

Securing AWS Infrastructure

Phase 1: Securing Data in Amazon S3

Task 1.1: Create a Bucket, Apply a Bucket Policy, and Test Access

- **Description:** Creating an Amazon S3 bucket, applying a bucket policy to control access, and testing the access restrictions.
- **Steps:**
 1. Created an S3 bucket via AWS Management Console/CLI.
 2. Applied a bucket policy to restrict access (based on roles, IP ranges, or conditions).
 3. Tested access by attempting to upload or retrieve objects as different users.
- **Tools:** AWS S3, AWS Management Console, AWS CLI.

Policy

```
1 {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Effect": "Deny",  
6             "Principal": "*",  
7             "Action": "s3:*",  
8             "Resource": [  
9                 "arn:aws:s3::data-bucket-321",  
10                "arn:aws:s3::data-bucket-321/*"  
11            ],  
12            "Condition": {  
13                "StringNotEquals": {  
14                    "aws:PrincipalArn": [  
15                        "arn:aws:iam::939695913401:role/voclabs",  
16                        "arn:aws:iam::939695913401:user/paulo",  
17                        "arn:aws:iam::939695913401:user/sofia"  
18                    ]  
19                }  
20            }  
21        },  
22    ]  
23 }
```

Task 1.2: Enable Versioning and Object-Level Logging on a Bucket

- **Description:** Enable versioning to keep track of different versions of objects and configure logging to track object access at the request level.
- **Steps:**
 1. Enabled versioning on the S3 bucket to store multiple object versions.
 2. Enabled server access logging for object-level activity.

3. Verified functionality by modifying an object and reviewing log files.

- **Tools:** AWS S3, AWS Management Console, AWS CLI.

Task 1.3: Implement the S3 Inventory Feature on a Bucket

- **Description:** Using S3 Inventory to generate reports on the objects in a bucket.
- **Steps:**
 1. Configured the S3 Inventory feature to create a report of bucket contents.
 2. Chose daily or weekly inventory frequency.
 3. Verified the output in CSV format by reviewing the generated inventory file.
- **Tools:** AWS S3, S3 Inventory, AWS CLI.

Task 1.4: Confirm That Versioning Works as Intended

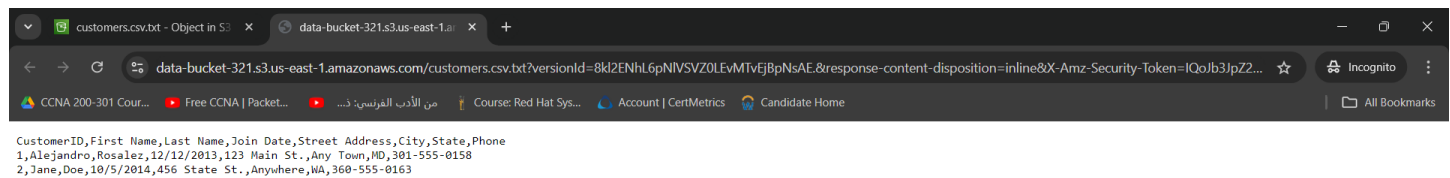
- **Description:** Testing the versioning capability to ensure that the bucket retains multiple versions of an object.
- **Steps:**
 1. Uploaded an initial version of an object.
 2. Uploaded a modified version of the same object.
 3. Reviewed object versions in the S3 console.
- **Tools:** AWS S3, AWS CLI.

The screenshot shows the Amazon S3 console interface. The left sidebar contains navigation options: 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 (selected), Dashboards, Storage Lens groups, and AWS Organizations settings. The main content area is titled 'Objects (3) Info' and includes buttons for Upload, Copy S3 URI, Copy URL, Download, Open, Delete, Actions, and Create folder. Below these buttons is a search bar 'Find objects by prefix' and a 'Show versions' toggle. The object list table is as follows:

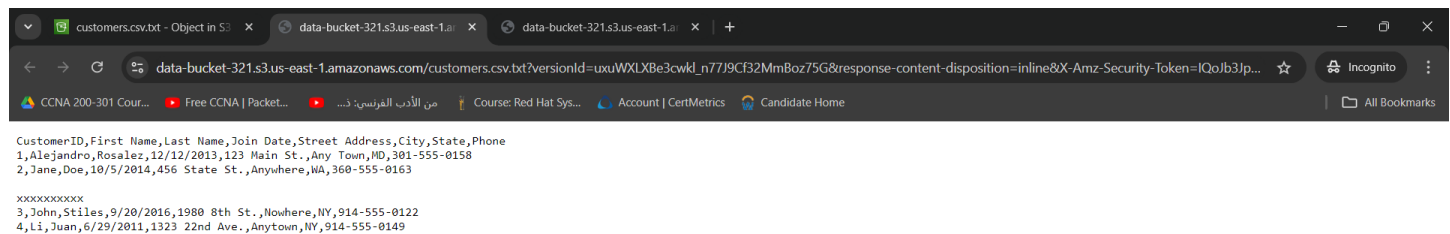
	Name	Type	Version ID	Last modified	Size	Storage class
<input type="checkbox"/>	customers.csv.txt	txt	uxuWXLXBe3cwkl_n77J9Cf32MmBoz75G	October 4, 2024, 14:31:30 (UTC+03:00)	340.0 B	Standard
<input type="checkbox"/>	customers.csv.txt	txt	8kl2ENhL6pNlVSZ0LEVM TvEjBpNsAE.	October 4, 2024, 14:30:17 (UTC+03:00)	204.0 B	Standard
<input type="checkbox"/>	myfile.txt	txt	null	October 2, 2024, 09:01:59 (UTC+03:00)	11.0 B	Standard

The bottom of the screenshot shows the Windows taskbar with the time 2:35 PM on 10/4/2024.

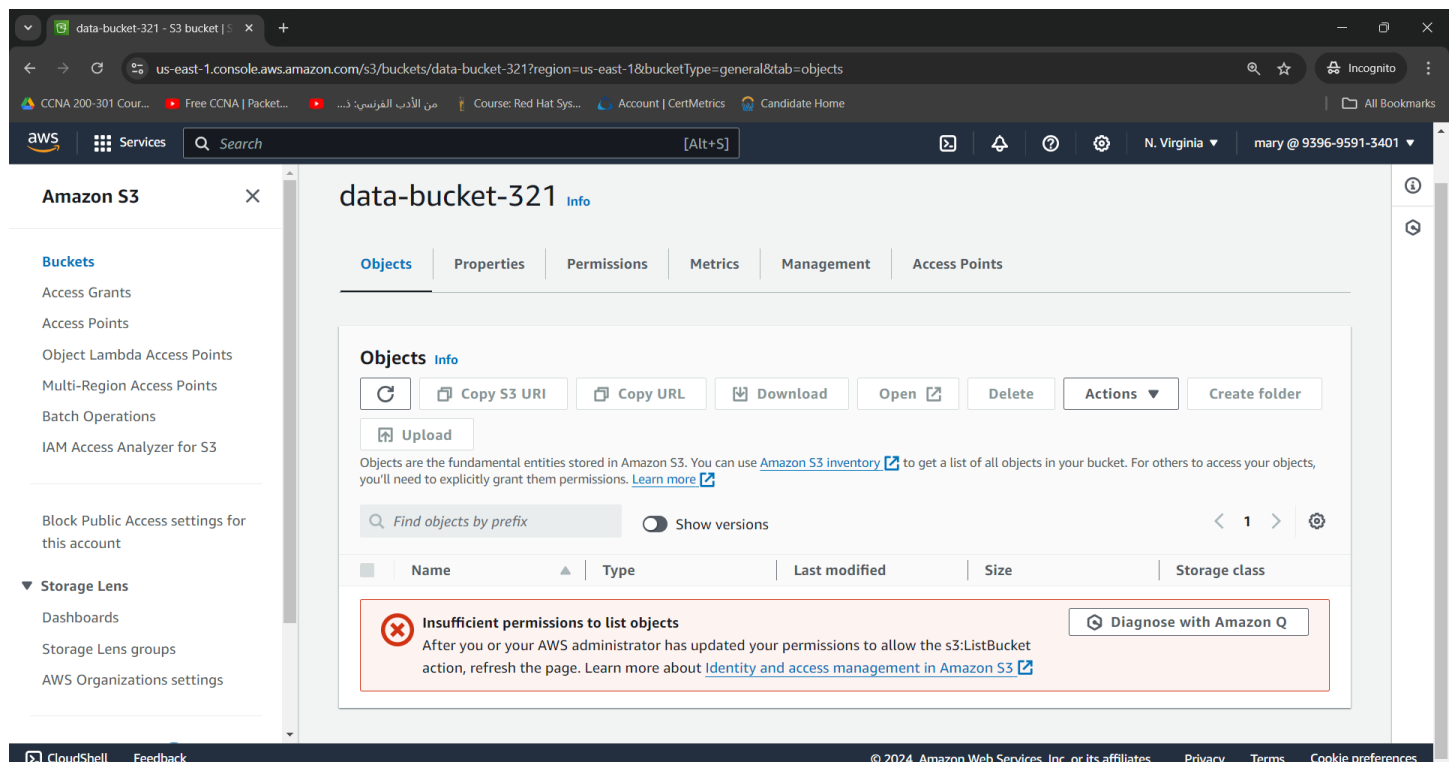
The first Uploaded file



The second Uploaded file after versioning



Logging from MARYs account



Task 1.5: Confirm Object-Level Logging and Query the Access Logs Using Athena

- Description:** Verifying object-level access logs and querying these logs using Amazon Athena.
- Steps:**

1. Configured S3 to log object-level activities.
2. Set up an Athena table to query the access logs.
3. Ran a sample query to filter specific access patterns or IP addresses.

- **Tools:** AWS S3, Amazon Athena, AWS CLI.

The screenshot shows the AWS Athena console interface. On the left, the 'Data' sidebar is visible with 'Data source' set to 'AwsDataCatalog' and 'Database' set to 'default'. The 'Tables and views' section shows a table named 'bucket_logs'. The main area displays the SQL configuration for 'Query 1'. The SQL code defines a table with a single column 'accesspointarn' of type 'STRING' and a 'ROW FORMAT SERDE' of 'org.apache.hadoop.hive.serde2.RegexSerDe'. The 'WITH SERDEPROPERTIES' section includes a complex regular expression for the 'input.regex' property. The table is stored as 'INPUTFORMAT org.apache.hadoop.mapred.TextInputFormat' and 'OUTPUTFORMAT org.apache.hadoop.hive.q1.io.HiveIgnoreKeyTextOutputFormat'. The location is set to 's3://s3-objects-access-log-
<UNIQUE-ID>/'. At the bottom, there are buttons for 'Run', 'Explain', 'Cancel', 'Clear', and 'Create', along with a 'Reuse query results' toggle.

The screenshot shows the AWS Athena console interface with the query results displayed. The SQL query is:

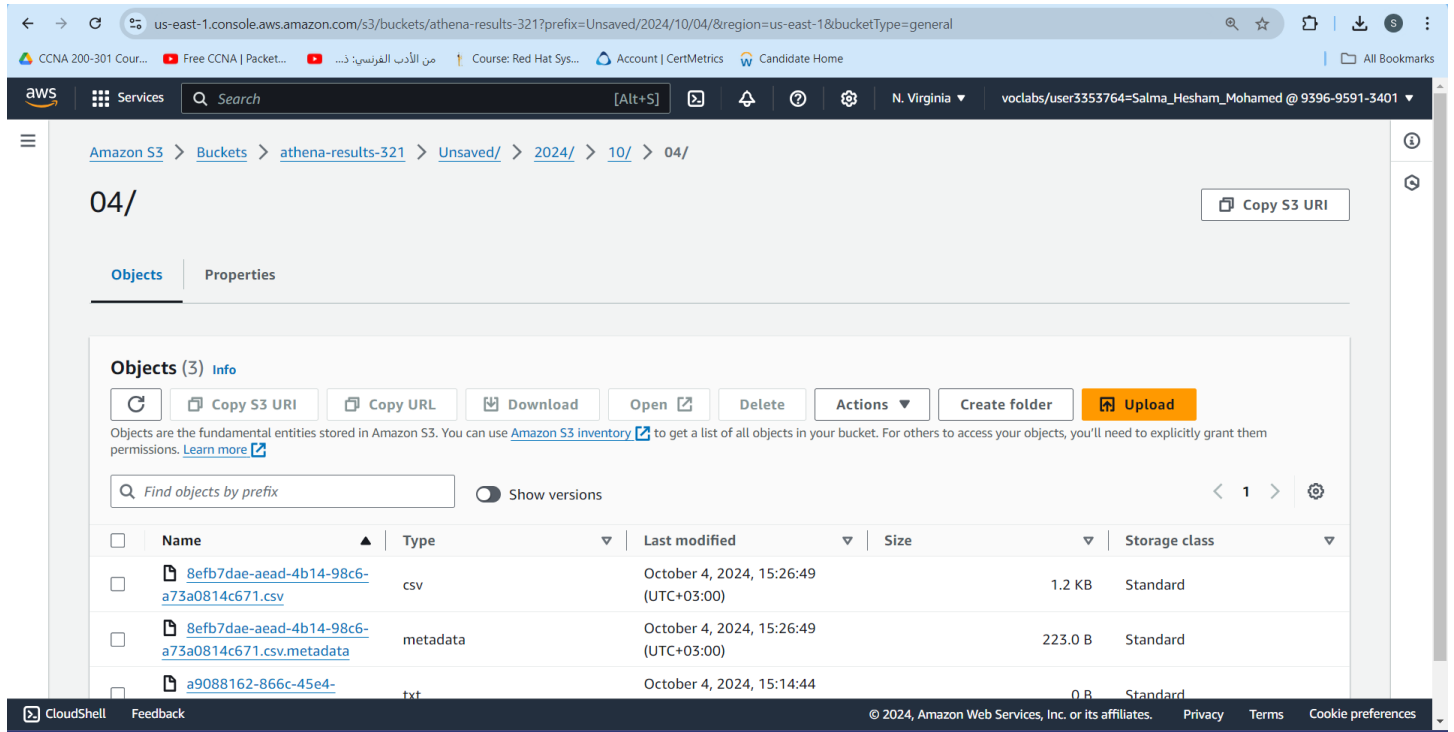

```
SELECT requester, operation, key, httpstatus
FROM "default"."bucket_logs"
WHERE requester LIKE 'arn:aws:iam%';
```

 The query is completed, with a time in queue of 63 ms, a run time of 863 ms, and 45.45 KB of data scanned. The results table has 15 rows. The first two rows are:

#	requester	operation	key	httpstatus
1	arn:aws:iam::939695913401:user/paulo	REST.GET.VERSIONING	-	200
2	arn:aws:iam::939695913401:user/paulo	REST.PUT.OBJECT	customers.csv.txt	200

 The interface includes a search bar for rows, pagination controls, and buttons for 'Copy' and 'Download results'.

The Athena Bucket that is used by Athena service to save its output



Task 1.6: Review the S3 Inventory Report Using S3 Select

- **Description:** Reviewing S3 Inventory reports by using S3 Select to filter and query specific data.
- **Steps:**
 1. Downloaded the S3 Inventory report.
 2. Used S3 Select to run a query on the CSV or Parquet report.
 3. Verified the results.
- **Tools:** AWS S3, S3 Select, AWS CLI.

Cost Assessment for Securing Amazon S3

- **Description:** Calculating costs for S3 features such as storage, versioning, logging, inventory reports, and Athena queries.

Phase 2: Securing VPCs

Task 2.1: Review LabVPC and Its Associated Resources

- **Description:** Reviewing the existing VPC, subnets, route tables, and security configurations.
- **Steps:**
 1. Reviewed the LabVPC configuration, including subnets, routing, and security groups.

2. Documented all associated resources and their purposes.

- **Tools:** AWS VPC Console, AWS CLI.

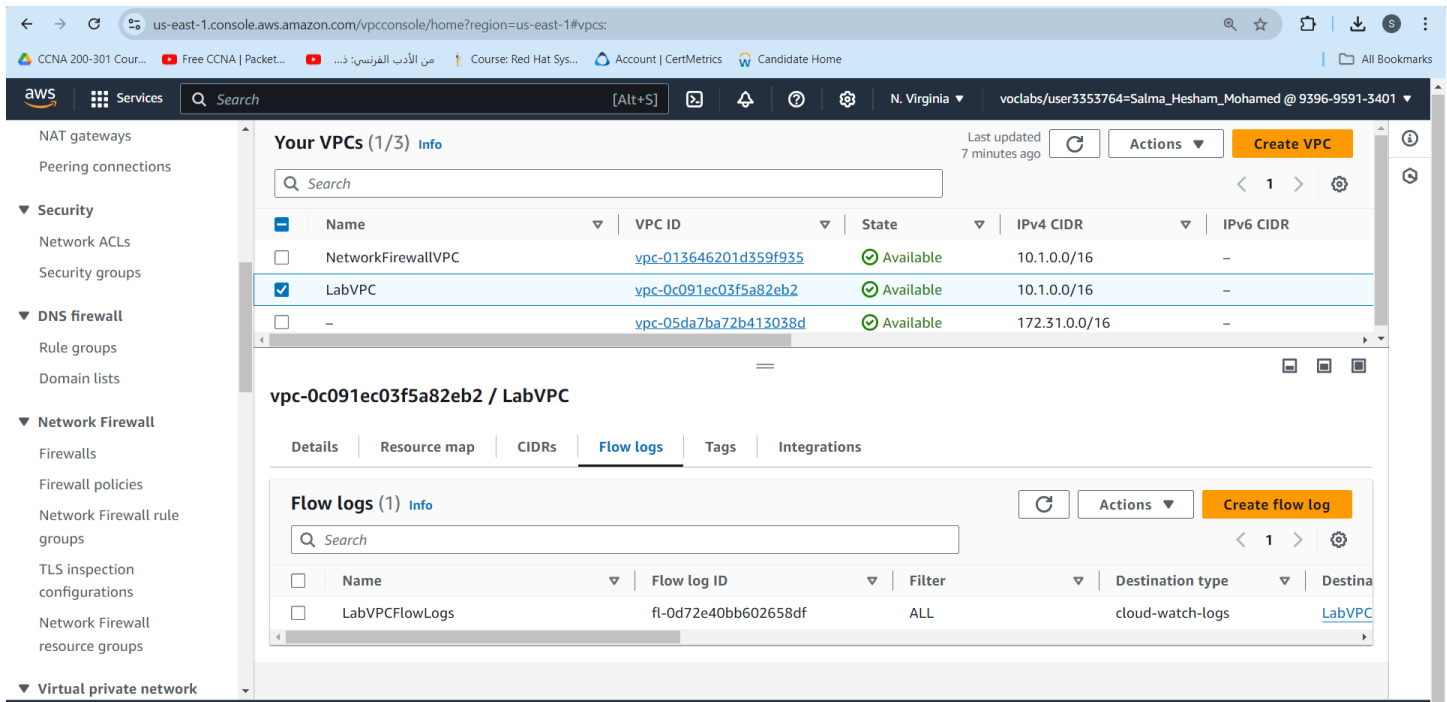
Task 2.2: Create a VPC Flow Log

- **Description:** Creating a VPC Flow Log to monitor traffic entering or exiting the VPC.

- **Steps:**

1. Created a VPC Flow Log from the AWS Management Console.
2. Sent the logs to either S3 or CloudWatch for analysis.
3. Verified the logs are collecting traffic data.

- **Tools:** AWS VPC Console, AWS CloudWatch Logs.



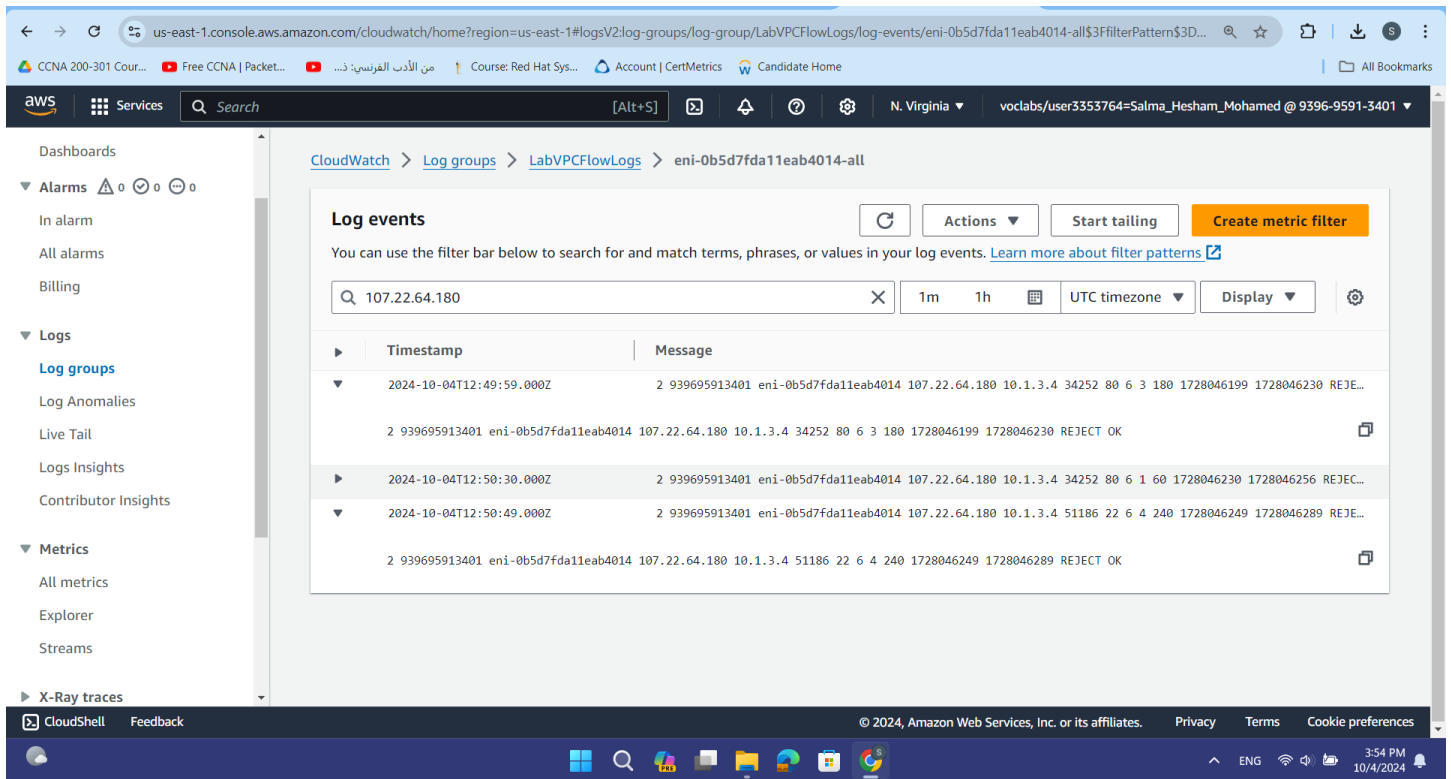
Task 2.3: Access the WebServer Instance from the Internet and Review VPC Flow Logs in CloudWatch

- **Description:** Accessing the web server and reviewing traffic logs in CloudWatch.

- **Steps:**

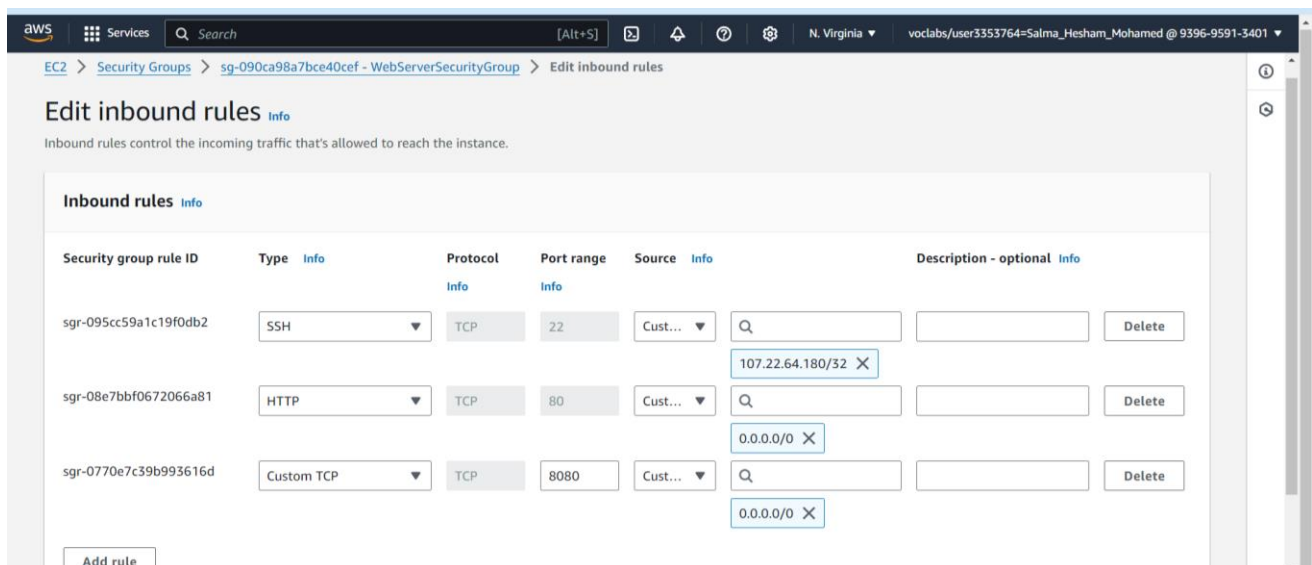
1. Accessed the WebServer instance using its public IP address.
2. Monitored the traffic using the VPC Flow Logs stored in CloudWatch.
3. Analyzed the log entries for potential anomalies.

- **Tools:** AWS EC2, AWS CloudWatch Logs, VPC Flow Logs.

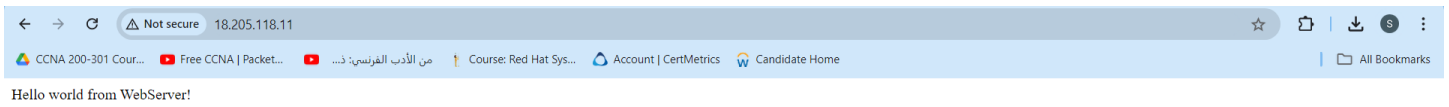


Task 2.4: Configure Route Table and Security Group Settings

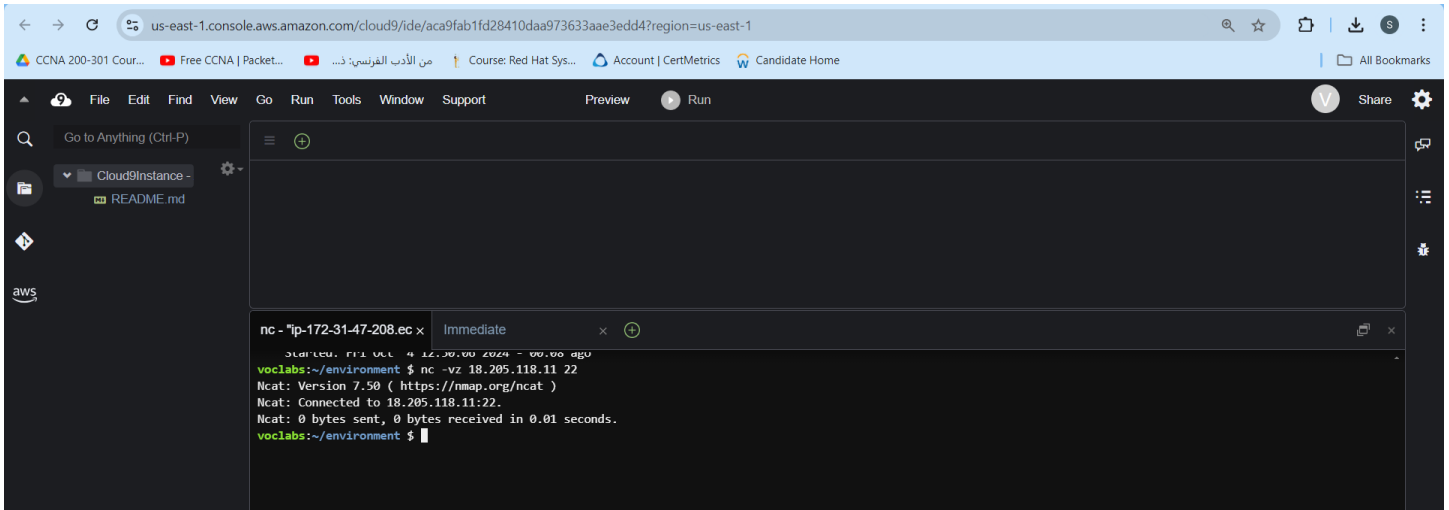
- **Description:** Ensuring correct route table and security group settings for secure communication.
- **Steps:**
 1. Configured the route table for proper routing of traffic.
 2. Applied security group rules to control inbound and outbound traffic.
 3. Tested connectivity to ensure the rules were properly applied.
- **Tools:** AWS VPC Console, AWS EC2 Console.



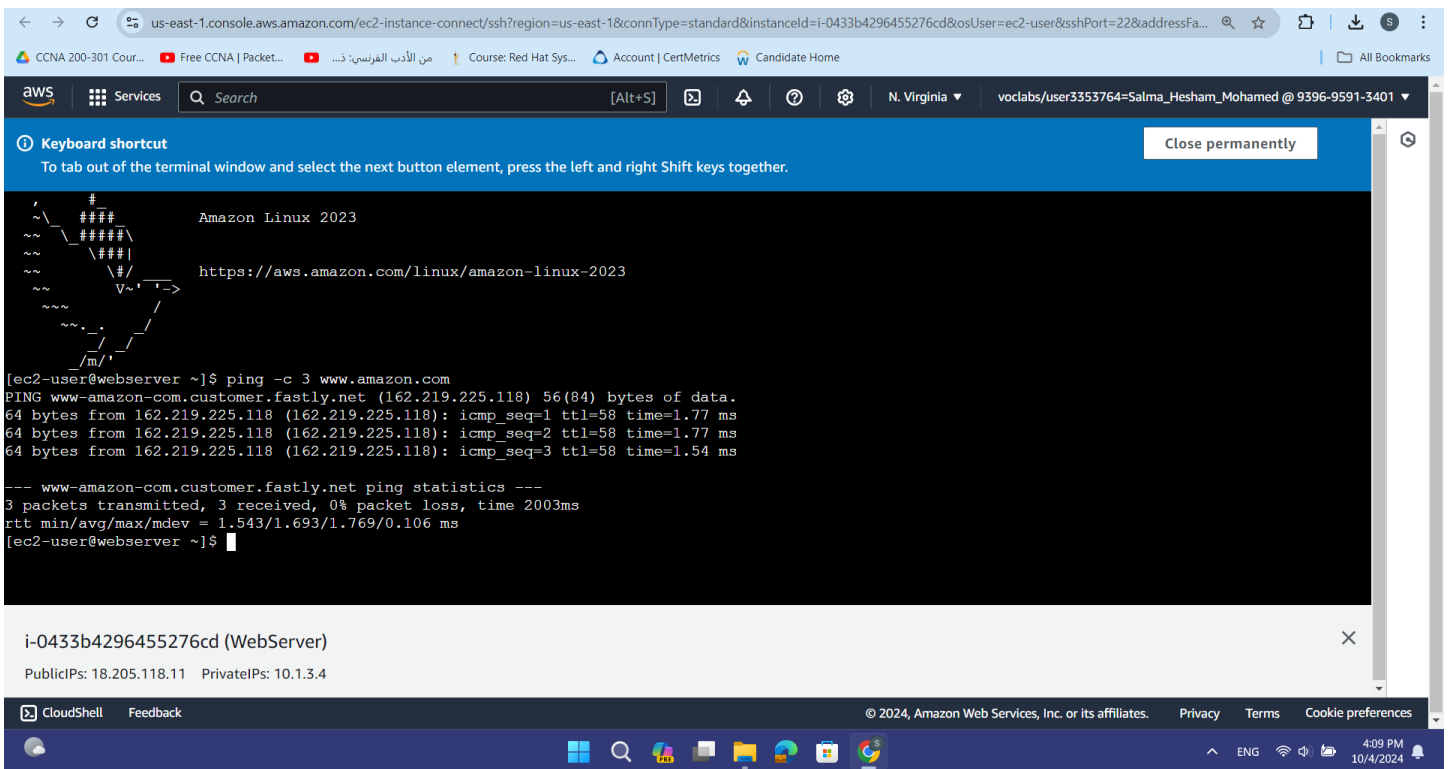
The WebServer instance accessed from port 80



The WebServer instance accessed from port 22



The WebServer instance accessed from port 8080



The Log events from CloudWatch

us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#logsV2:log-groups/log-group/LabVPCFlowLogs/log-events/eni-0b5d7fda11eab4014-all\$3FilterPattern\$3D...

CCNA 200-301 Cour... Free CCNA | Packet... من الأدب الفرنسي: ذ... Course: Red Hat Sys... Account | CertMetrics Candidate Home All Bookmarks

aws Services Search [Alt+S] N. Virginia voclabs/user3353764=Salma_Hesham_Mohamed @ 9396-9591-3401

Dashboards

Alarms 0 0 0 0

In alarm

All alarms

Billing

Logs

Log groups

Log Anomalies

Live Tail

Logs Insights

Contributor Insights

Metrics

All metrics

Explorer

Streams

X-Ray traces

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

107.22.64.180 1m 1h 5m UTC timezone Display

Timestamp	Message
2024-10-04T13:07:32.000Z	2 939695913401 eni-0b5d7fda11eab4014 107.22.64.180 10.1.3.4 60540 22 6 11 2241 1728047252 1728047280 ...
2 939695913401 eni-0b5d7fda11eab4014 107.22.64.180 10.1.3.4 60540 22 6 11 2241 1728047252 1728047280 ACCEPT OK	
2024-10-04T13:07:32.000Z	2 939695913401 eni-0b5d7fda11eab4014 10.1.3.4 107.22.64.180 22 60540 6 7 1897 1728047252 1728047280 A...
2 939695913401 eni-0b5d7fda11eab4014 10.1.3.4 107.22.64.180 22 60540 6 7 1897 1728047252 1728047280 ACCEPT OK	
2024-10-04T13:08:29.000Z	2 939695913401 eni-0b5d7fda11eab4014 107.22.64.180 10.1.3.4 53616 22 6 14 2453 1728047309 1728047343 ...
2 939695913401 eni-0b5d7fda11eab4014 107.22.64.180 10.1.3.4 53616 22 6 14 2453 1728047309 1728047343 ACCEPT OK	
2024-10-04T13:08:29.000Z	2 939695913401 eni-0b5d7fda11eab4014 10.1.3.4 107.22.64.180 22 53616 6 10 2161 1728047309 1728047343 ...
2 939695913401 eni-0b5d7fda11eab4014 10.1.3.4 107.22.64.180 22 53616 6 10 2161 1728047309 1728047343 ACCEPT OK	

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

us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#logsV2:log-groups/log-group/LabVPCFlowLogs/log-events/eni-0b5d7fda11eab4014-all\$3FilterPattern\$3D...

CCNA 200-301 Cour... Free CCNA | Packet... من الأدب الفرنسي: ذ... Course: Red Hat Sys... Account | CertMetrics Candidate Home All Bookmarks

aws Services Search [Alt+S] N. Virginia voclabs/user3353764=Salma_Hesham_Mohamed @ 9396-9591-3401

Dashboards

Alarms 0 0 0 0

In alarm

All alarms

Billing

Logs

Log groups

Log Anomalies

Live Tail

Logs Insights

Contributor Insights

Metrics

All metrics

Explorer

Streams

X-Ray traces

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

197.160.23.223 1m 1h 15m UTC timezone Display

Timestamp	Message
2024-10-04T13:00:45.000Z	2 939695913401 eni-0b5d7fda11eab4014 197.160.23.223 10.1.3.4 58820 80 6 8 1292 1728046845 1728046862 ...
2 939695913401 eni-0b5d7fda11eab4014 197.160.23.223 10.1.3.4 58820 80 6 8 1292 1728046845 1728046862 ACCEPT OK	
2024-10-04T13:00:45.000Z	2 939695913401 eni-0b5d7fda11eab4014 10.1.3.4 197.160.23.223 80 58820 6 6 1015 1728046845 1728046862 ...
2 939695913401 eni-0b5d7fda11eab4014 10.1.3.4 197.160.23.223 80 58820 6 6 1015 1728046845 1728046862 ACCEPT OK	
2024-10-04T13:00:45.000Z	2 939695913401 eni-0b5d7fda11eab4014 197.160.23.223 10.1.3.4 58821 80 6 4 190 1728046845 1728046862 A...
2 939695913401 eni-0b5d7fda11eab4014 197.160.23.223 10.1.3.4 58821 80 6 4 190 1728046845 1728046862 ACCEPT OK	
2024-10-04T13:00:45.000Z	2 939695913401 eni-0b5d7fda11eab4014 10.1.3.4 197.160.23.223 80 58821 6 2 92 1728046845 1728046862 AC...
2 939695913401 eni-0b5d7fda11eab4014 10.1.3.4 197.160.23.223 80 58821 6 2 92 1728046845 1728046862 ACCEPT OK	

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

4:13 PM 10/4/2024

Task 2.5: Secure the WebServerSubnet with a Network ACL

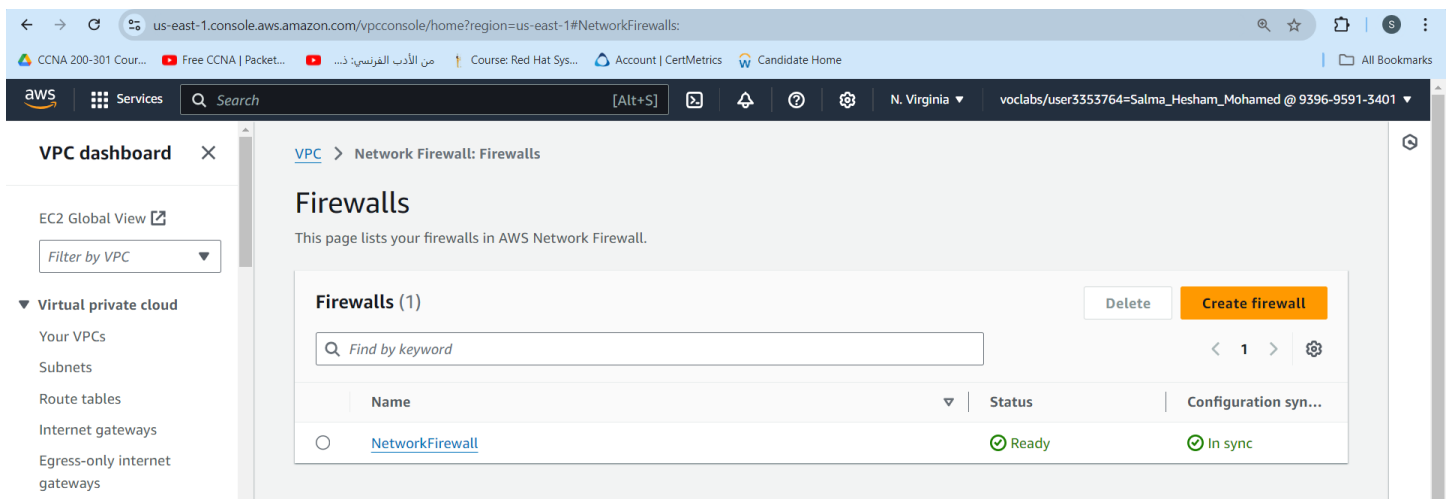
- **Description:** Securing the WebServer subnet using a network ACL to filter traffic.
- **Steps:**
 1. Created a network ACL for the WebServerSubnet.
 2. Applied rules to control inbound and outbound traffic at the subnet level.
 3. Tested traffic flow to ensure the ACL rules were working.
- **Tools:** AWS VPC Console, AWS CLI.

Task 2.6: Review NetworkFirewallVPC and Its Associated Resources

- **Description:** Reviewing the VPC associated with a network firewall and ensuring the necessary resources are in place.
- **Steps:**
 1. Reviewed the configuration of the NetworkFirewallVPC.
 2. Documented the associated subnets, route tables, and firewall rules.
- **Tools:** AWS VPC Console, AWS CLI.

Task 2.7: Create a Network Firewall

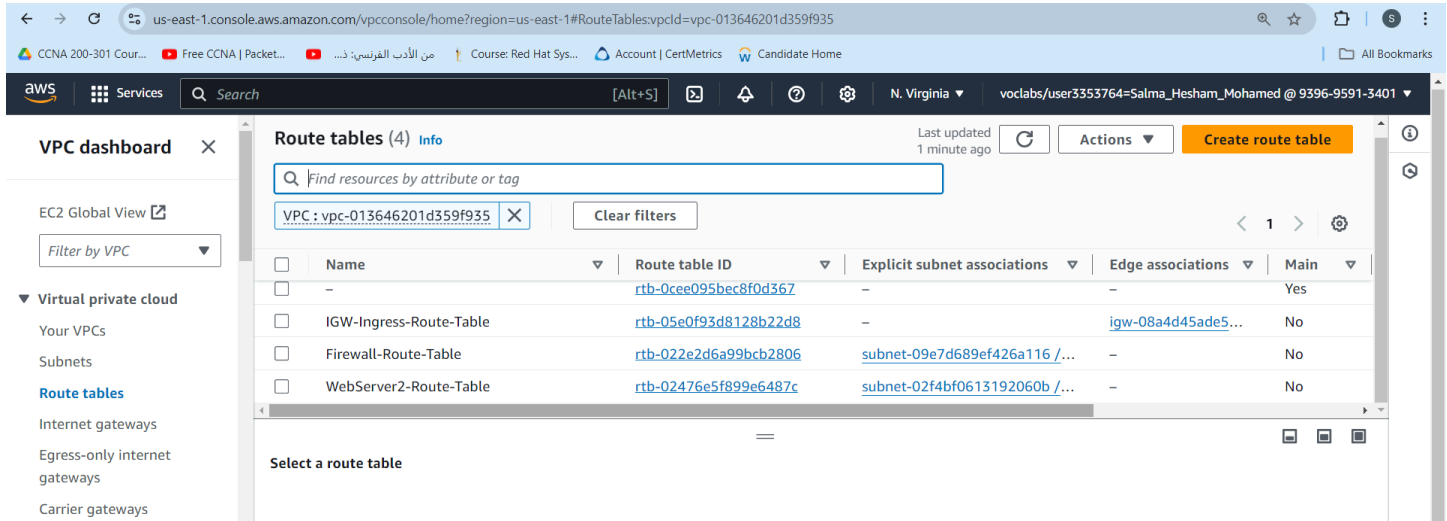
- **Description:** Creating a network firewall for additional protection of the VPC.
- **Steps:**
 1. Configured a network firewall in the VPC.
 2. Defined firewall rules to control traffic.
 3. Applied the firewall to the appropriate subnets and route tables.
- **Tools:** AWS Network Firewall, AWS VPC Console.



Task 2.8: Create Route Tables

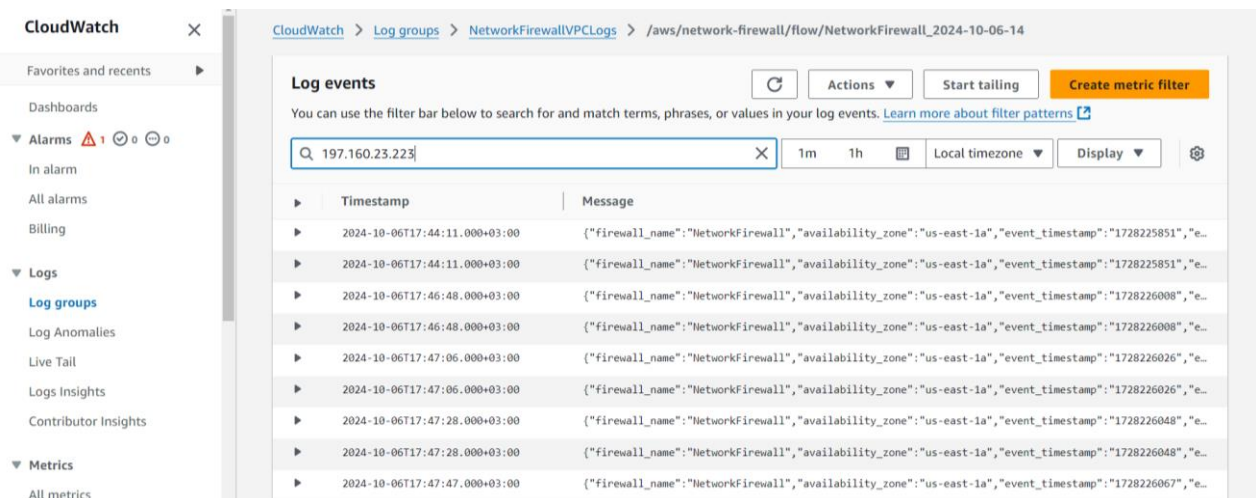
- **Description:** Creating and configuring route tables to ensure proper routing within the VPC.

- **Steps:**
 1. Created a new route table.
 2. Defined routes to control traffic flow between subnets.
 3. Associated the route table with the correct subnets.
- **Tools:** AWS VPC Console, AWS CLI.



Task 2.9: Configure Logging for the Network Firewall

- **Description:** Enabling logging for the network firewall to monitor traffic and rule hits.
- **Steps:**
 1. Enabled firewall logging to CloudWatch.
 2. Monitored logs to review any blocked or allowed traffic.
- **Tools:** AWS Network Firewall, AWS CloudWatch Logs.

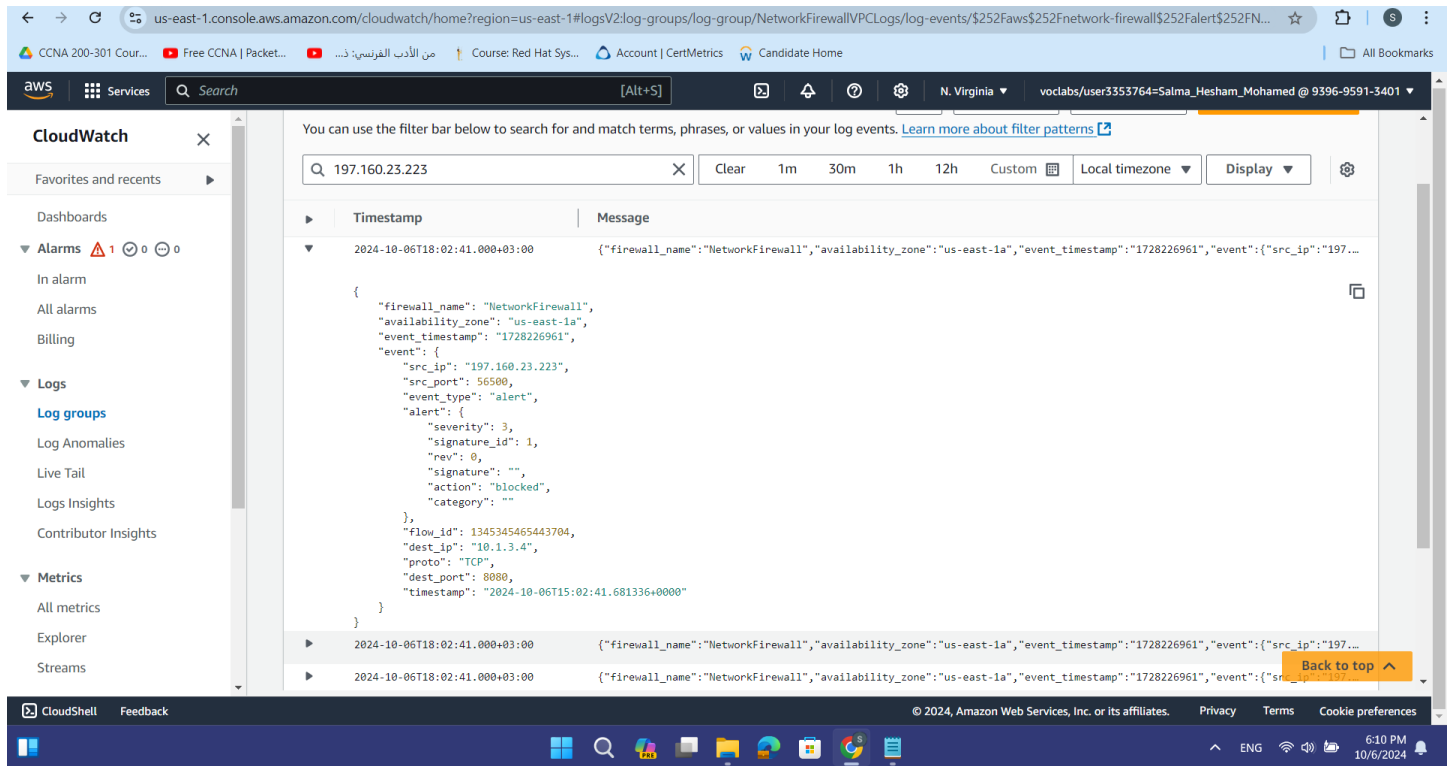


Task 2.10: Configure the Firewall Policy and Test Access

- **Description:** Configuring firewall policies and testing network access.
- **Steps:**

1. Defined firewall policies for specific traffic patterns.
 2. Tested access from external and internal sources to ensure the policy is effective.
- **Tools:** AWS Network Firewall, AWS VPC Console.

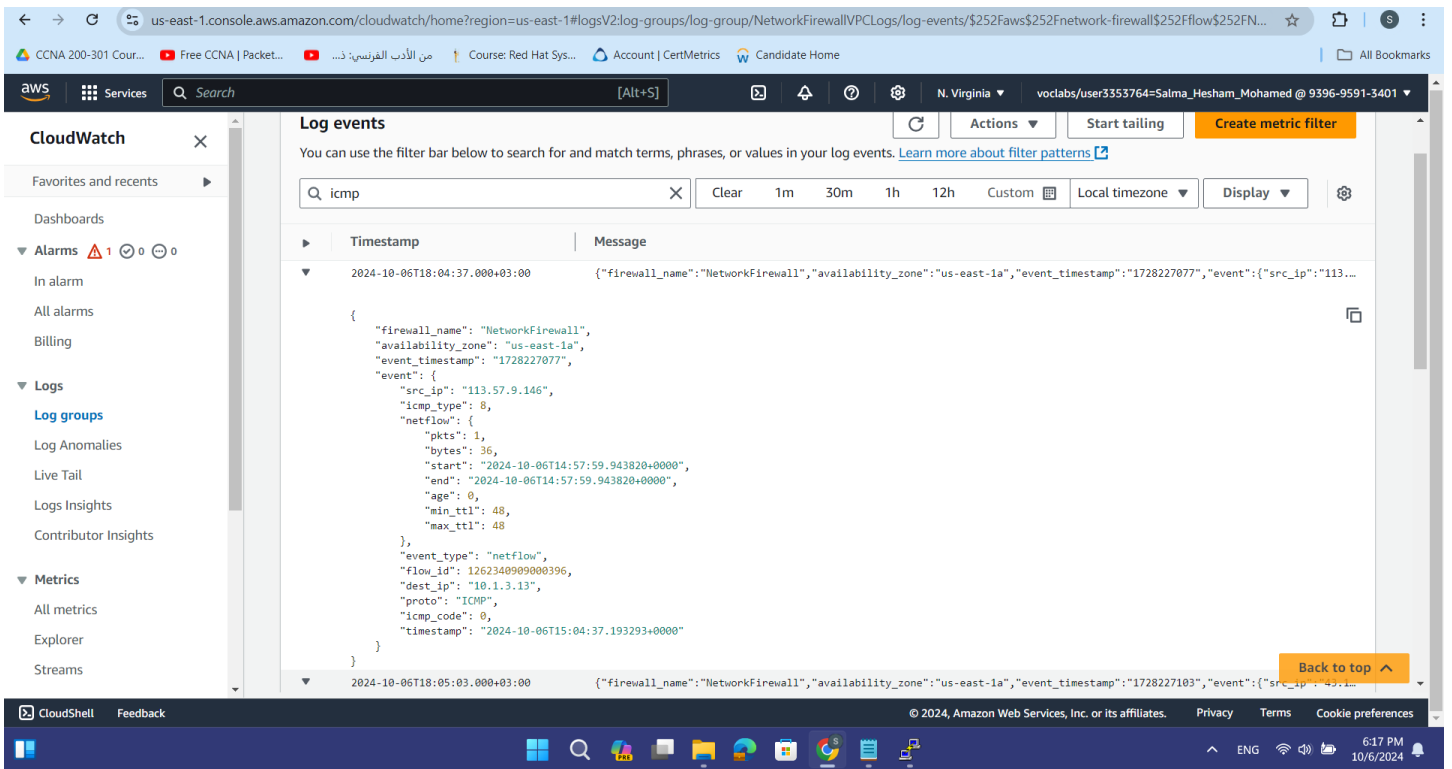
The Firewall policy did not allow access to port 8080



Cost Estimate for Securing VPC with a Network Firewall

- **Description:** Providing an estimate for the costs of securing the VPC using network firewalls, flow logs, and traffic monitoring.

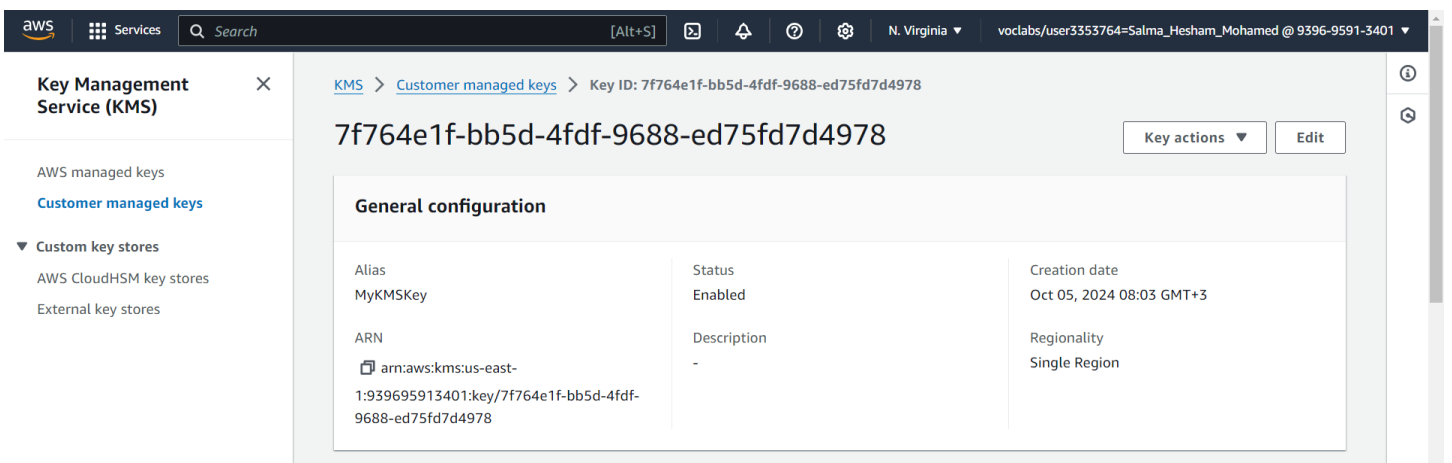
The Firewall policy allow access to ping



Phase 3: Securing AWS Resources Using AWS KMS

Task 3.1: Create a Customer Managed Key and Configure Key Rotation

- **Description:** Creating a KMS key and enabling key rotation.
- **Steps:**
 1. Created a customer managed KMS key.
 2. Configured automatic key rotation.
 3. Verified encryption of a test object using the key.
- **Tools:** AWS KMS, AWS CLI.



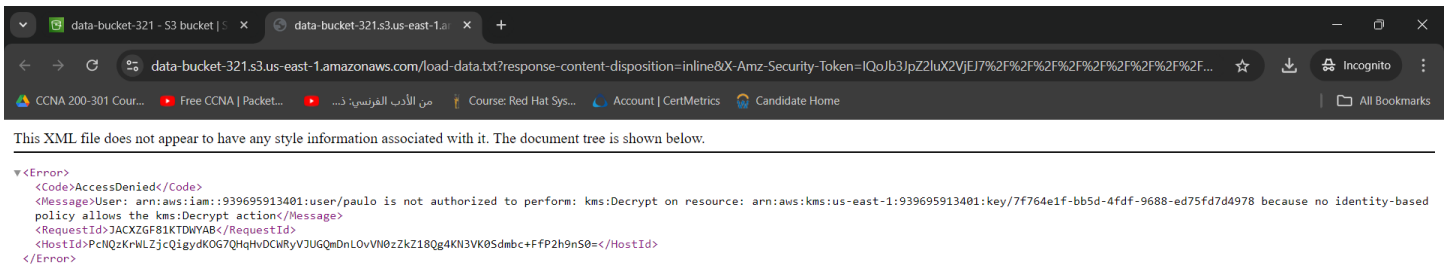
Task 3.2: Update the AWS KMS Key Policy and Analyze an IAM Policy

- **Description:** Updating the KMS key policy and reviewing an IAM policy.

- **Steps:**
 1. Updated the KMS key policy to control access.
 2. Reviewed and analyzed an IAM policy to ensure proper access permissions.
- **Tools:** AWS KMS, IAM, AWS CLI.

Task 3.3: Use AWS KMS to Encrypt Data in Amazon S3

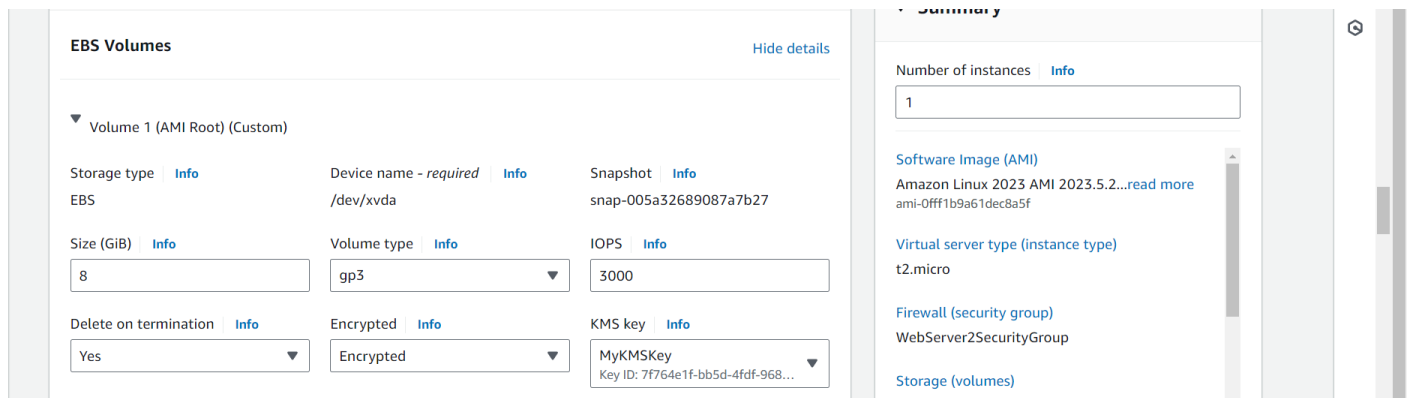
- **Description:** Encrypting objects in S3 using AWS KMS.
- **Steps:**
 1. Configured S3 bucket to use KMS for server-side encryption.
 2. Uploaded objects and verified their encryption status.
- **Tools:** AWS KMS, S3 Console.

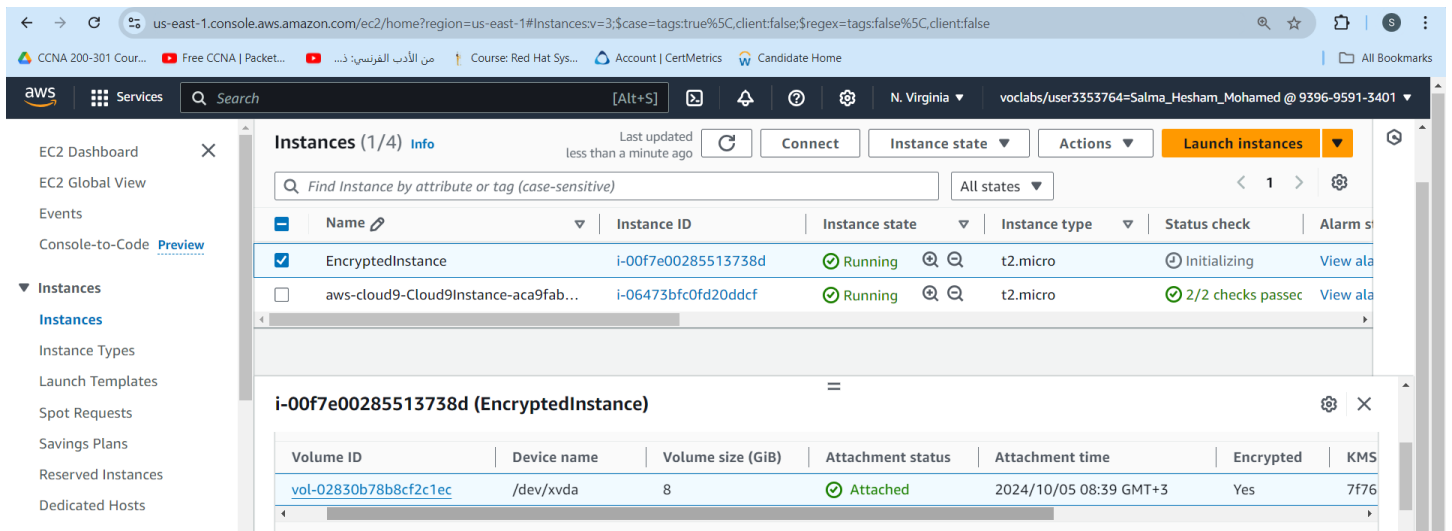


Task 3.4: Use AWS KMS to Encrypt the Root Volume of an EC2 Instance

- **Description:** Encrypting the root volume of an EC2 instance using AWS KMS.
- **Steps:**
 1. Created an encrypted EBS volume using KMS.
 2. Attached it as the root volume to an EC2 instance.
 3. Verified that the volume was encrypted.

Creating Encrypted EBS Volume

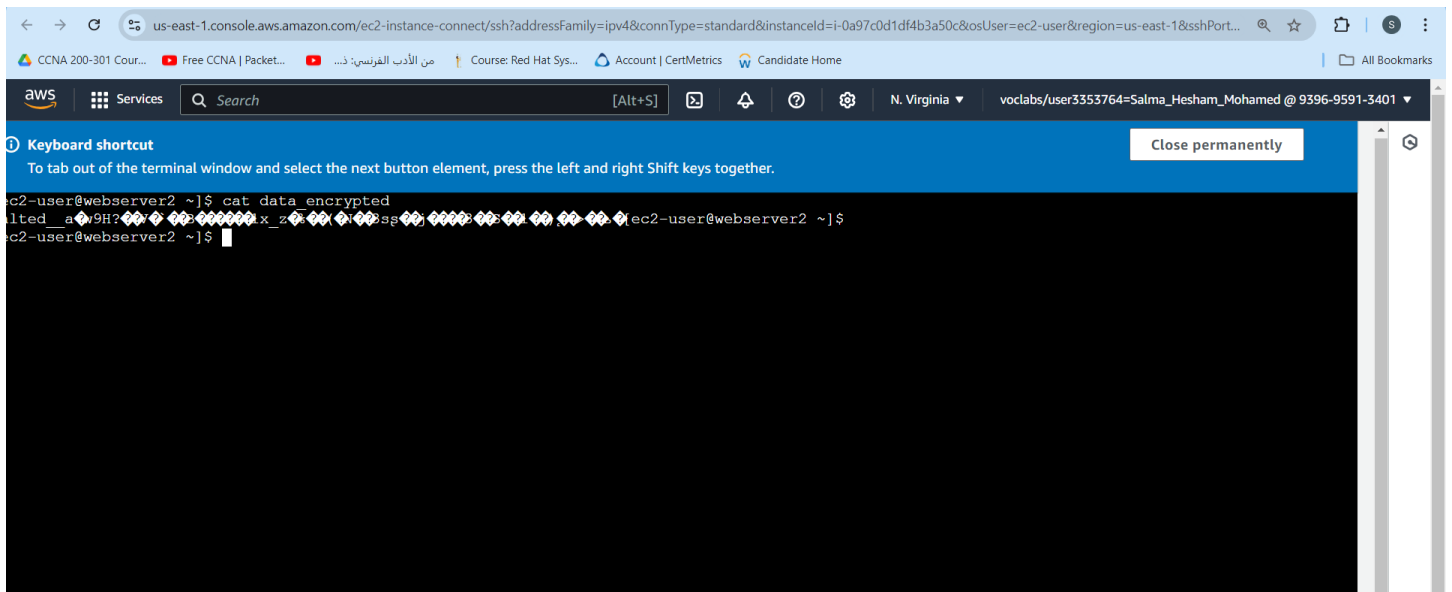




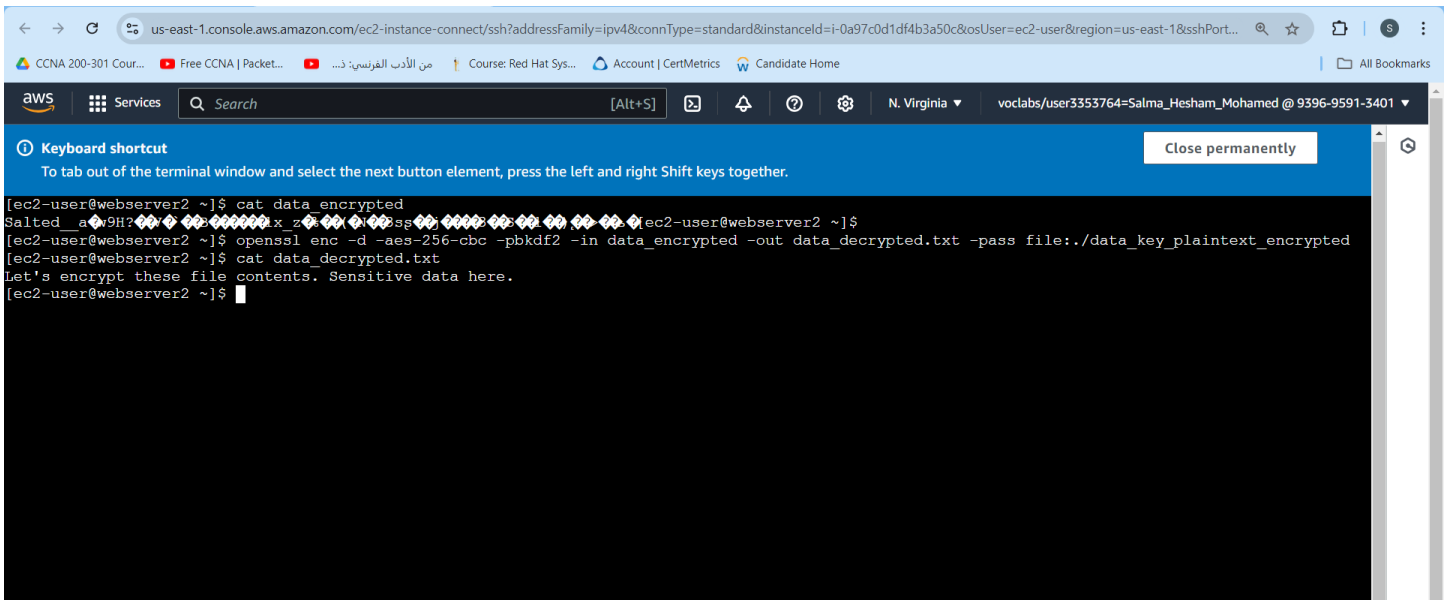
Task 3.5: Use AWS KMS Envelope Encryption to Encrypt Data In Place

- **Description:** Implementing envelope encryption using KMS to encrypt sensitive data.
- **Steps:**
 1. Used AWS KMS to generate a data encryption key (DEK).
 2. Encrypted the DEK using the KMS key.
 3. Encrypted data with the DEK and stored the encrypted DEK alongside it.
- **Tools:** AWS KMS, AWS CLI.

The Encrypted data on the EBS Volume



The File after being decrypted



```
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?addressFamily=ipv4&connType=standard&instanceId=i-0a97c0d1df4b3a50c&osUser=ec2-user&region=us-east-1&sshPort=22

CCNA 200-301 Cour... Free CCNA | Packet... من الأدب الفرنسي: ذو... Course: Red Hat Sys... Account | CertMetrics Candidate Home All Bookmarks

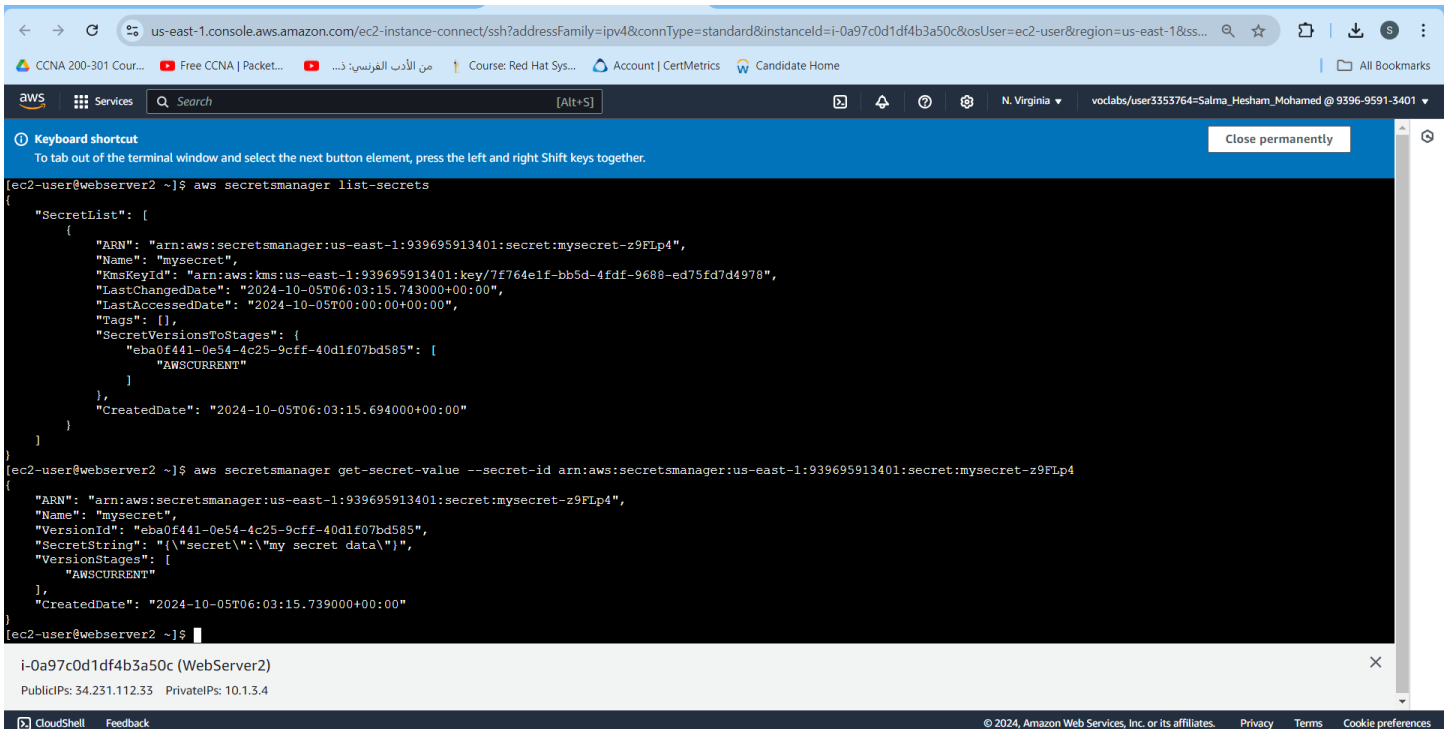
aws Services Search [Alt+S] N. Virginia voclabs/user3353764=Salma_Hesham_Mohamed @ 9396-9591-3401

Keyboard shortcut
To tab out of the terminal window and select the next button element, press the left and right Shift keys together. Close permanently

[ec2-user@webserver2 ~]$ cat data_encrypted
Salted a9H?x zss[ec2-user@webserver2 ~]$
[ec2-user@webserver2 ~]$ openssl enc -d -aes-256-cbc -pbkdf2 -in data_encrypted -out data_decrypted.txt -pass file:./data_key_plaintext_encrypted
[ec2-user@webserver2 ~]$ cat data_decrypted.txt
let's encrypt these file contents. Sensitive data here.
[ec2-user@webserver2 ~]$
```

Task 3.6: Use AWS KMS to Encrypt a Secrets Manager Secret

- **Description:** Encrypting secrets stored in AWS Secrets Manager using KMS.
- **Steps:**
 1. Created a new secret in Secrets Manager.
 2. Configured Secrets Manager to encrypt the secret with a KMS key.
 3. Verified encryption by retrieving the secret securely.
- **Tools:** AWS KMS, AWS Secrets Manager.



```
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?addressFamily=ipv4&connType=standard&instanceId=i-0a97c0d1df4b3a50c&osUser=ec2-user&region=us-east-1&sshPort=22

CCNA 200-301 Cour... Free CCNA | Packet... من الأدب الفرنسي: ذو... Course: Red Hat Sys... Account | CertMetrics Candidate Home All Bookmarks

aws Services Search [Alt+S] N. Virginia voclabs/user3353764=Salma_Hesham_Mohamed @ 9396-9591-3401

Keyboard shortcut
To tab out of the terminal window and select the next button element, press the left and right Shift keys together. Close permanently

[ec2-user@webserver2 ~]$ aws secretsmanager list-secrets
{
  "SecretList": [
    {
      "ARN": "arn:aws:secretsmanager:us-east-1:939695913401:secret:mysecret-z9FLp4",
      "Name": "mysecret",
      "KmsKeyId": "arn:aws:kms:us-east-1:939695913401:key/7f764e1f-bb5d-4fdf-9688-ed75fd7d4978",
      "LastChangedDate": "2024-10-05T06:03:15.743000+00:00",
      "LastAccessedDate": "2024-10-05T00:00:00+00:00",
      "Tags": [],
      "SecretVersionsToStages": {
        "eba0f441-0e54-4c25-9cff-40d1f07bd585": [
          "AWSCURRENT"
        ]
      },
      "CreateDate": "2024-10-05T06:03:15.694000+00:00"
    }
  ]
}
[ec2-user@webserver2 ~]$ aws secretsmanager get-secret-value --secret-id arn:aws:secretsmanager:us-east-1:939695913401:secret:mysecret-z9FLp4
{
  "ARN": "arn:aws:secretsmanager:us-east-1:939695913401:secret:mysecret-z9FLp4",
  "Name": "mysecret",
  "VersionId": "eba0f441-0e54-4c25-9cff-40d1f07bd585",
  "SecretString": "{\"secret\":\"my secret data\"}",
  "VersionStages": [
    "AWSCURRENT"
  ],
  "CreateDate": "2024-10-05T06:03:15.739000+00:00"
}
[ec2-user@webserver2 ~]$
```

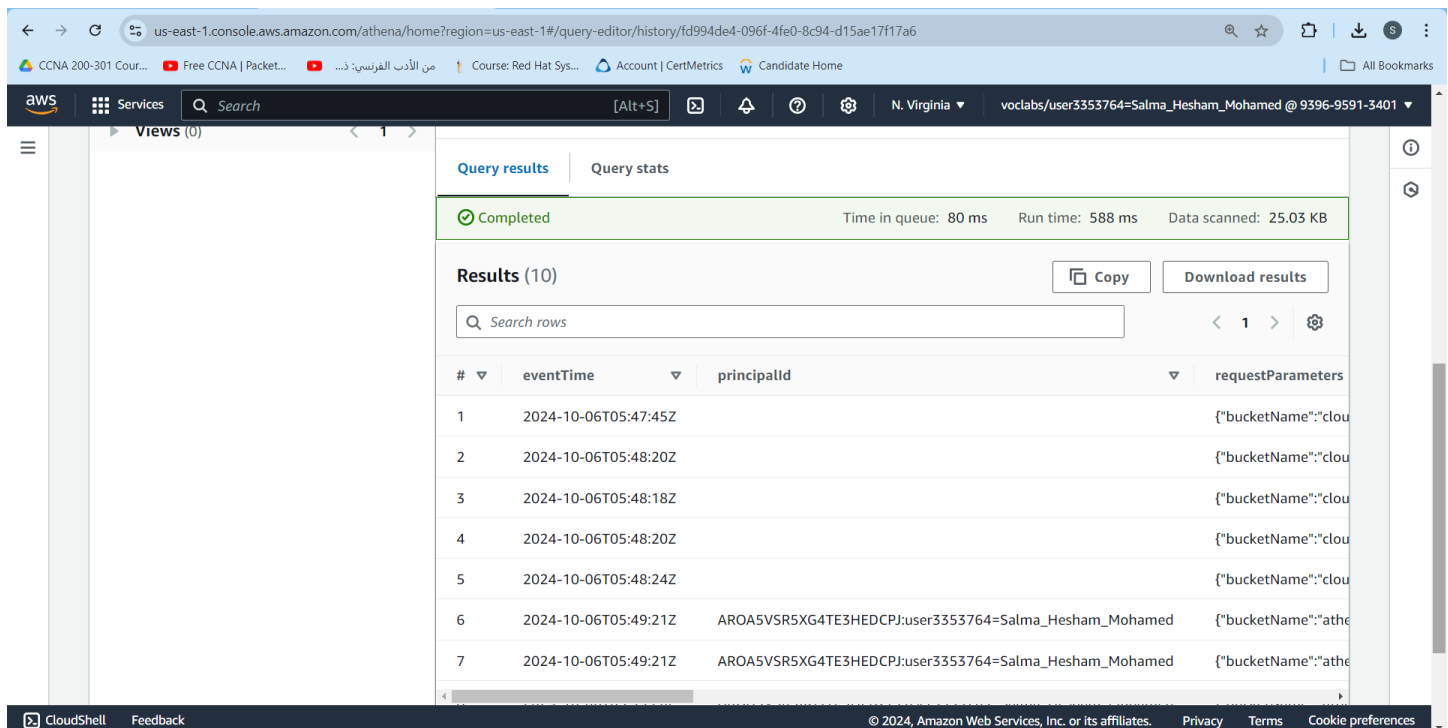

Cost Assessment for Using AWS KMS

- **Description:** Assessing the costs for using AWS KMS, including key management, encryption, and decryption operations.

Phase 4: Monitoring and Logging

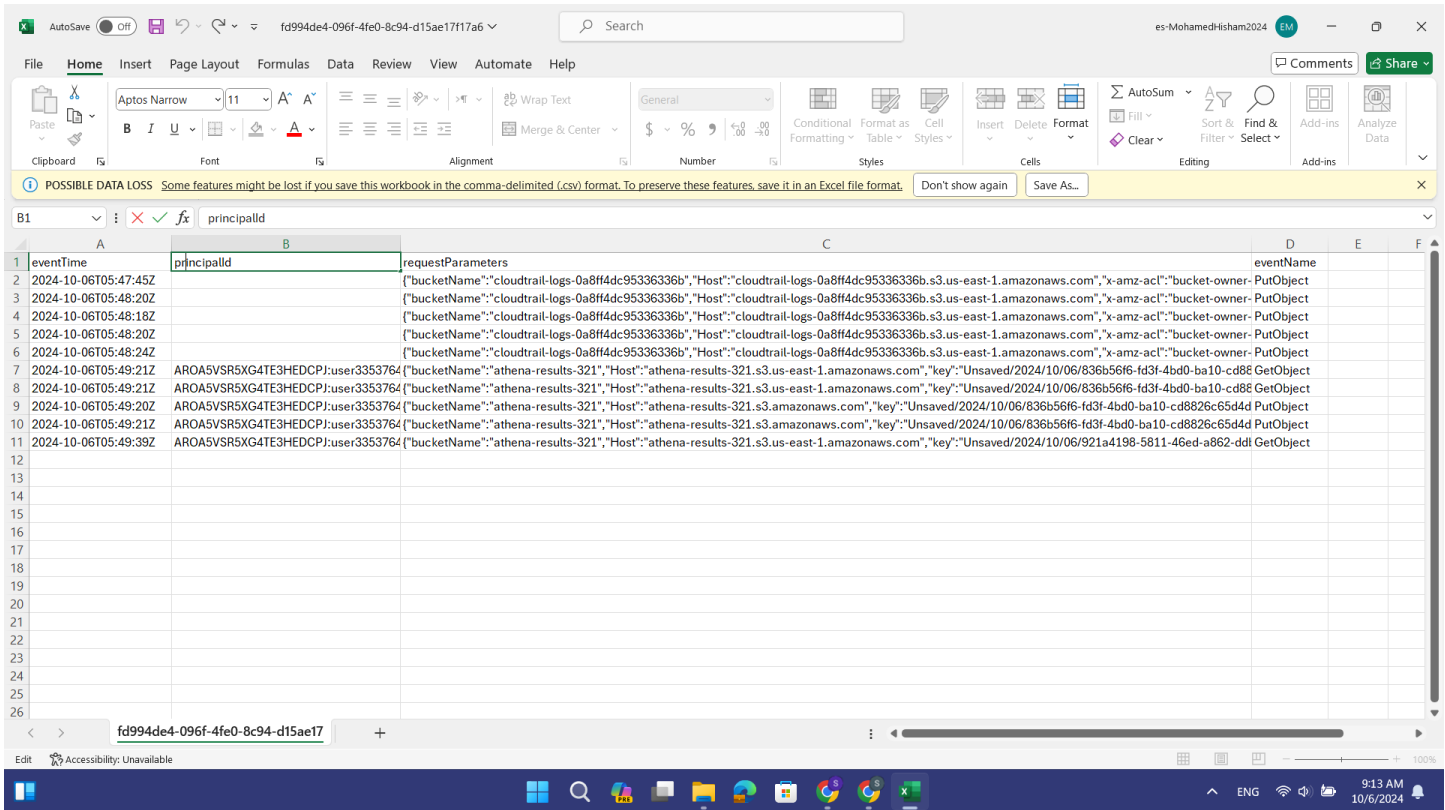
Task 4.1: Use CloudTrail to Record Amazon S3 API Calls

- **Description:** Configuring AWS CloudTrail to monitor and log API activity on S3.
- **Steps:**
 1. Enabled CloudTrail to log S3 API calls.
 2. Configured it to log data events for S3.
 3. Reviewed CloudTrail logs for S3 activity.
- **Tools:** AWS CloudTrail, AWS CloudWatch.



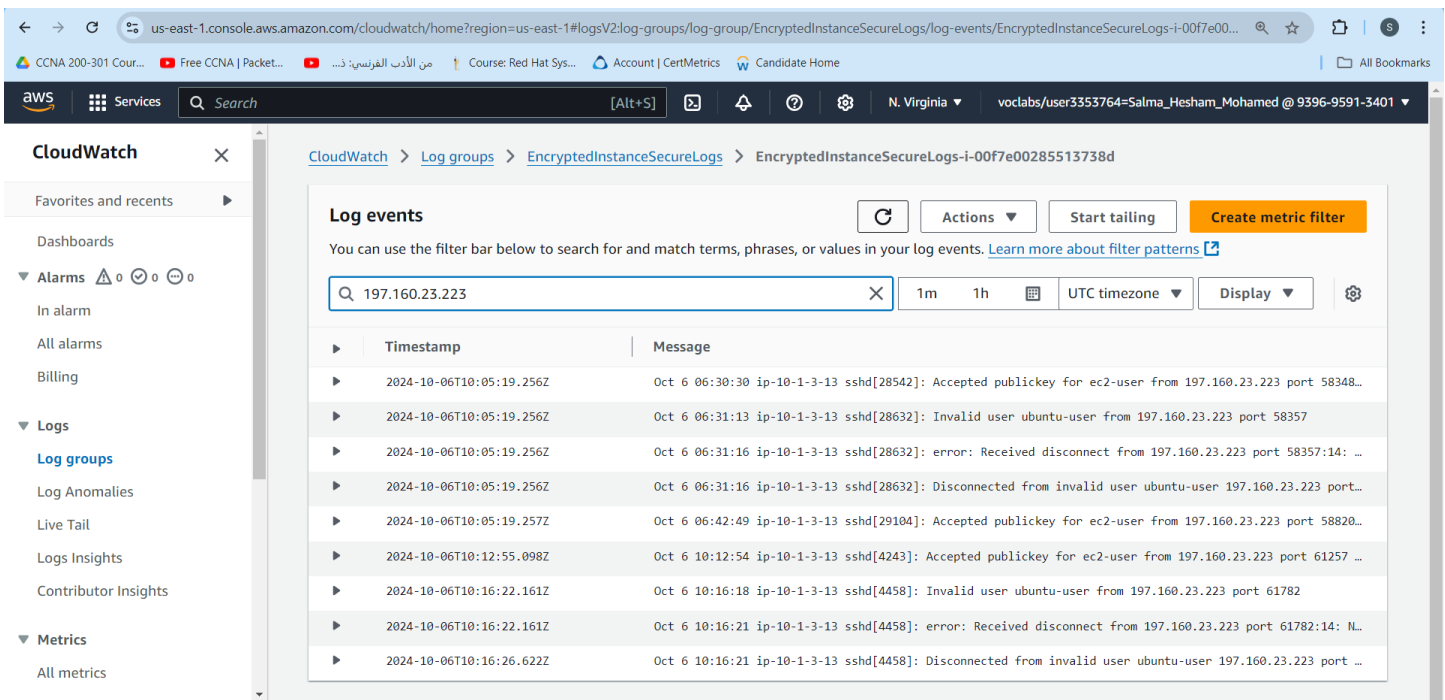
The screenshot displays the AWS Athena console interface. The top navigation bar shows the AWS logo, 'Services', a search bar, and the current region 'N. Virginia'. The main content area is titled 'Query results' and shows a completed query with the following details: 'Time in queue: 80 ms', 'Run time: 588 ms', and 'Data scanned: 25.03 KB'. Below this, the 'Results (10)' section is visible, featuring a search bar and a table of results. The table has four columns: '#', 'eventTime', 'principalId', and 'requestParameters'. The first five rows show generic S3 API calls, while the last two rows show calls from the user 'AROASVSR5XG4TE3HEDCPJ:user3353764=Salma_Hesham_Mohamed'.

#	eventTime	principalId	requestParameters
1	2024-10-06T05:47:45Z		{"bucketName":"cloud"
2	2024-10-06T05:48:20Z		{"bucketName":"cloud"
3	2024-10-06T05:48:18Z		{"bucketName":"cloud"
4	2024-10-06T05:48:20Z		{"bucketName":"cloud"
5	2024-10-06T05:48:24Z		{"bucketName":"cloud"
6	2024-10-06T05:49:21Z	AROASVSR5XG4TE3HEDCPJ:user3353764=Salma_Hesham_Mohamed	{"bucketName":"athena"
7	2024-10-06T05:49:21Z	AROASVSR5XG4TE3HEDCPJ:user3353764=Salma_Hesham_Mohamed	{"bucketName":"athena"



Task 4.2: Use CloudWatch Logs to Monitor Secure Logs

- **Description:** Monitoring logs from different AWS services using CloudWatch Logs.
- **Steps:**
 1. Configured CloudWatch Logs to capture logs from VPC, EC2, and S3.
 2. Reviewed log streams and filtered security-relevant data.
 3. Created a CloudWatch Dashboard to monitor logs in real-time.



- **Tools:** AWS CloudWatch Logs.

Task 4.3: Create a CloudWatch Alarm to Send Notifications for Security Incidents

- **Description:** Setting up CloudWatch alarms to alert on security incidents.
- **Steps:**
 1. Created a CloudWatch alarm based on log metrics (e.g., failed login attempts).
 2. Configured the alarm to send notifications via SNS.
 3. Tested the alarm by triggering a security event.
- **Tools:** AWS CloudWatch, AWS SNS.

The screenshot shows the AWS CloudWatch Alarms console in the us-east-1 region. The left sidebar contains navigation links for CloudWatch, Alarms, Logs, and Metrics. The main panel displays a list of alarms. One alarm is shown in the 'In alarm' state:

Name	State	Last state update (Local)	Conditions
Not valid users exceeding limit on EncryptedInstance	In alarm	2024-10-06 13:35:47	NotValidUsers >= 5 for 1 datapoints within 1 day

The screenshot shows a Gmail inbox with an email from AWS Notifications. The email subject is "ALARM: 'Not valid users exceeding limit on EncryptedInstance' in US East (N. Virginia)". The email body contains the following details:

Alarm Details:

- Name: Not valid users exceeding limit on EncryptedInstance
- Description: Not valid access attempts over SSH to the EncryptedInstance server have exceeded 4 in the last 24 hours.
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [6.0 (05/10/24 10:35:00)] was greater than or equal to the threshold (5.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Sunday 06 October, 2024 10:35:47 UTC
- AWS Account: 839695913401
- Alarm Arn: arn:aws:cloudwatch:us-east-1:839695913401:alarm:Not valid users exceeding limit on EncryptedInstance

Threshold:

- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 5.0 for at least 1 of the last 1 period(s) of 60 seconds.

Task 4.4: Configure AWS Config to Assess Security Settings and Remediate AWS Resources

- **Description:** Using AWS Config to monitor and assess the security configurations of AWS resources.
- **Steps:**
 1. Enabled AWS Config and defined rules to monitor security compliance.
 2. Configured automatic remediation actions for non-compliant resources.
 3. Reviewed the AWS Config dashboard for violations and remediation history.
- **Tools:** AWS Config, AWS CLI.

AWS Config > Rules

Rules

Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the compliance results.

Rules

View details

Edit rule

Actions ▼

Add rule

Any status ▼

< 1 > ⚙

	Name	Remediation action	Type	Compliance
<input type="radio"/>	s3-bucket-logging-enabled	AWS-ConfigureS3BucketLogging	AWS managed	✔ Compliant

Cost Assessment for Monitoring and Logging

- **Description:** Estimating costs for logging and monitoring services, including CloudTrail, CloudWatch, Config, and SNS notifications.

Contact your AWS representative: [Contact Sales](#) Export date: **10/9/2024**Language: **English**

Estimate URL: <https://calculator.aws/#/estimate?id=805942edbce1f6f6e0da22785d8492a8a86773c5>

Estimate summary

Upfront cost

0.00 USD

Monthly cost

0.76 USD

Total 12 months cost


9.12 USD


Includes upfront cost

Detailed Estimate

Name	Group	Region	Upfront cost	Monthly cost
Amazon Simple Storage Service (S3)	No group applied	US East (N. Virginia)	0.00 USD	0.02 USD
Status: -				
Description:				
Config summary: S3 Standard storage (1 GB per month), PUT, COPY, POST, LIST requests to S3 Standard (10), GET, SELECT, and all other requests from S3 Standard (10), Data returned by S3 Select (1 GB per month)				
Amazon Athena	No group applied	US East (N. Virginia)	0.00 USD	0.74 USD
Status: -				
Description: Verifying object-level access logs and querying these logs using Amazon Athena.				
Config summary: Total number of queries (5 per day), Amount of data scanned per query (1 GB)				

Acknowledgement

AWS Pricing Calculator provides only an estimate of your AWS fees and doesn't include any taxes that might apply. Your actual fees depend on a variety of factors, including your actual usage of AWS services. [Learn more](#) 

Contact your AWS representative: [Contact Sales](#) Export date: **10/9/2024**Language: **English**

Estimate URL: [https://calculator.aws/#/estimate?](https://calculator.aws/#/estimate?id=72d94b77b163b6f5b0a715ec445524b568544234)
id=72d94b77b163b6f5b0a715ec445524b568544234

Estimate summary

Upfront cost	Monthly cost	Total 12 months cost
0.00 USD	15.63 USD	187.56 USD
		Includes upfront cost

Detailed Estimate

Name	Group	Region	Upfront cost	Monthly cost
Amazon Virtual Private Cloud (VPC)	No group applied	US East (N. Virginia)	0.00 USD	14.60 USD

Status: -**Description:** Using VPC to isolate the network and secure the infrastructure**Config summary:** Number of In-use public IPv4 addresses (4), Number of Idle public IPv4 addresses (0)


AWS Network Firewall	No group applied	US East (N. Virginia)	0.00 USD	0.73 USD
-----------------------------	------------------	-----------------------	----------	----------


Status: -**Description:** Creating a network firewall for additional protection of the VPC.**Config summary:** Number of AWS Network Firewall endpoints (1), Usage per endpoint (1 hours), Advanced Inspection usage per endpoint (0 hours), Data processed per month (5 GB), Advanced Inspection data processed per month (3 GB)

Amazon CloudWatch	No group applied	US East (N. Virginia)	0.00 USD	0.30 USD
--------------------------	------------------	-----------------------	----------	----------

Status: -**Description:** Accessing the web server and reviewing traffic logs in CloudWatch.**Config summary:** Number of Metrics (includes detailed and custom metrics) (1), GetMetricData: Number of metrics requested (1), GetMetricWidgetImage: Number of metrics requested (1), Number of other API requests (1)

Acknowledgement

AWS Pricing Calculator provides only an estimate of your AWS fees and doesn't include any taxes that might apply. Your actual fees depend on a variety of factors, including your actual usage of AWS services. [Learn more](#) 

Contact your AWS representative: [Contact Sales](#) Export date: **10/9/2024**Language: **English**Estimate URL: **<https://calculator.aws/#/estimate?id=41f232f46031df3f7c8dc0453d34a05beb9c1eab>**

Estimate summary

Upfront cost

0.00 USD

Monthly cost

4.00 USD

Total 12 months cost

48.00 USD


Includes upfront cost


Detailed Estimate

Name	Group	Region	Upfront cost	Monthly cost
AWS Key Management Service	No group applied	US East (N. Virginia)	0.00 USD	4.00 USD

Status: -**Description:** Creating a KMS key for Service Security**Config summary:** Number of customer managed Customer Master Keys (CMK) (4), Number of symmetric requests (1000)

Acknowledgement

AWS Pricing Calculator provides only an estimate of your AWS fees and doesn't include any taxes that might apply. Your actual fees depend on a variety of factors, including your actual usage of AWS services. [Learn more](#) 

Contact your AWS representative: [Contact Sales](#) Export date: **10/9/2024**Language: **English**Estimate URL: <https://calculator.aws/#/estimate?id=91e9f721d1f782f3f556c062fd470819055aea71>

Estimate summary

Upfront cost

0.00 USD

Monthly cost

0.38 USD

Total 12 months cost

4.56 USD

Includes upfront cost

Detailed Estimate

Name	Group	Region	Upfront cost	Monthly cost
AWS CloudTrail	No group applied	US East (N. Virginia)	0.00 USD	0.00 USD

Status: -**Description:** Use CloudTrail to Record Amazon S3 API Calls**Config summary:** Management events units (exact number), Write management trails (1), Read management trails (1), Data events units (millions), S3 trails (1), Lambda trails (1), Insight events units (millions), Trails with Insight events (1), Write management events (5 per month), Read management events (5 per month)

Amazon CloudWatch	No group applied	US East (N. Virginia)	0.00 USD	0.30 USD
--------------------------	------------------	-----------------------	----------	----------

Status: -**Description:** Monitoring logs from different AWS services using CloudWatch Logs**Config summary:** Number of Metrics (includes detailed and custom metrics) (1), GetMetricData: Number of metrics requested (5), GetMetricWidgetImage: Number of metrics requested (5), Number of other API requests (3)

Amazon Simple Notification Service (SNS)

No group applied

US East (N. Virginia)

0.00 USD

0.00 USD

Status: -**Description:**

Config summary: Requests (5 per month), HTTP/HTTPS Notifications (5 per month), EMAIL/EMAIL-JSON Notifications (5 per month), SQS Notifications (5 per month), Amazon Web Services Lambda (0 million per month), Amazon Kinesis Data Firehose (0 million per month)

AWS Config

No group applied

US East (N. Virginia)

0.00 USD

0.08 USD

Status: -

Description: Using AWS Config to monitor and assess the security configurations of AWS resources.

Config summary: Number of Continuous Configuration items recorded (5), Number of Periodic Configuration items recorded (5), Number of Config rule evaluations (3)

Acknowledgement

AWS Pricing Calculator provides only an estimate of your AWS fees and doesn't include any taxes that might apply. Your actual fees depend on a variety of factors, including your actual usage of AWS services. [Learn more](#) 