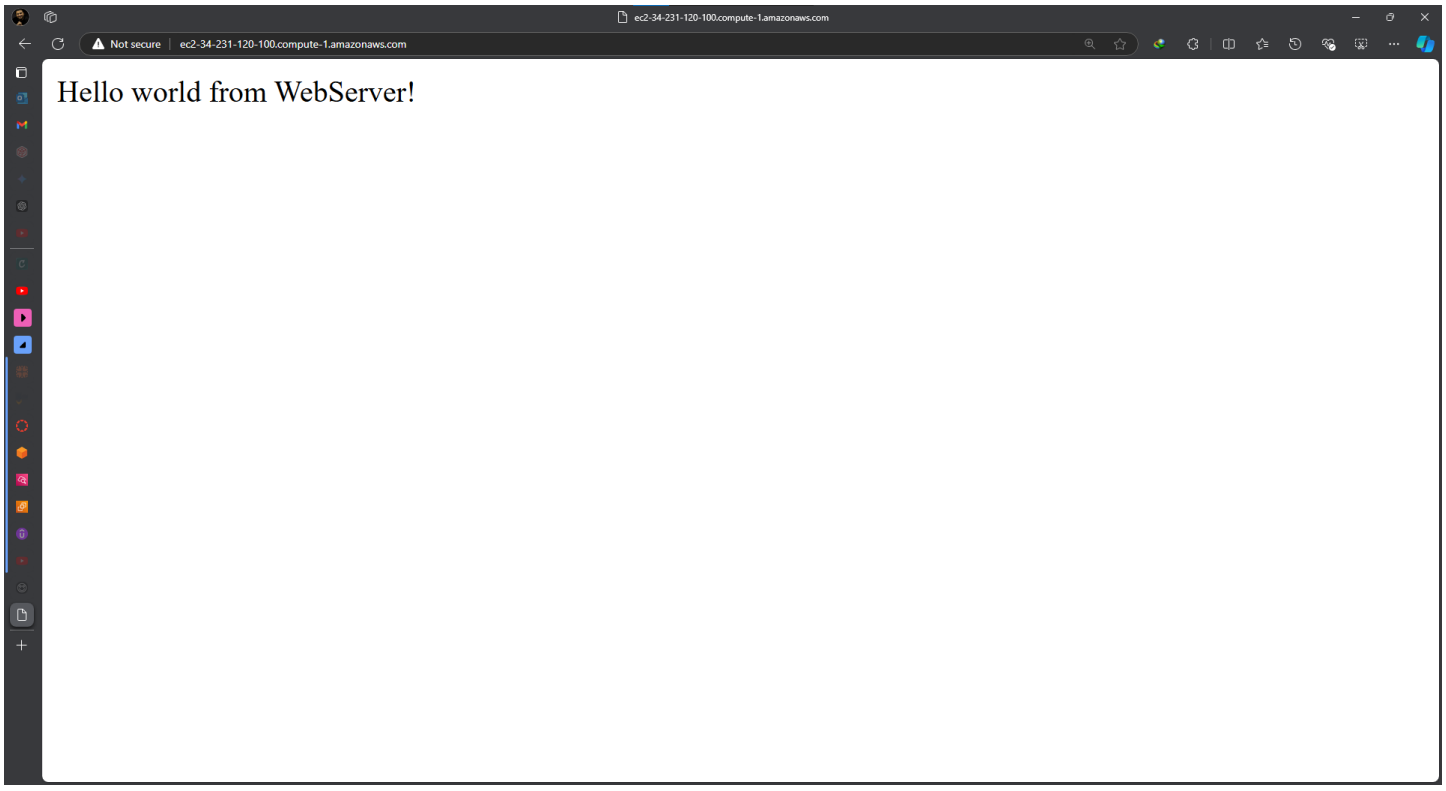




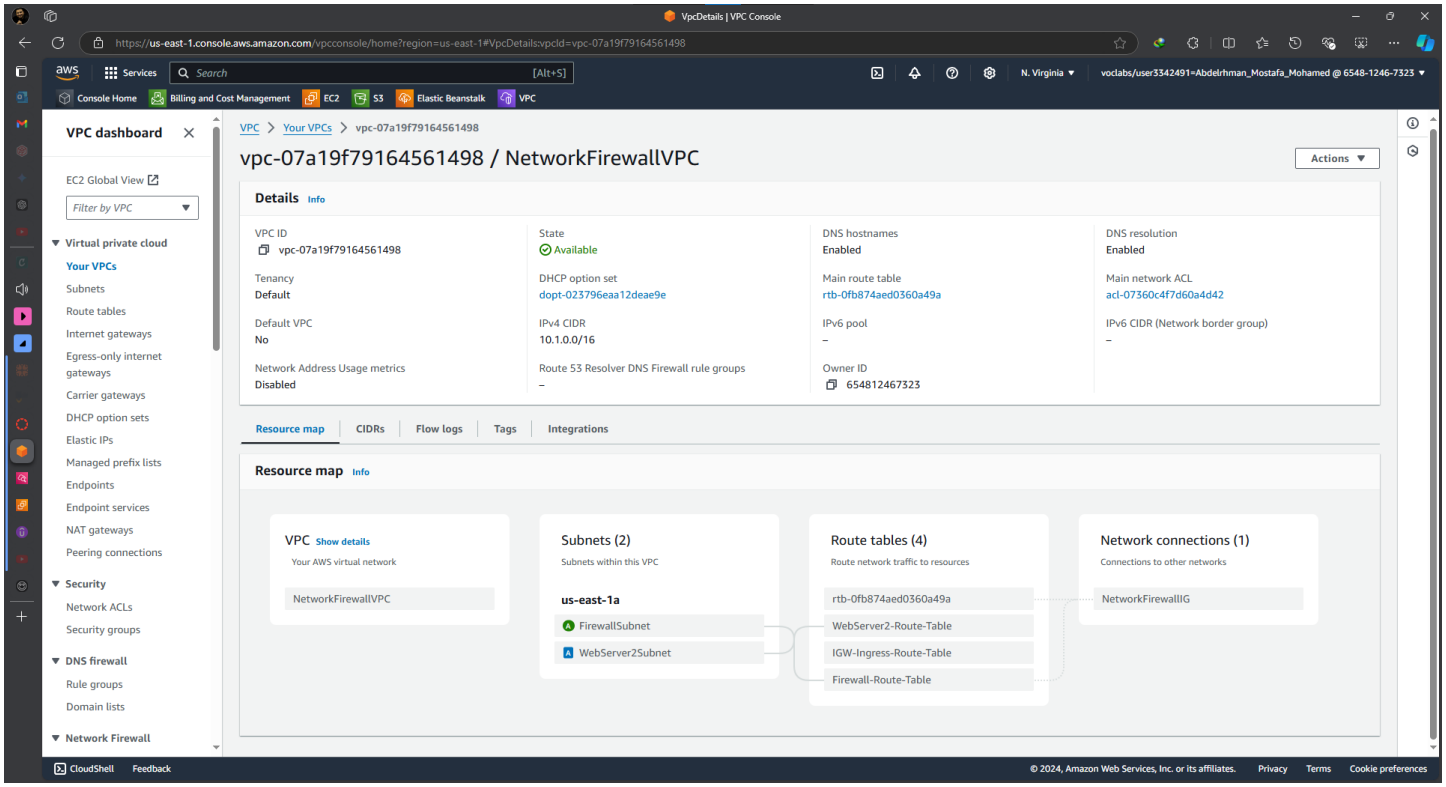

ec2-34-231-120-100.compute-1.amazonaws.com
Not secure
ec2-34-231-120-100.compute-1.amazonaws.com
Hello world from WebServer!

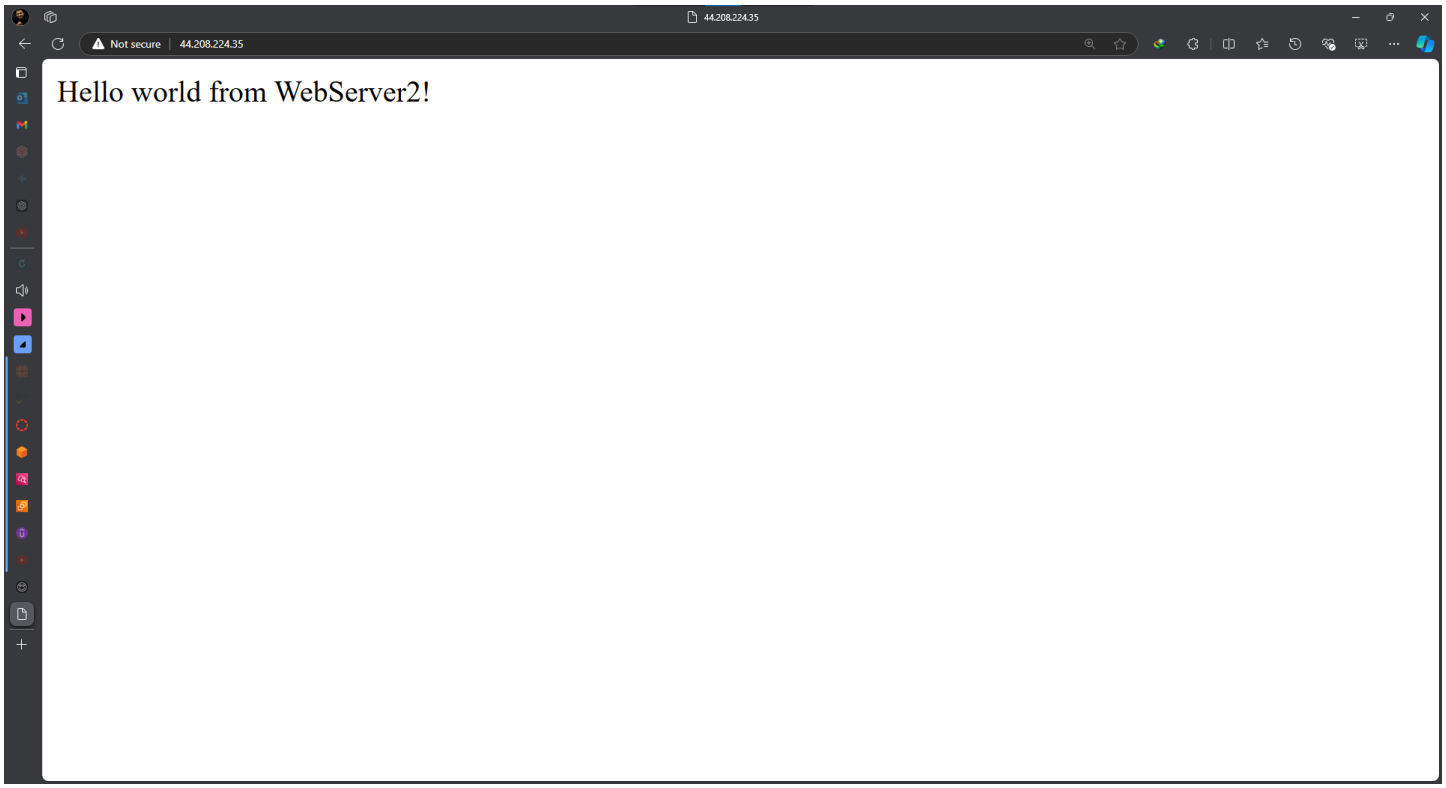
Task 2.5: Secure the WebServerSubnet with a network ACL

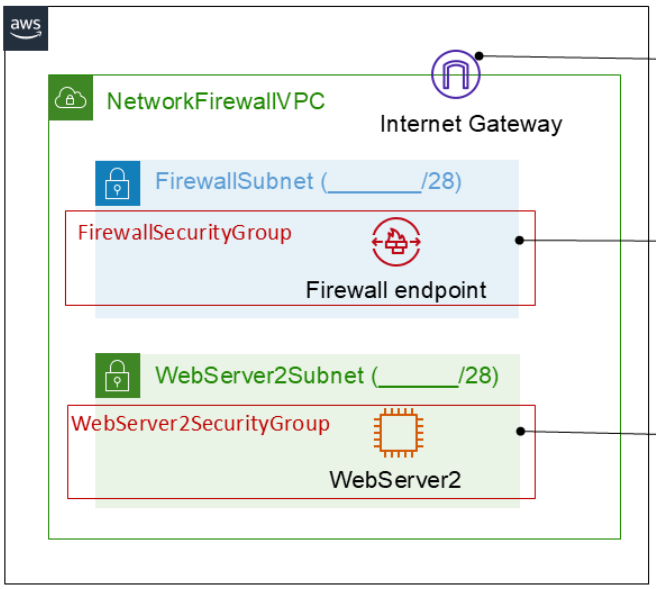




Task 2.6: Review NetworkFirewallVPC and its associated resources







IGW-Ingress-Route-Table

Destination	Target
10.1.0.0/16	local
10.1.3.0/28	vpce-0ee5aaf4208bc1d15

Firewall-Route-Table

Destination	Target
0.0.0.0/0	igw-05afa5bee40c5a0cb
10.1.0.0/16	local

WebServer2-Route-Table

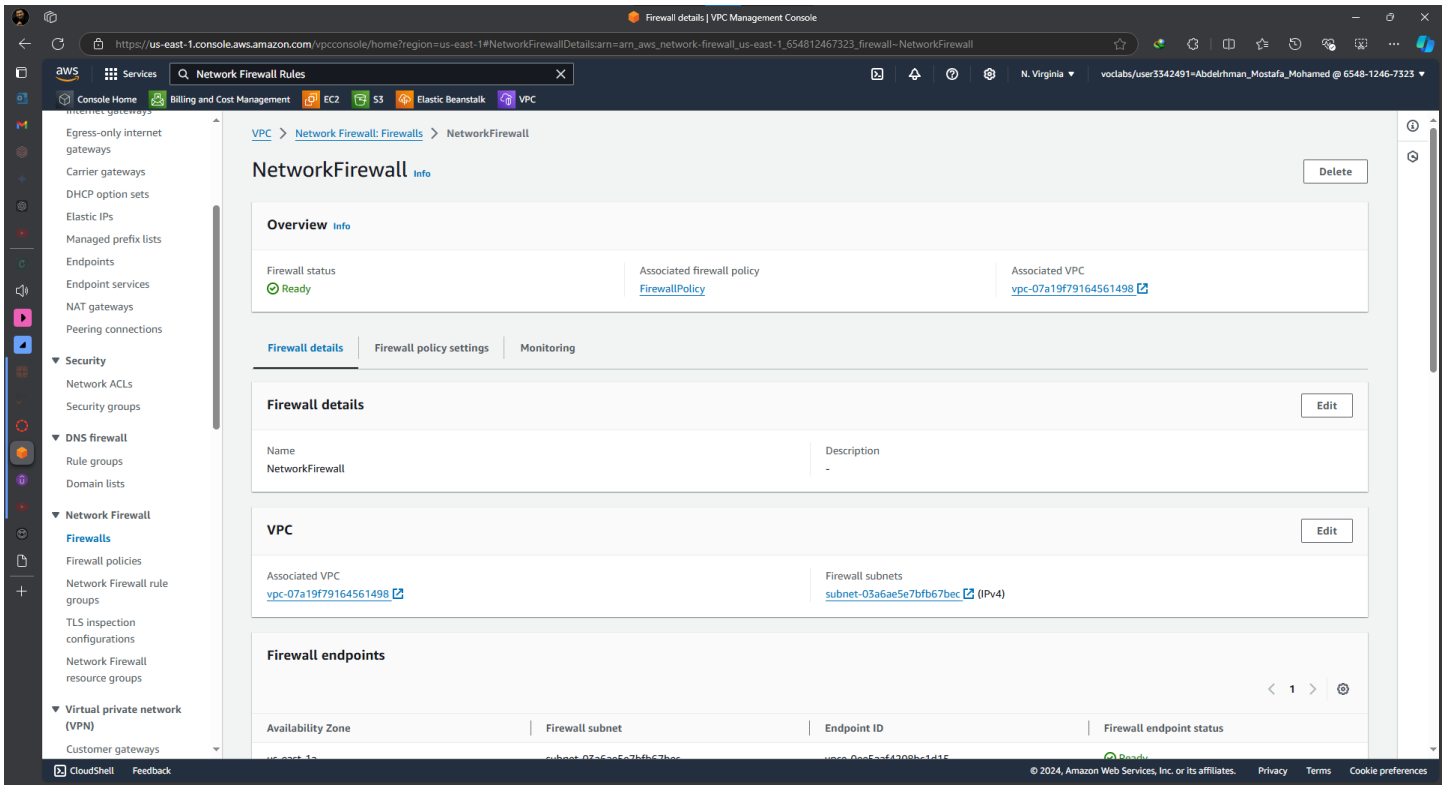
Destination	Target
0.0.0.0/0	vpce-0ee5aaf4208bc1d15
10.1.0.0/16	local

Network Firewall Rules

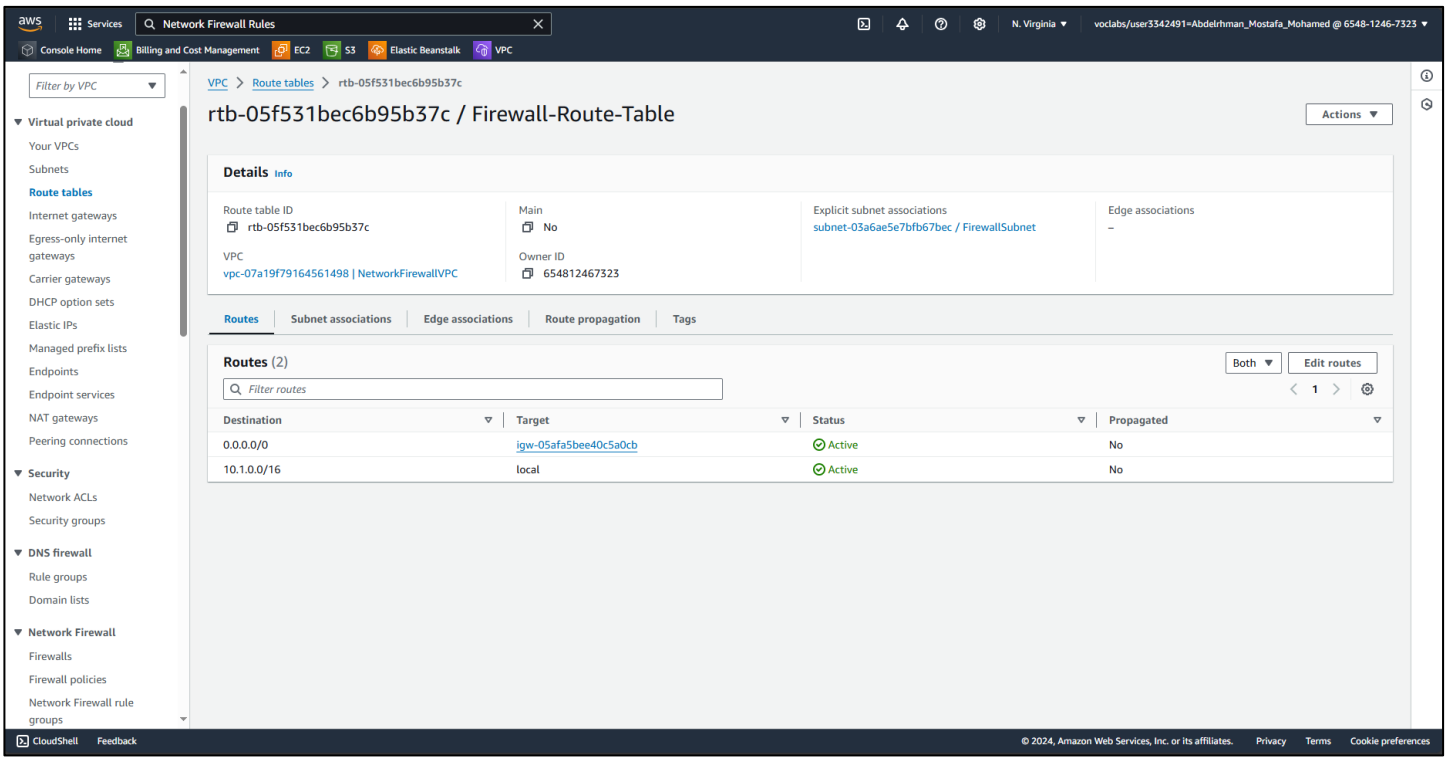
Protocol	Port	Action
TCP	80	Pass
TCP	22	Pass
TCP	443	Pass
ICMP	ANY	Pass

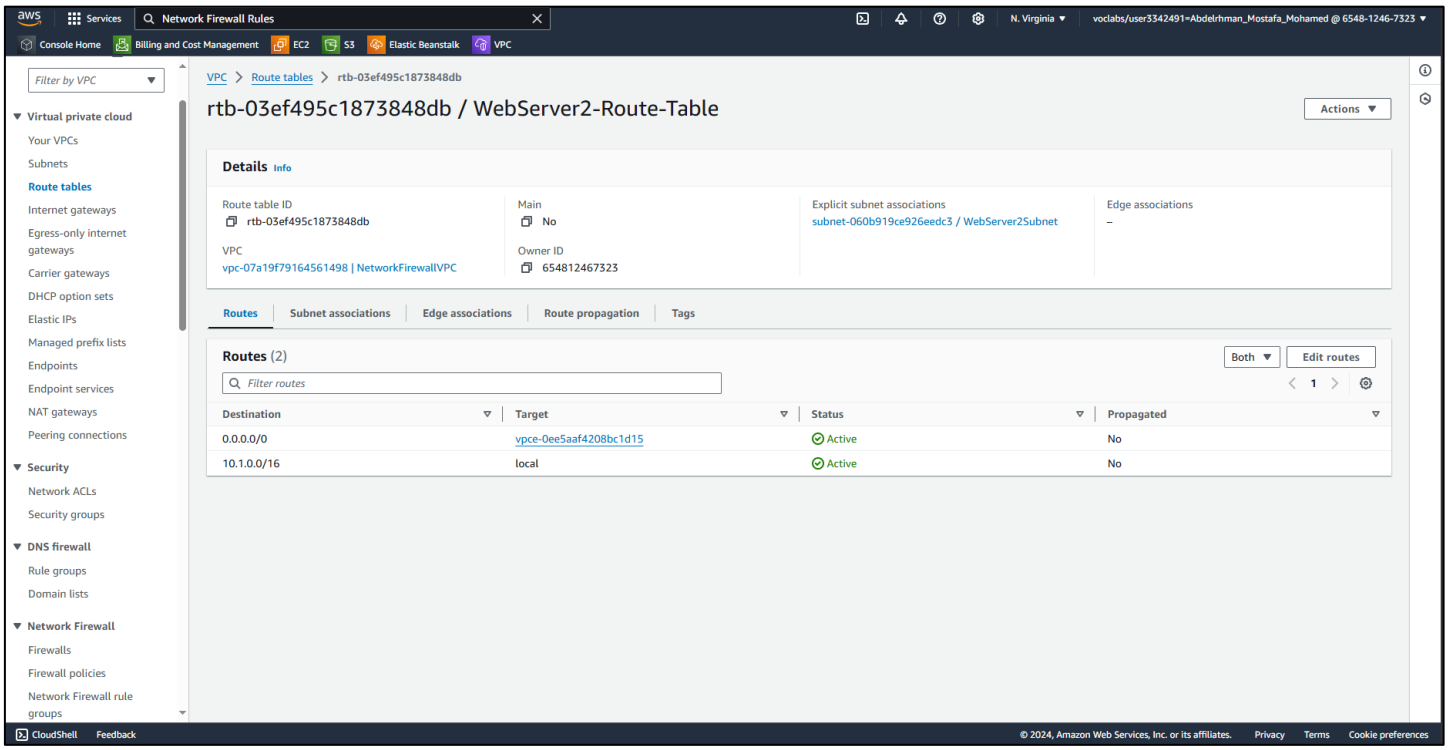
aws

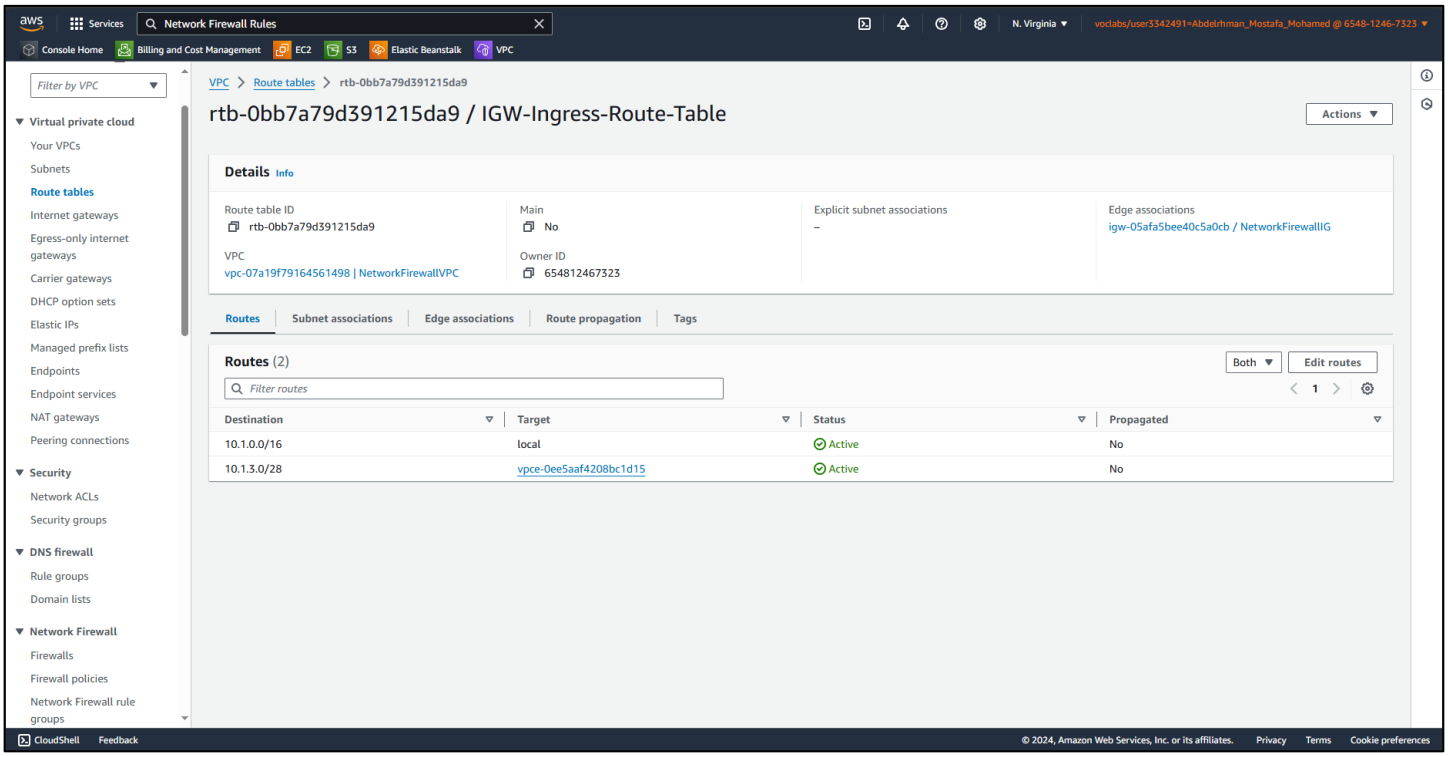
Task 2.7: Create a network firewall



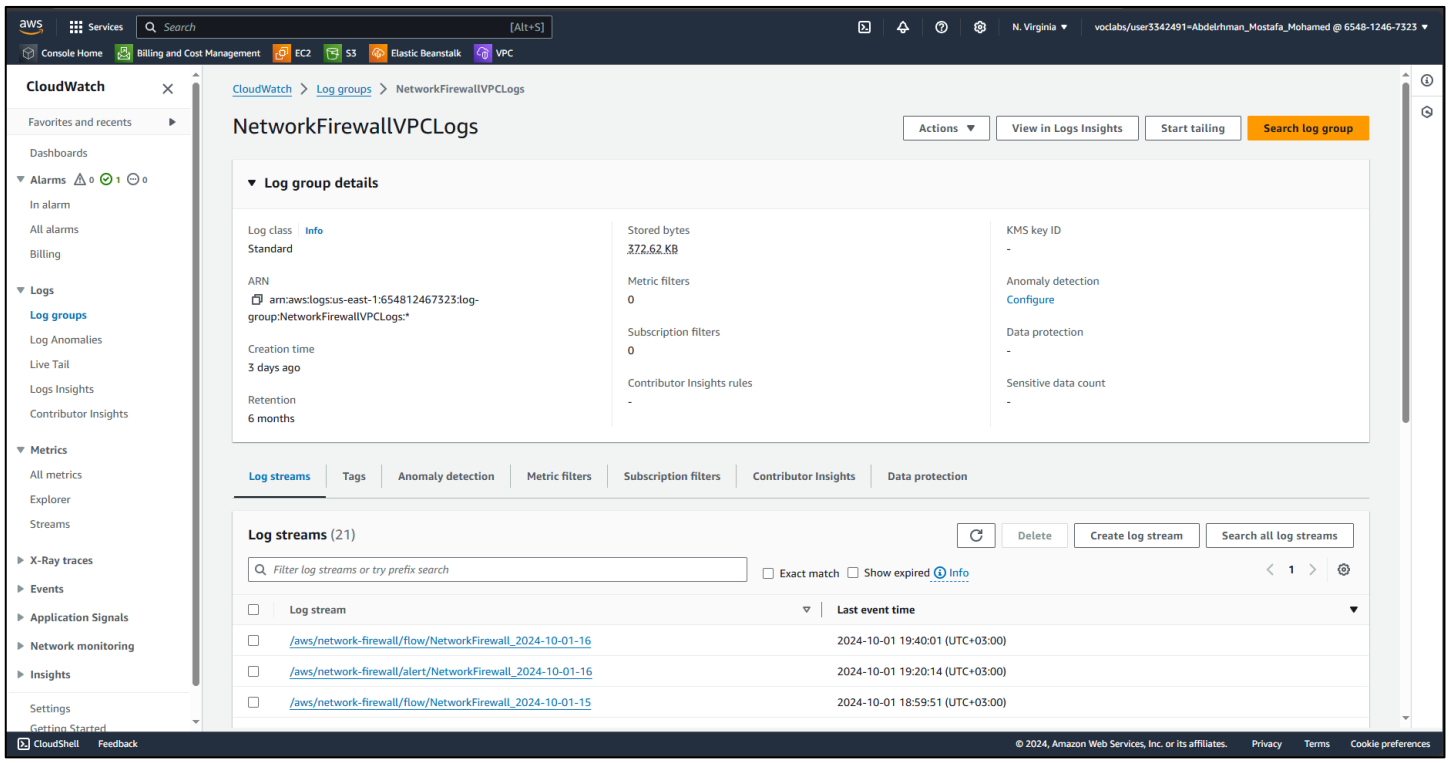
Task 2.8: Create route tables



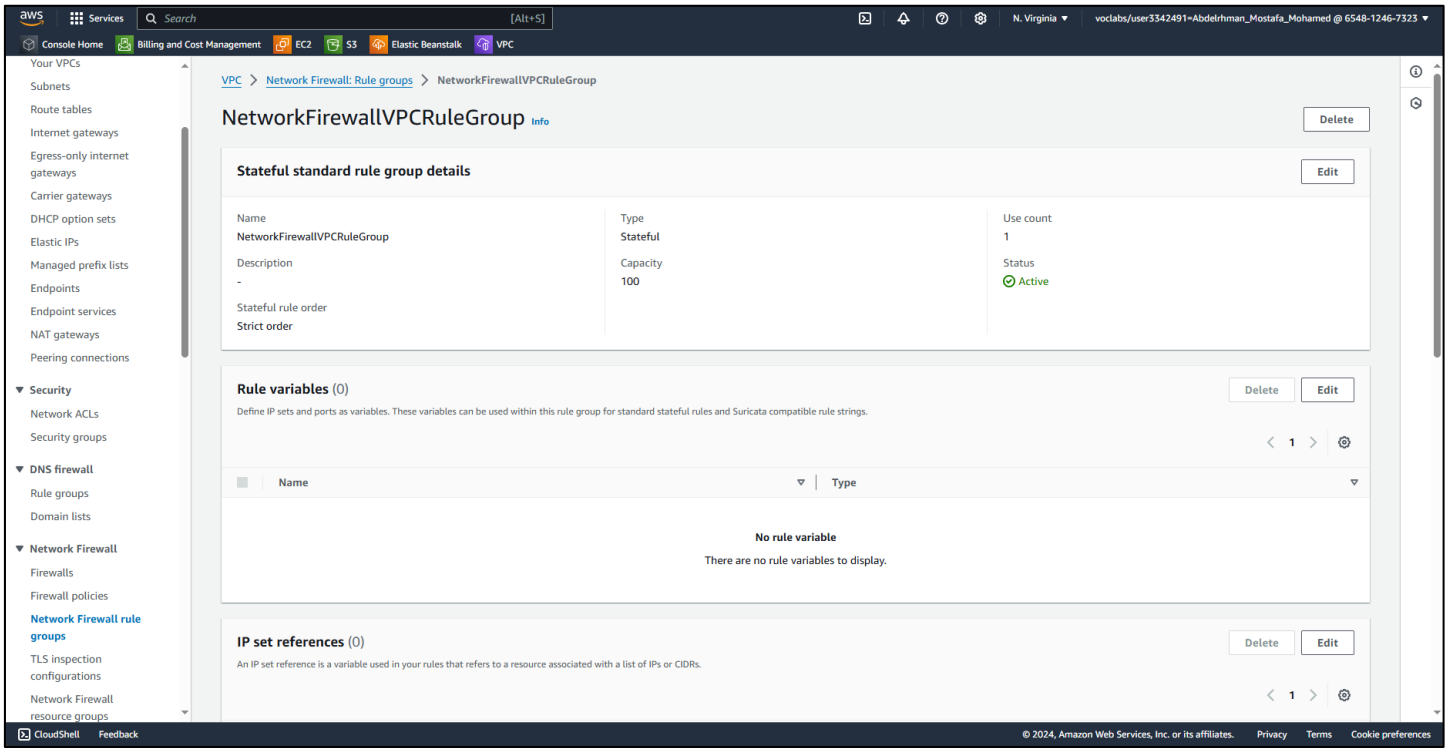


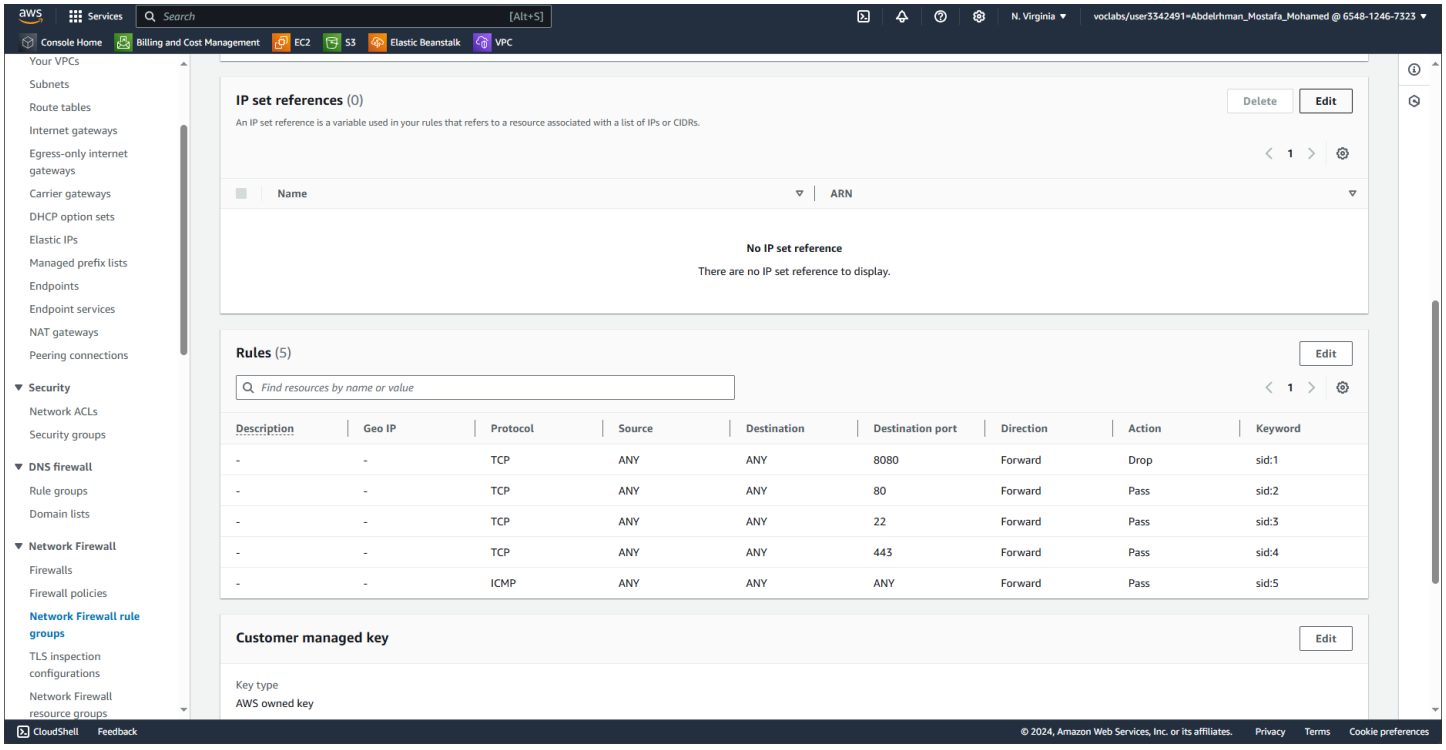

Services
Network Firewall Rules
Console Home
Billing and Cost Management
EC2
S3
Elastic Beanstalk
VPC
N. Virginia
voclabs/user3342491=Abdelrhman_Mostafa_Mohamed @ 6548-1246-7323
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
DNS firewall
Rule groups
Domain lists
Network Firewall
Firewalls
Firewall policies
Network Firewall rule groups
VPC > Route tables > rtb-0bb7a79d391215da9
rtb-0bb7a79d391215da9 / IGW-Ingress-Route-Table
Actions
Details Info
Route table ID
rtb-0bb7a79d391215da9
Main
No
Explicit subnet associations
–
Edge associations
igw-05afa5bee40c5a0cb / NetworkFirewallIG
VPC
vpc-07a19f79164561498 | NetworkFirewallVPC
Owner ID
654812467323
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (2)
Both
Edit routes
Filter routes
1
Destination
Target
Status
Propagated
10.1.0.0/16
local
Active
No
10.1.3.0/28
vpce-0ee5aaf4208bc1d15
Active
No
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Task 2.9: Configure logging for the network firewall



Task 2.10: Configure the firewall policy and test access

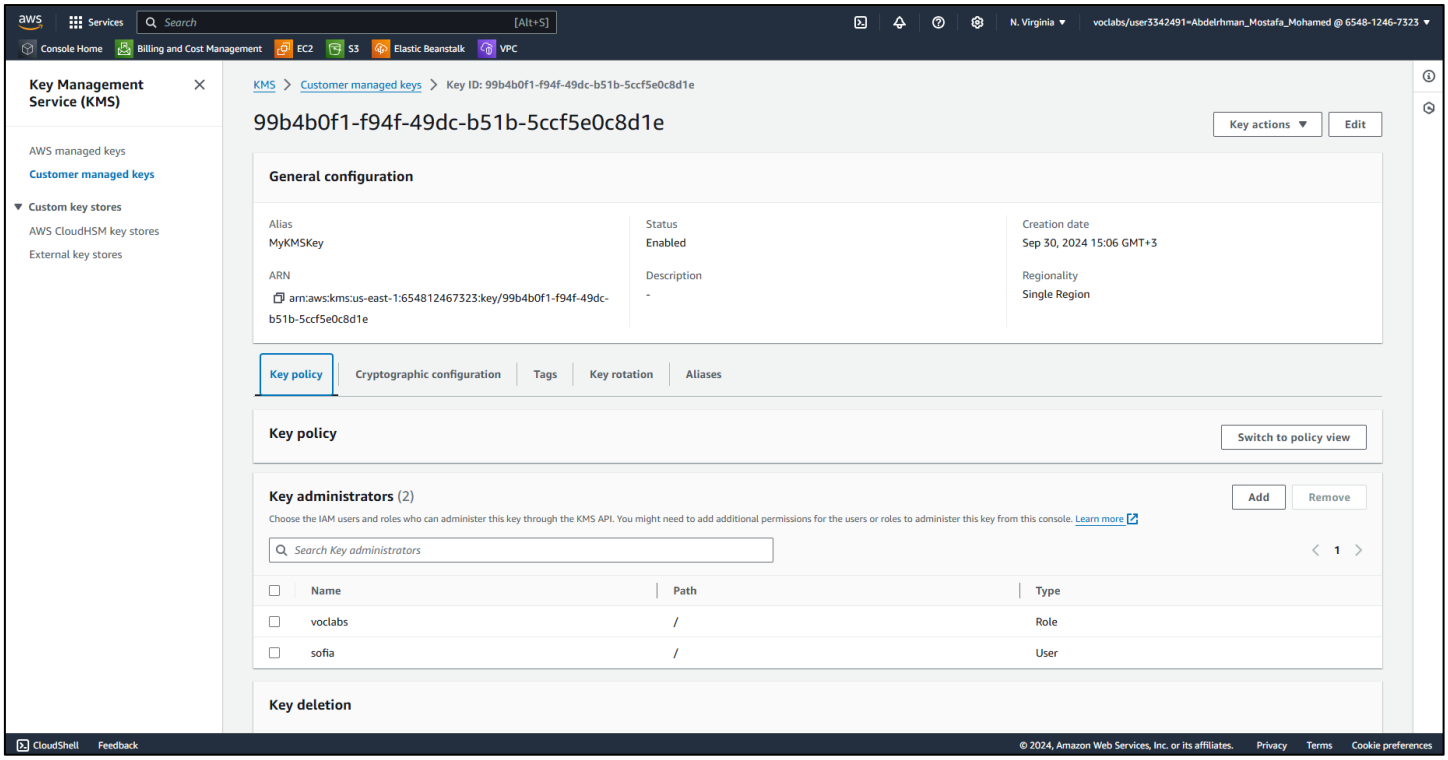


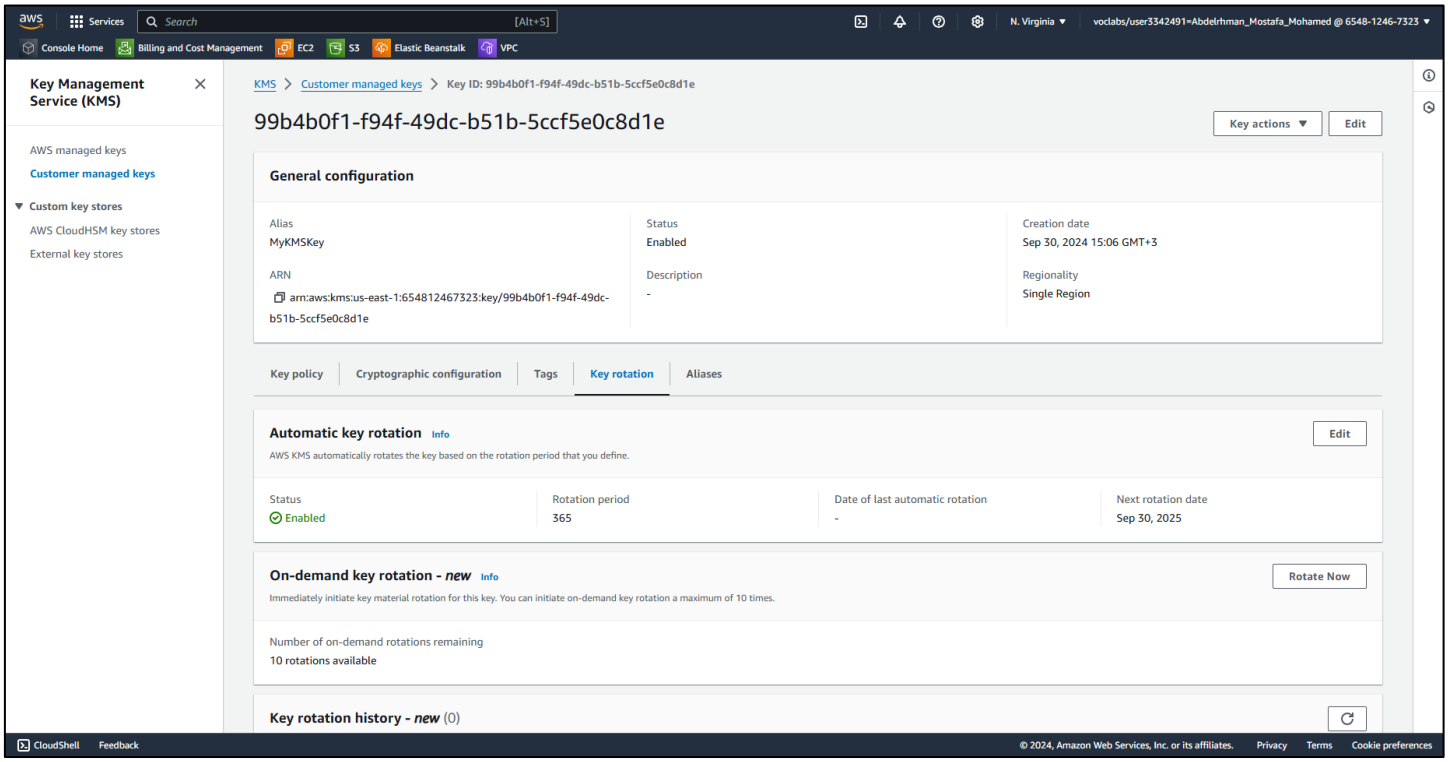


Cost estimate to secure a VPC with a network firewall : CSV File

Phase 3: Securing AWS resources by using AWS KMS

Task 3.1: Create a customer managed key and configure key rotation



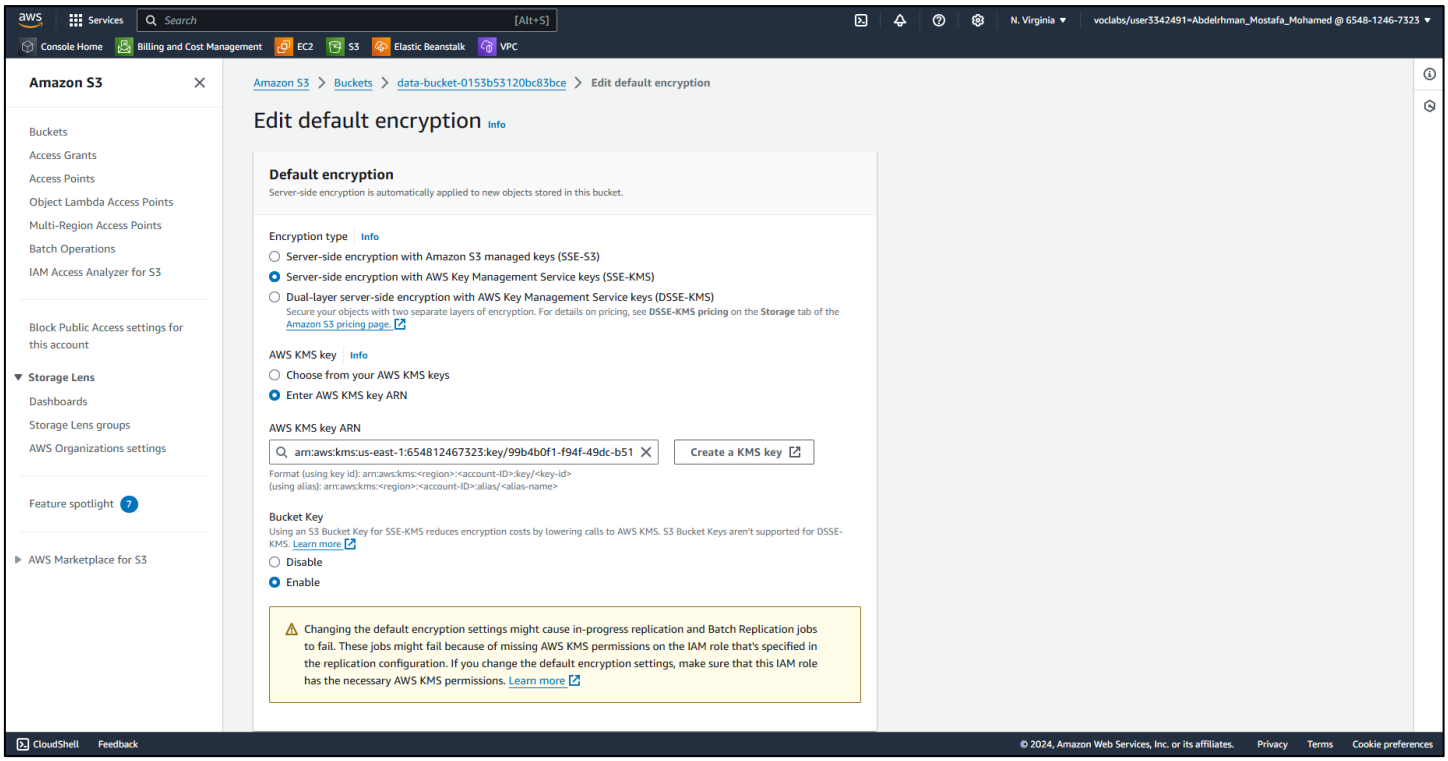


Task 3.2: Update the AWS KMS key policy and analyze an IAM policy

Key policy

Edit | Switch to default view

```
{
    "Sid": "Allow access for Key Administrators",
    "Effect": "Allow",
    "Principal": {
        "AWS": [
            "arn:aws:iam::654812467323:role/voclabs",
            "arn:aws:iam::654812467323:user/sofia"
        ]
    },
    "Action": [
        "kms:Create*",
        "kms:Describe*",
        "kms:Enable*",
```



aws | Services | Search [Alt+S] | N. Virginia | voclabs/user3342491=Abdelrhman_Mostafa_Mohamed @ 6548-1246-7323

Console Home | Billing and Cost Management | EC2 | S3 | Elastic Beanstalk | VPC

Amazon S3

- Buckets
- Access Grants
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

- Storage Lens
  - Dashboards
  - Storage Lens groups
  - AWS Organizations settings

Feature spotlight 7

- AWS Marketplace for S3

Amazon S3 > Buckets > data-bucket-0153b53120bc83bce > Edit default encryption

Edit default encryption Info

Default encryption

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info

- Server-side encryption with Amazon S3 managed keys (SSE-S3)
- Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing** on the **Storage** tab of the Amazon S3 pricing page.

AWS KMS key Info

- Choose from your AWS KMS keys
- Enter AWS KMS key ARN

AWS KMS key ARN

arn:aws:kms:us-east-1:654812467323:key/99b4b0f1-f94f-49dc-b51 | Create a KMS key

Format (using key id): arn:aws:kms:<region>:<account-ID>:key/<key-id>
(using alias): arn:aws:kms:<region>:<account-ID>:alias/<alias-name>

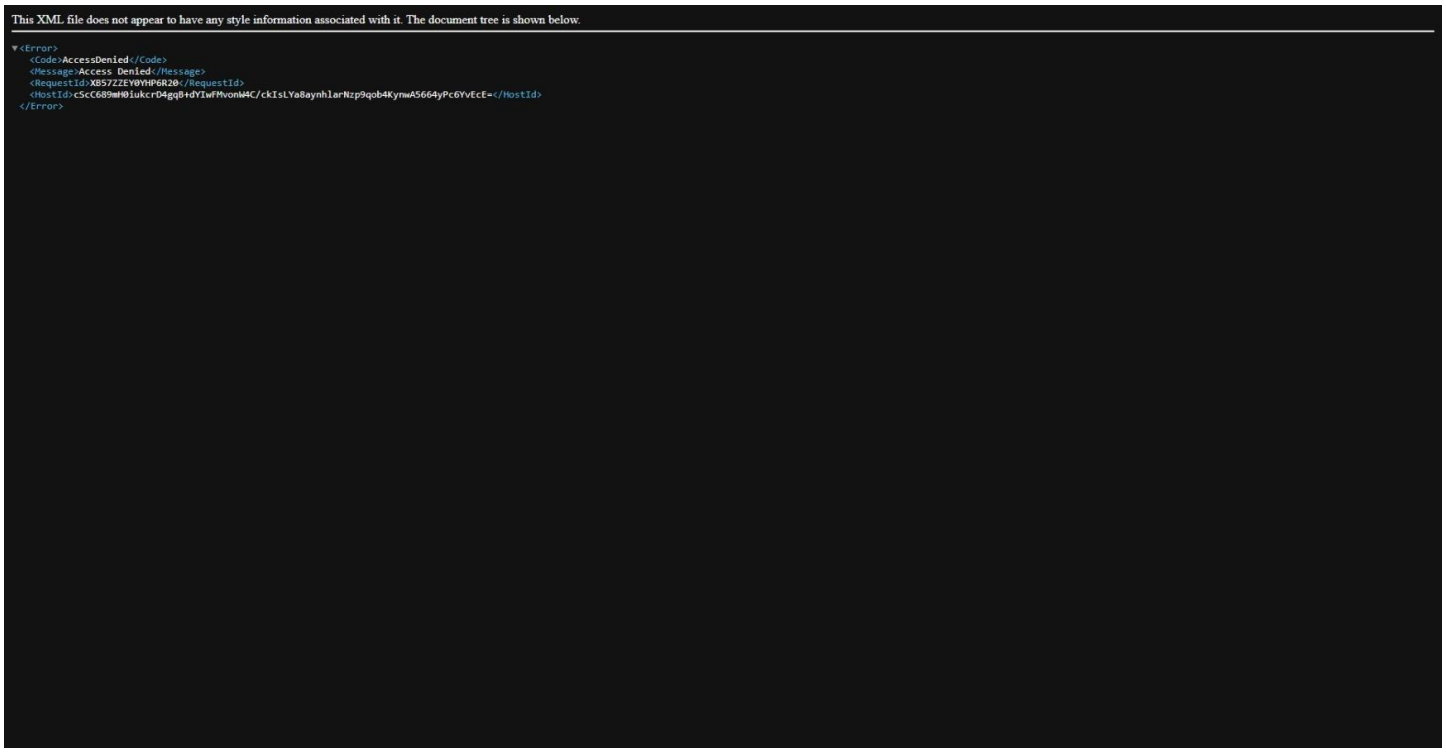
Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more

- Disable
- Enable

⚠ Changing the default encryption settings might cause in-progress replication and Batch Replication jobs to fail. These jobs might fail because of missing AWS KMS permissions on the IAM role that's specified in the replication configuration. If you change the default encryption settings, make sure that this IAM role has the necessary AWS KMS permissions. Learn more

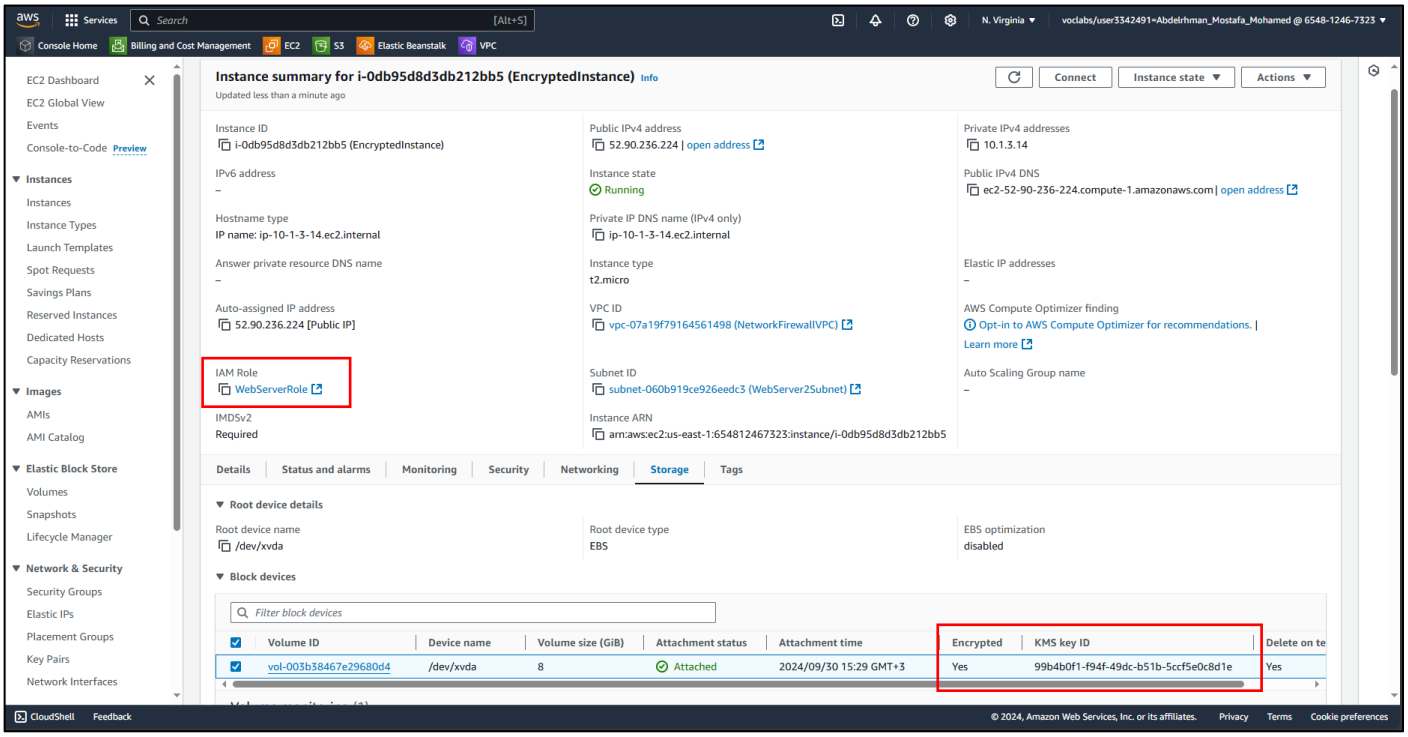
CloudShell | Feedback | © 2024, Amazon Web Services, Inc. or its affiliates. | Privacy | Terms | Cookie preferences



This XML file does not appear to have any style information associated with it. The document tree is shown below.

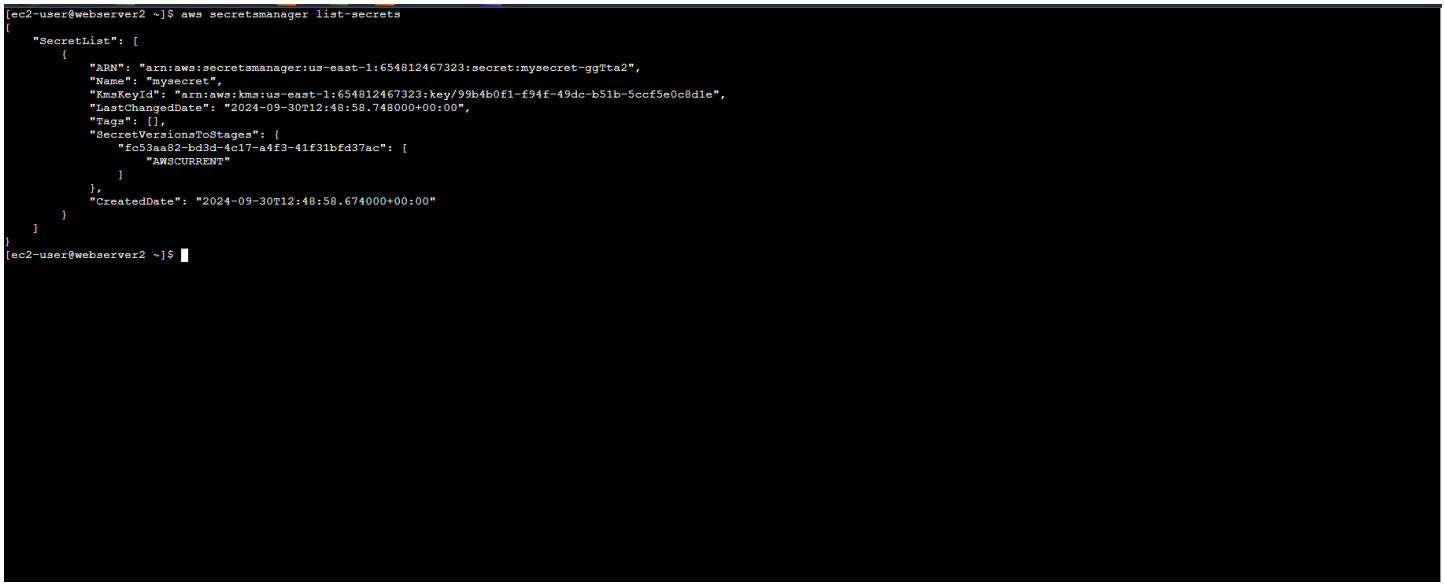
```
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>X857ZZEY0YHP6R20</RequestId>
  <HostId>cScC689mH0iukcrD4gqB+dYIwFMvonW4C/ckIsLYa8aynhlarNzp9qob4KynwA5664yPc6YvEcE=</HostId>
</Error>
```

Task 3.4: Use AWS KMS to encrypt the root volume of an EC2 instance



Task 3.5: Use AWS KMS envelope encryption to encrypt data in place

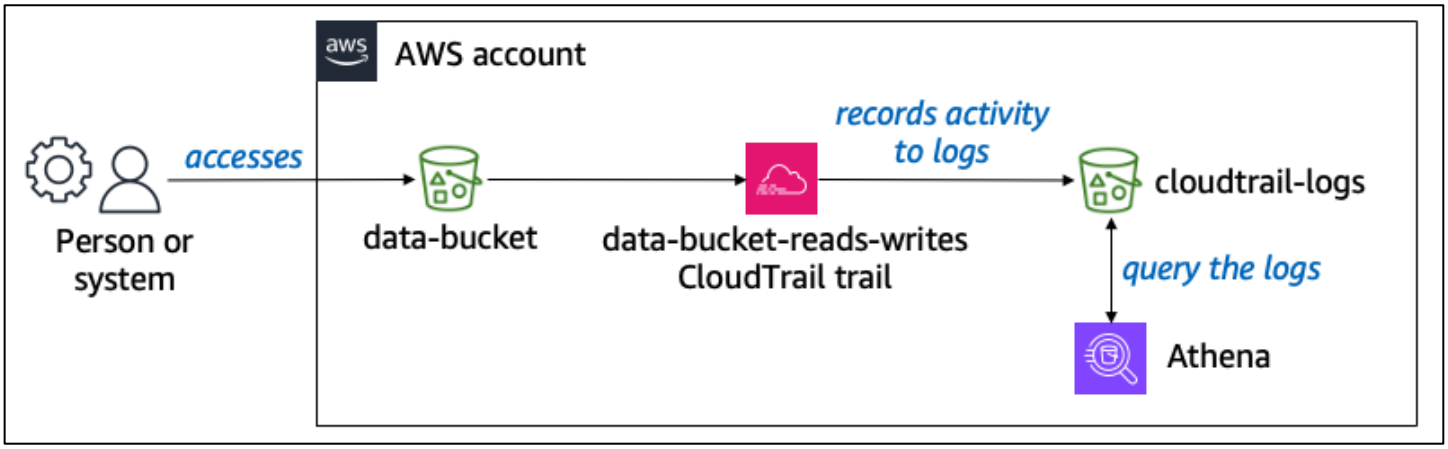
Task 3.6: Use AWS KMS to encrypt a Secrets Manager secret

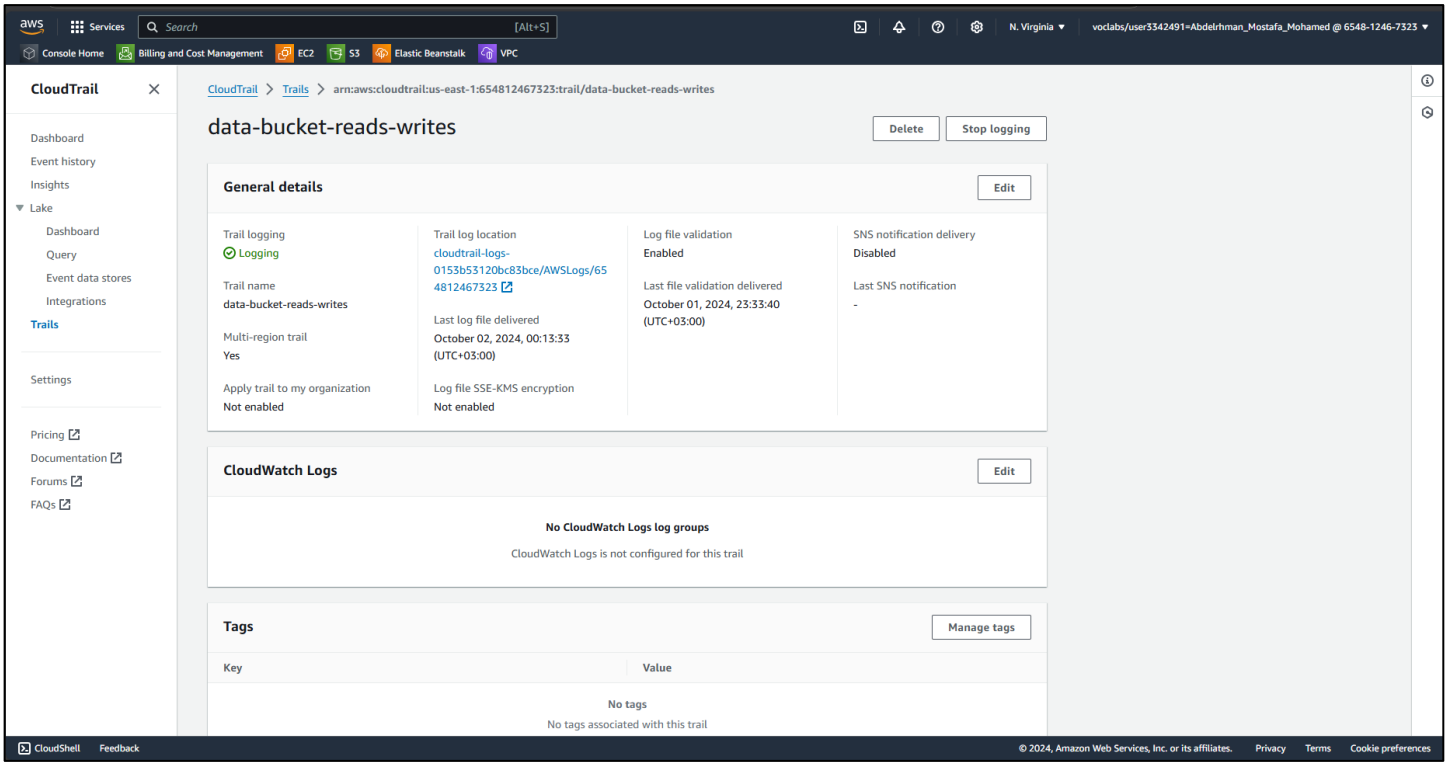


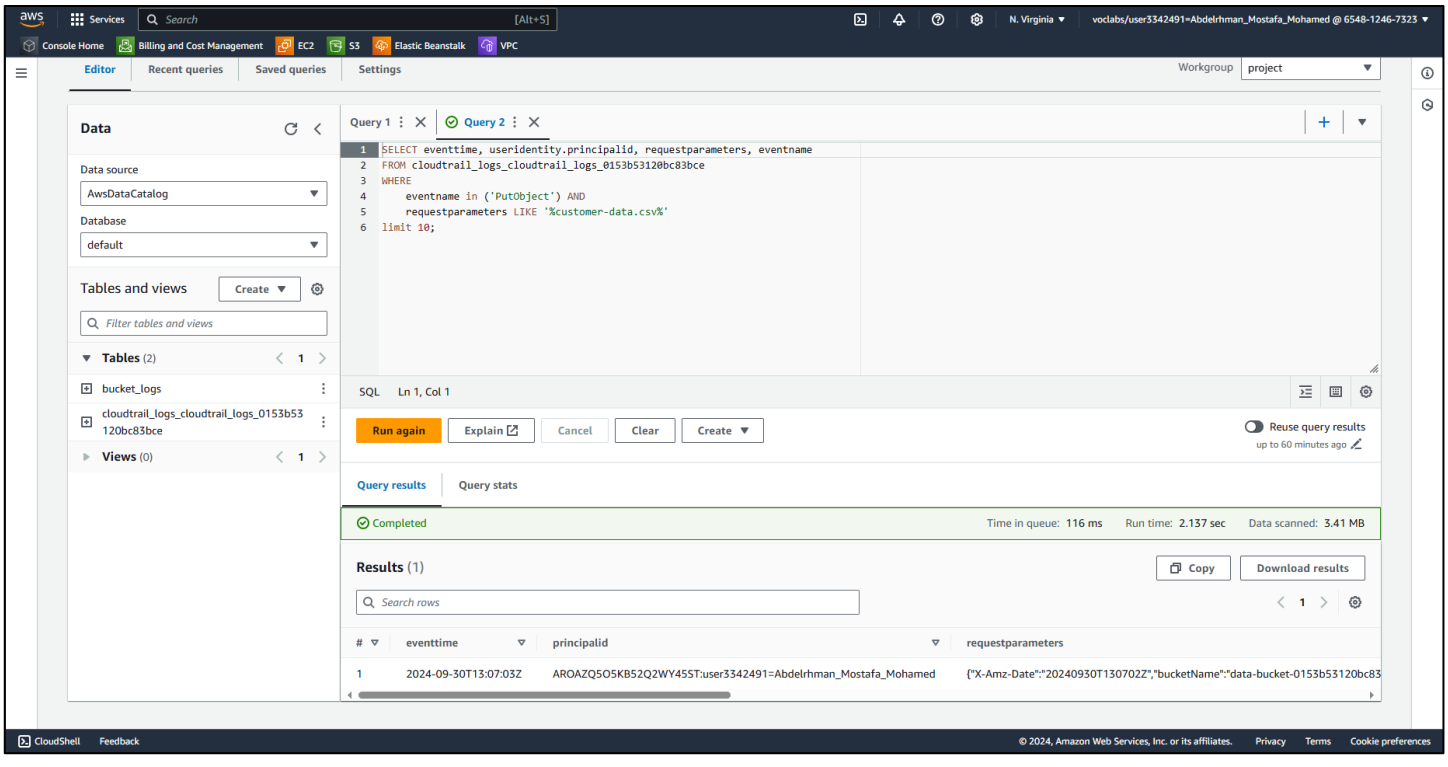
Cost assessment for using AWS KMS CSV file

Phase 4: Monitoring and logging

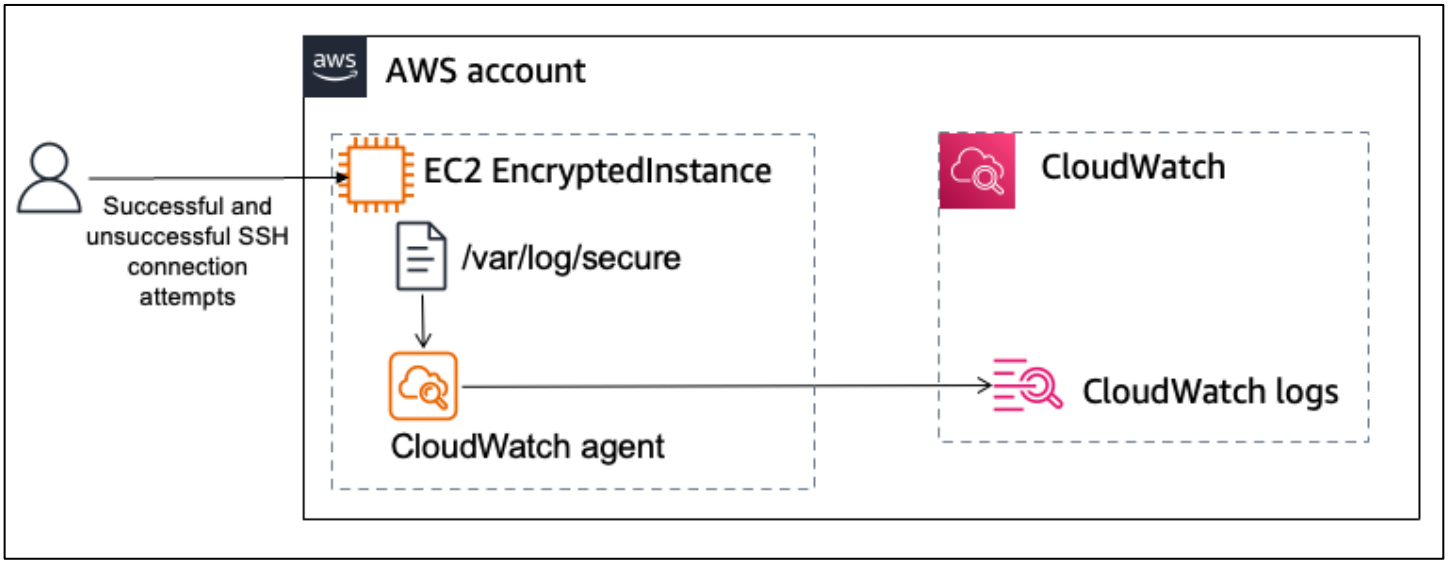
Task 4.1: Use CloudTrail to record Amazon S3 API calls

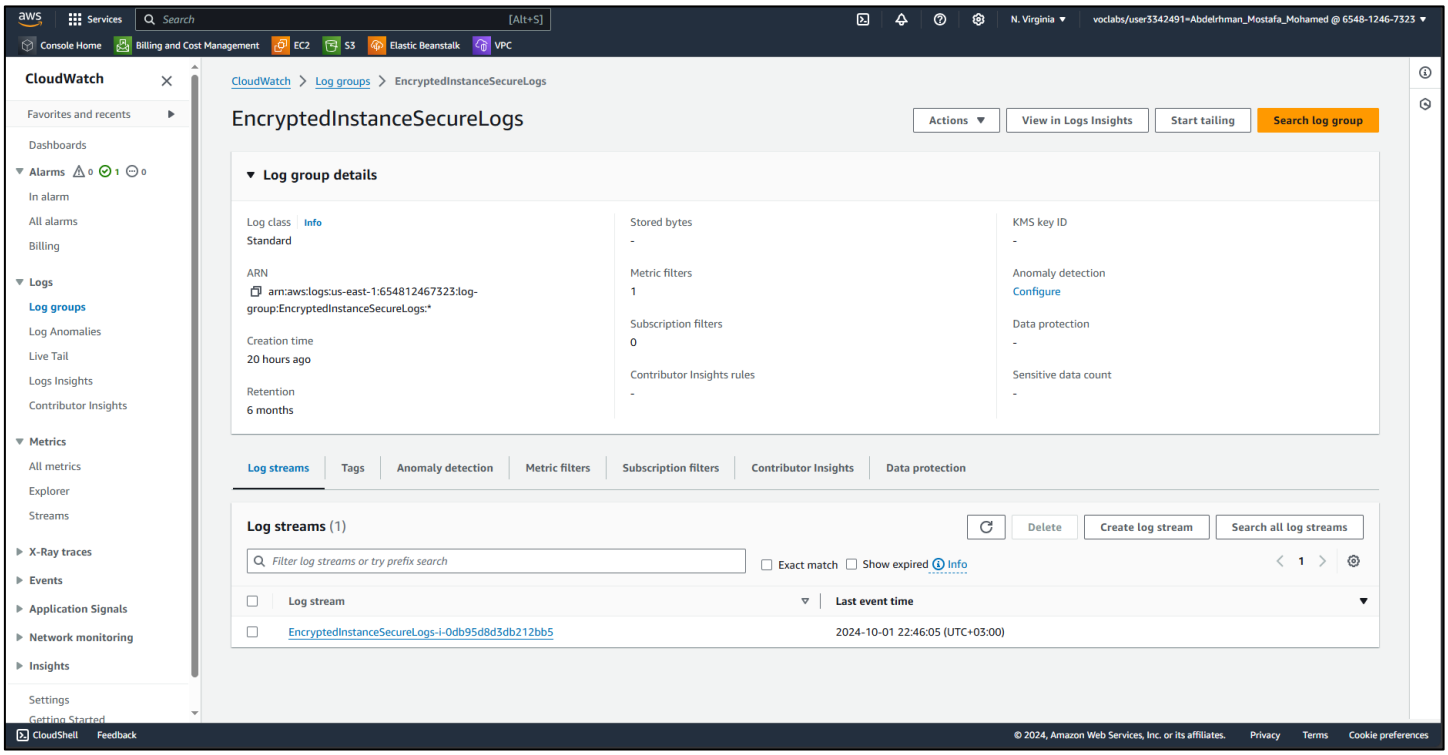


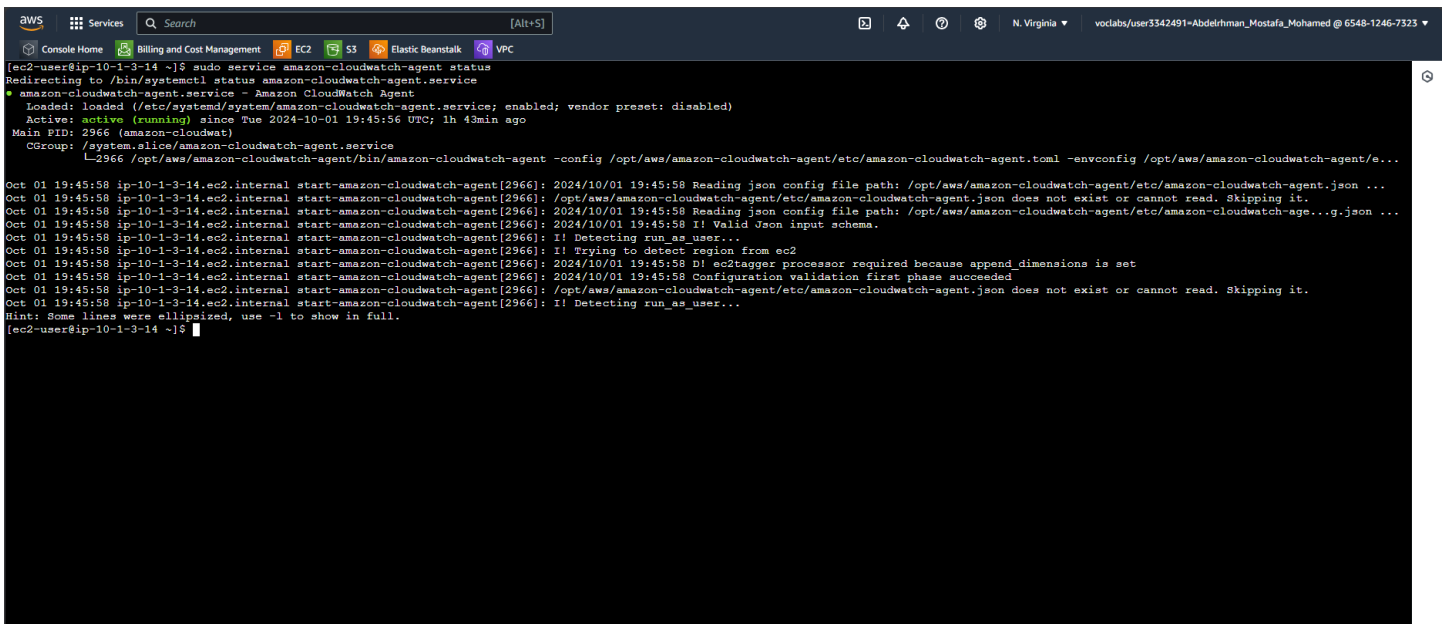




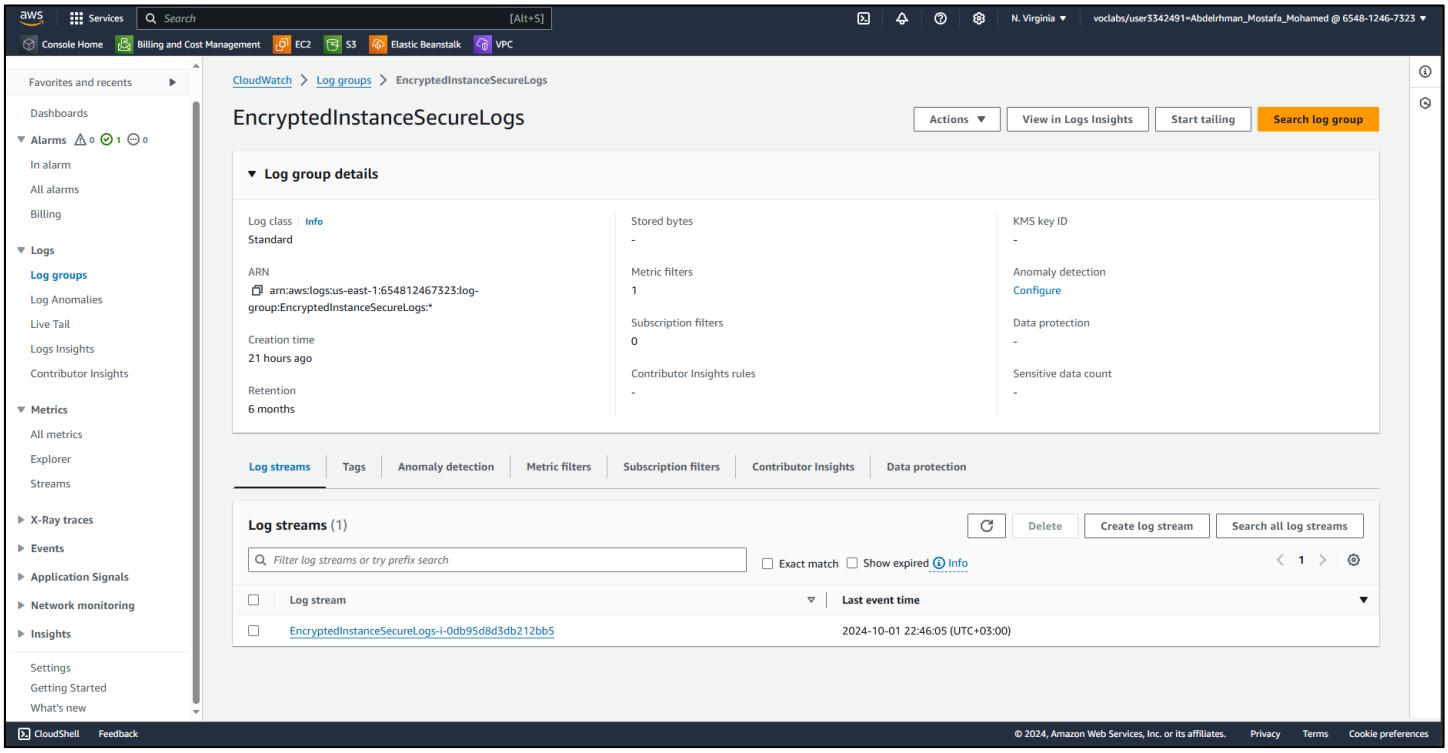
Task 4.2: Use CloudWatch Logs to monitor secure logs

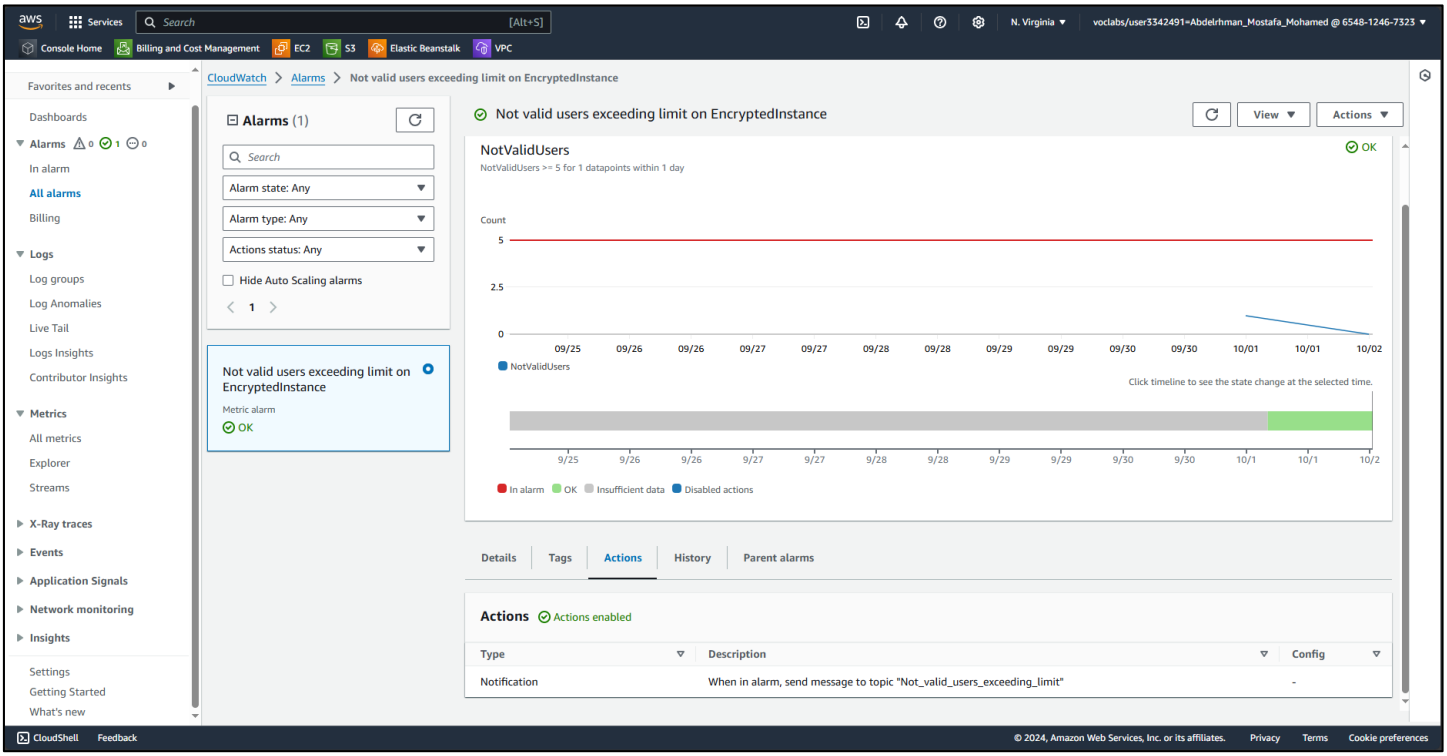




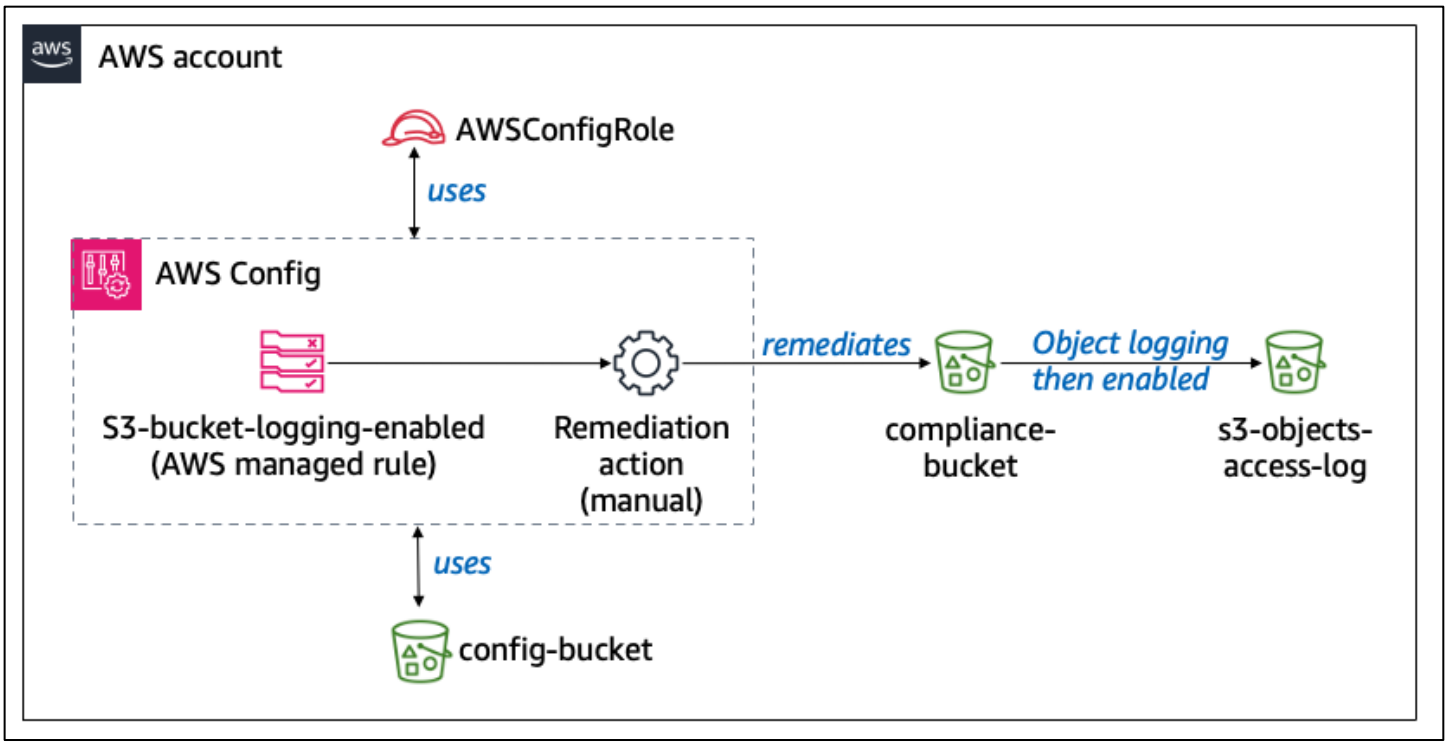


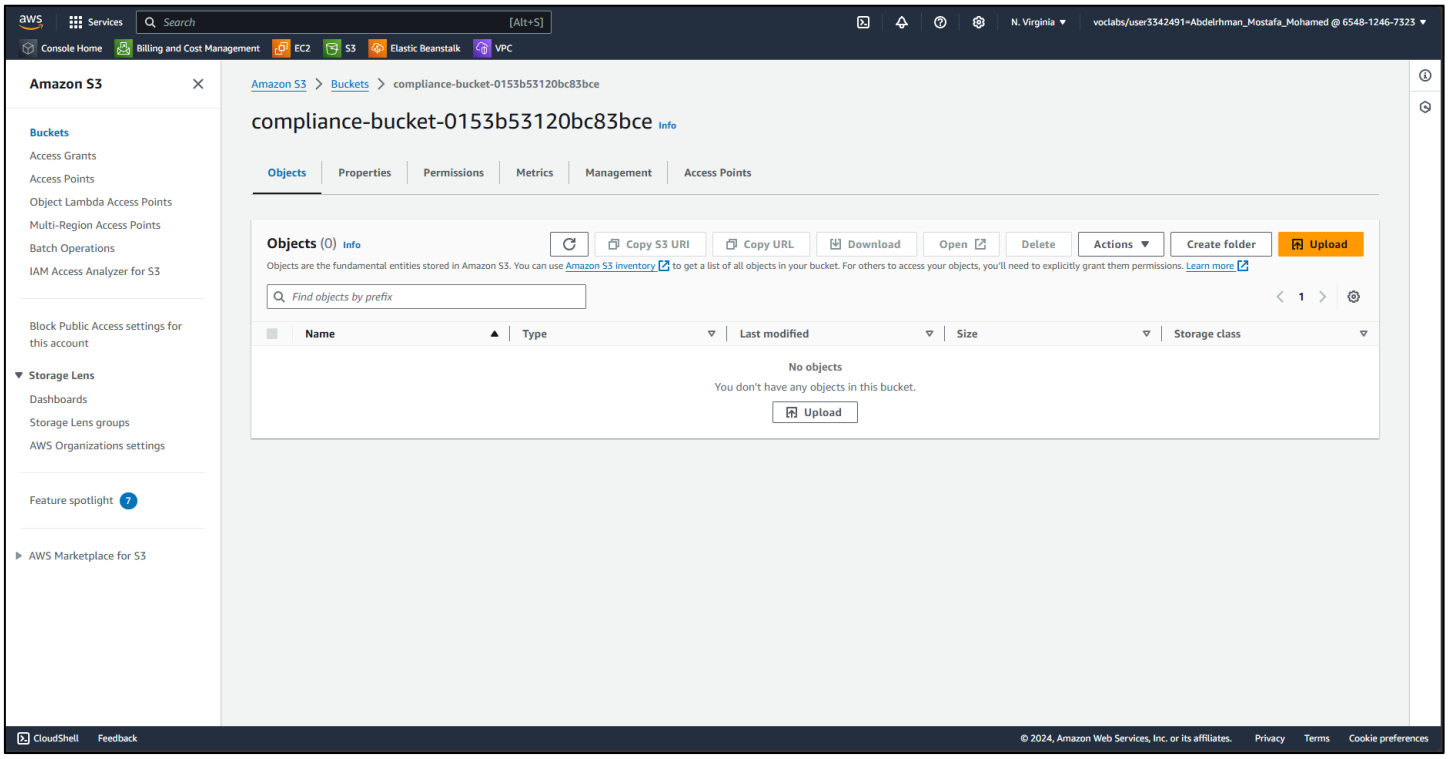
Task 4.3: Create a CloudWatch alarm to send notifications for security incidents

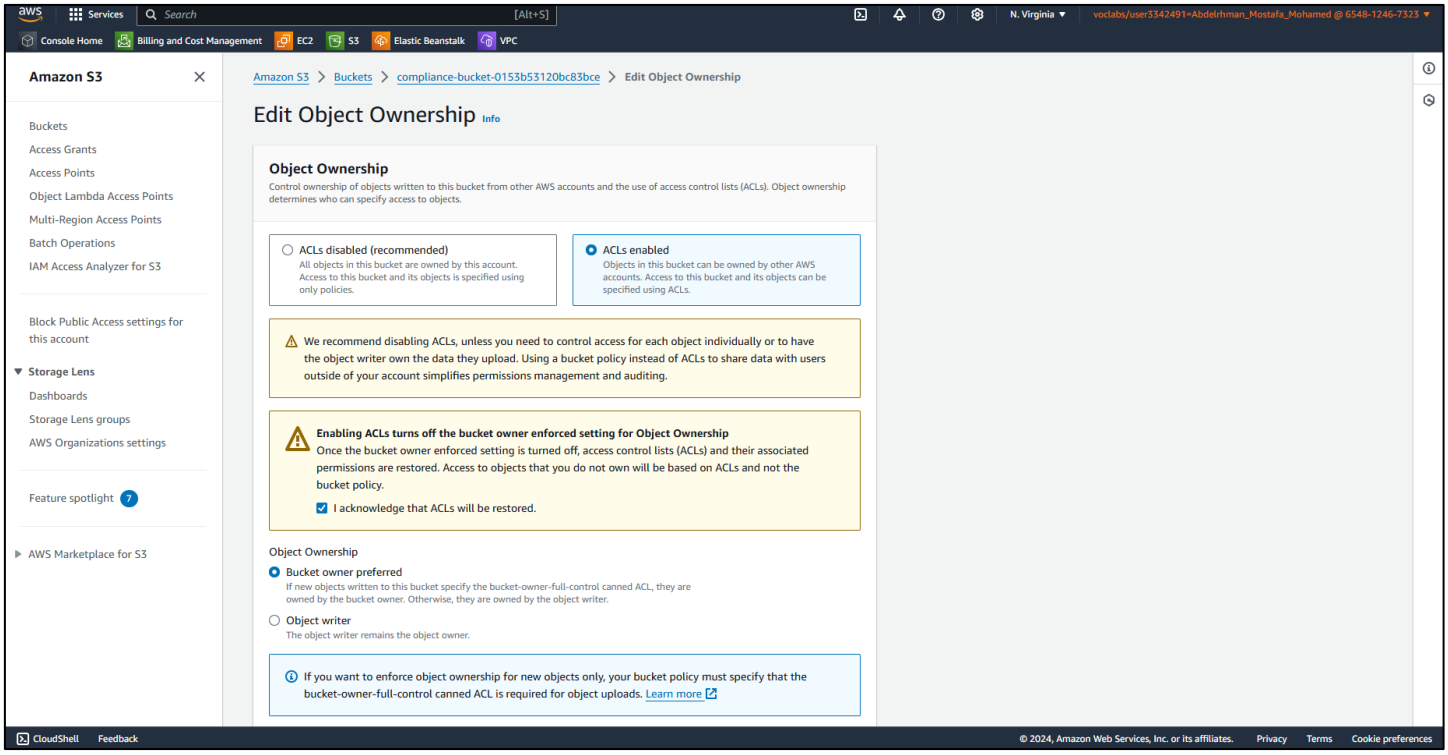


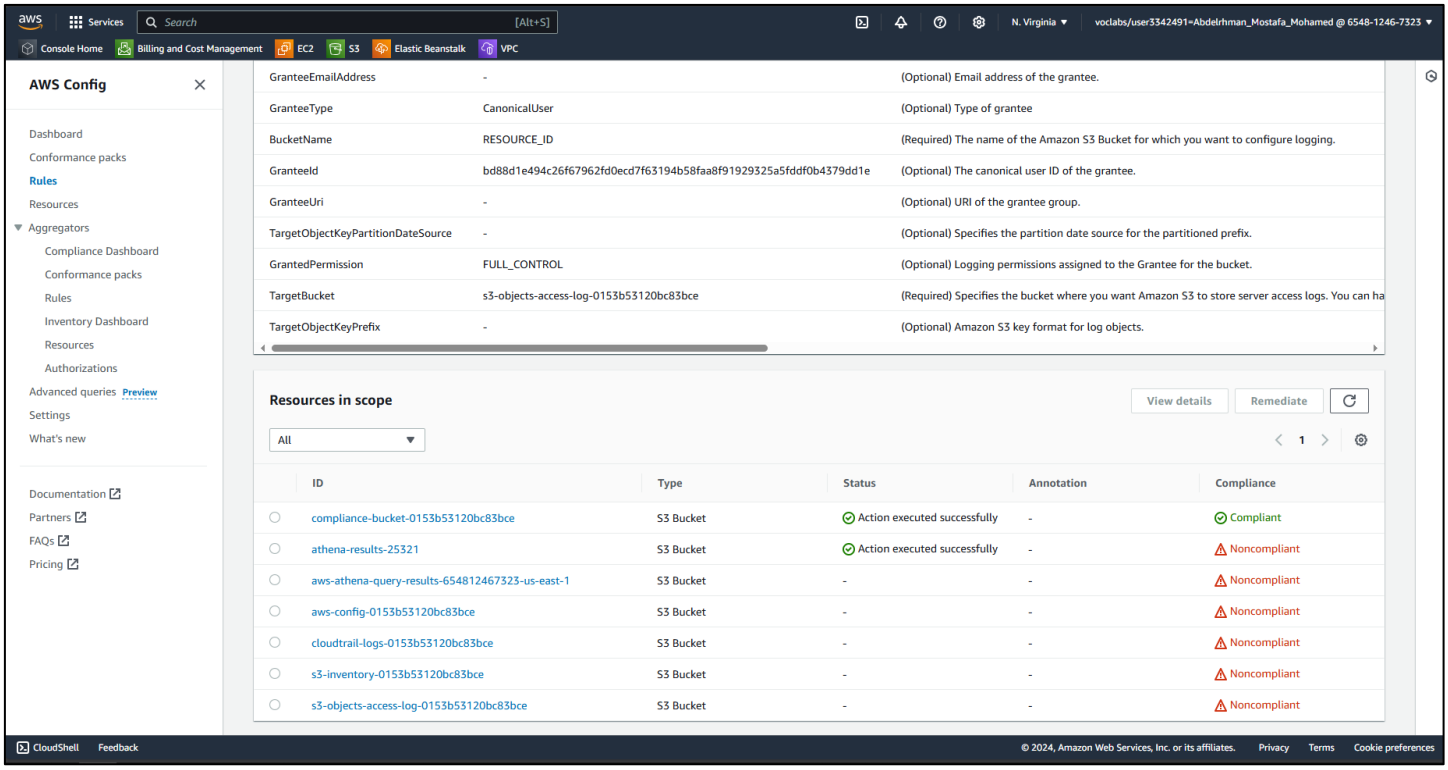


Task 4.4: Configure AWS Config to assess security settings and remediate the configuration of AWS resources









Cost assessment for monitoring and logging : CSV File

Badge Link