Project2: Cloud Security Builder

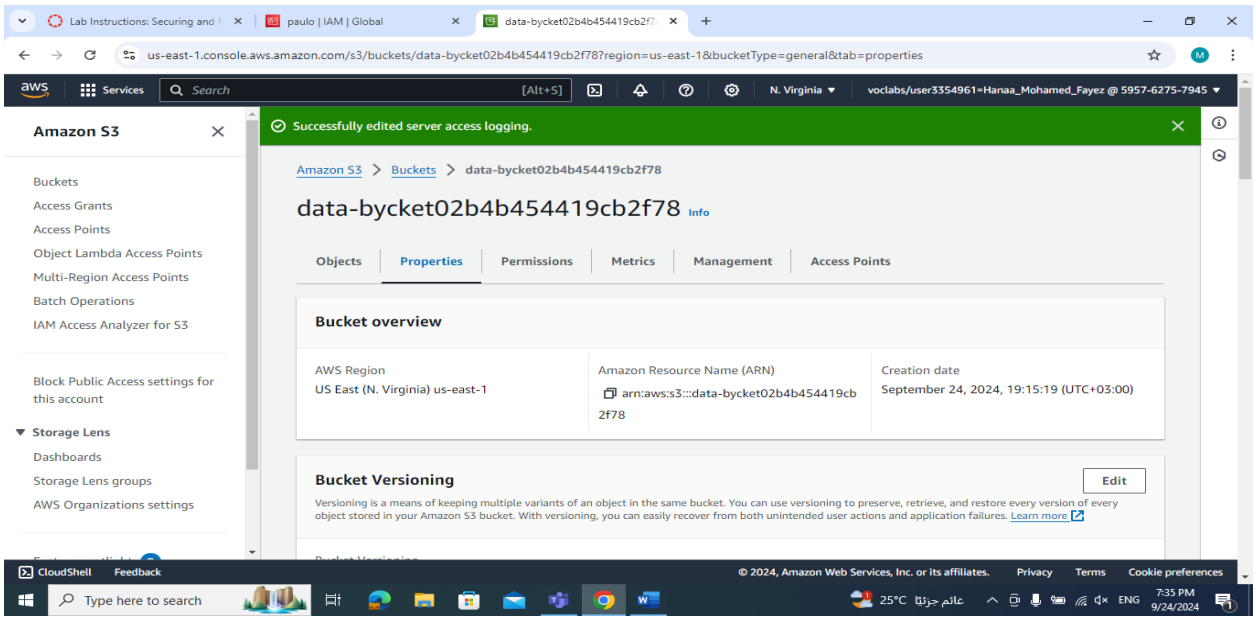
In this project, the challenged is to create resources in AWS and to implement security on them.

- Secure access to objects in an Amazon Simple Storage Service (Amazon S3) bucket.
- Secure network access to virtual network.
- Encrypt data at rest by using AWS Key Management Service (AWS KMS) on an Amazon Elastic Block Store (Amazon EBS) volume.
- Manage encryption keys by using AWS KMS.
- Create a monitoring and incident response system by using Amazon CloudWatch and AWS

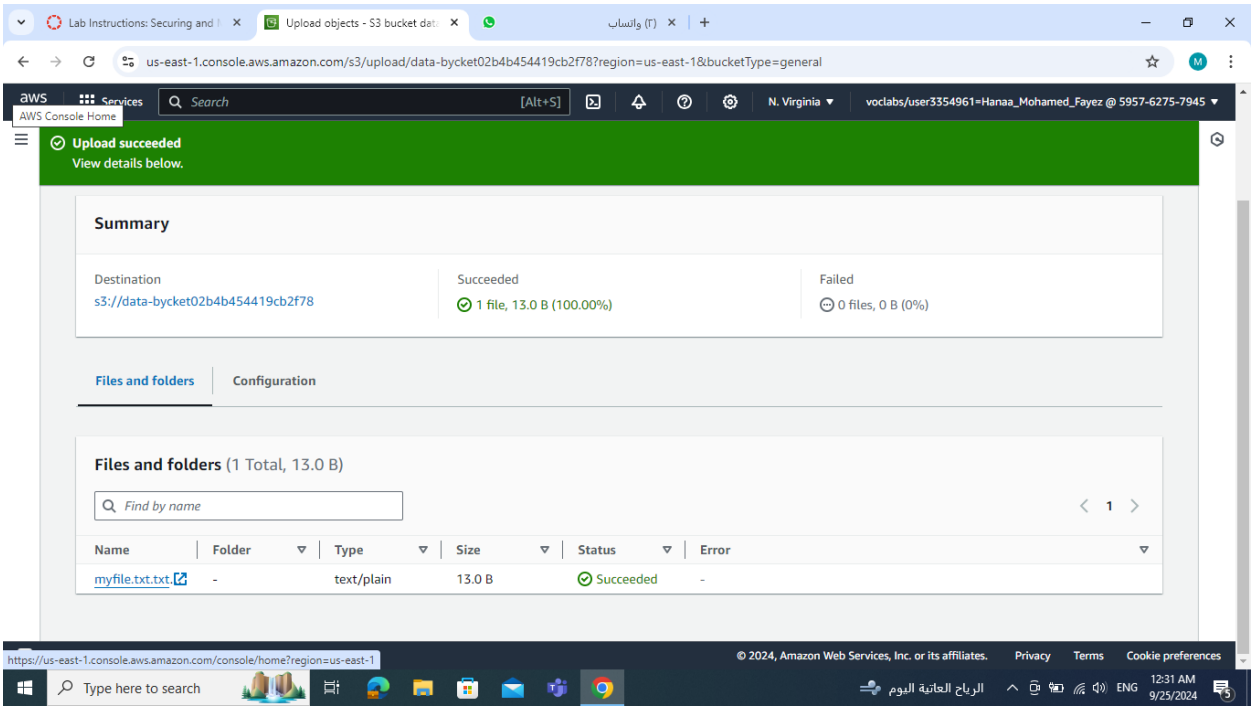
Phase 1: Securing data in Amazon S3

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

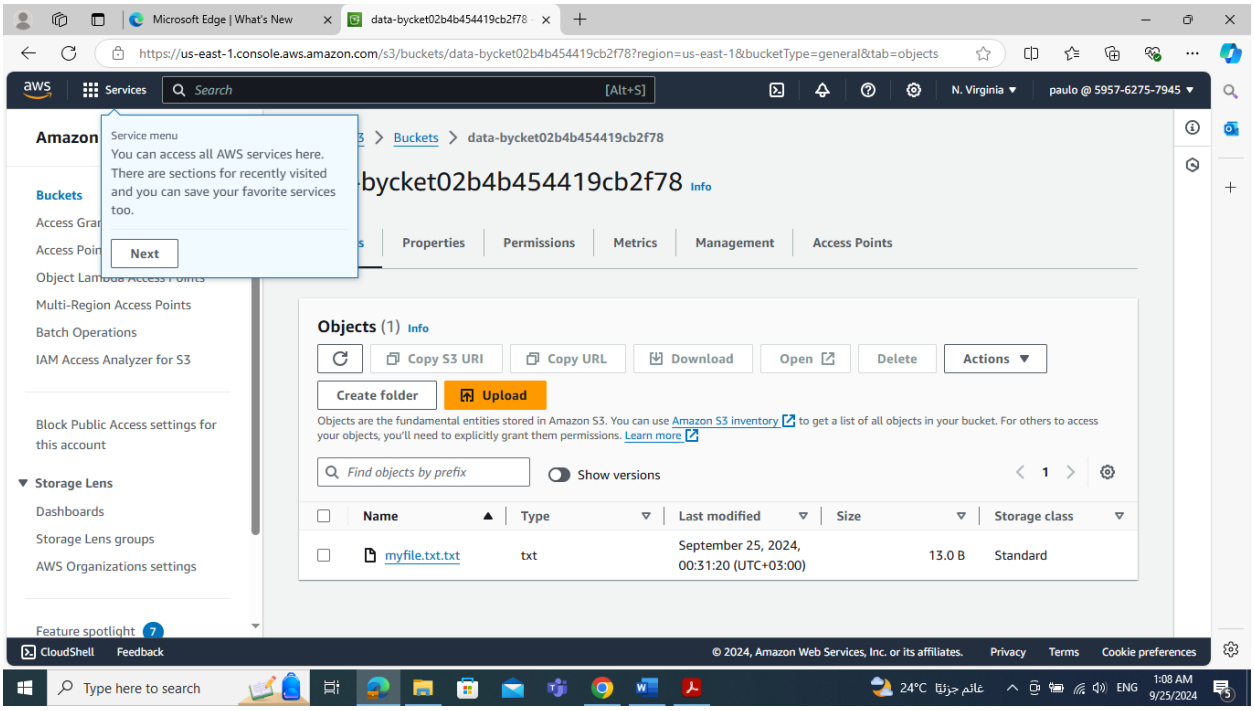
Create a new bucket named **data-bycket02b4b454419cb2f78**

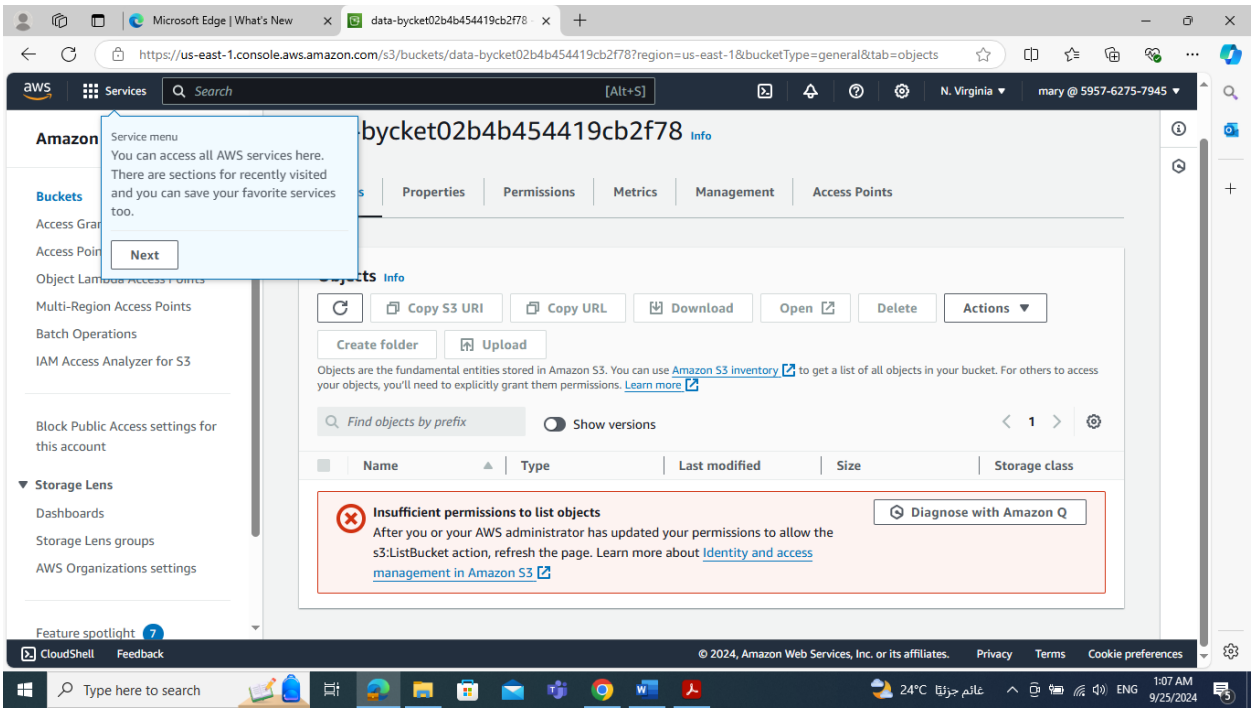


Upload an object to the *data-bucket*



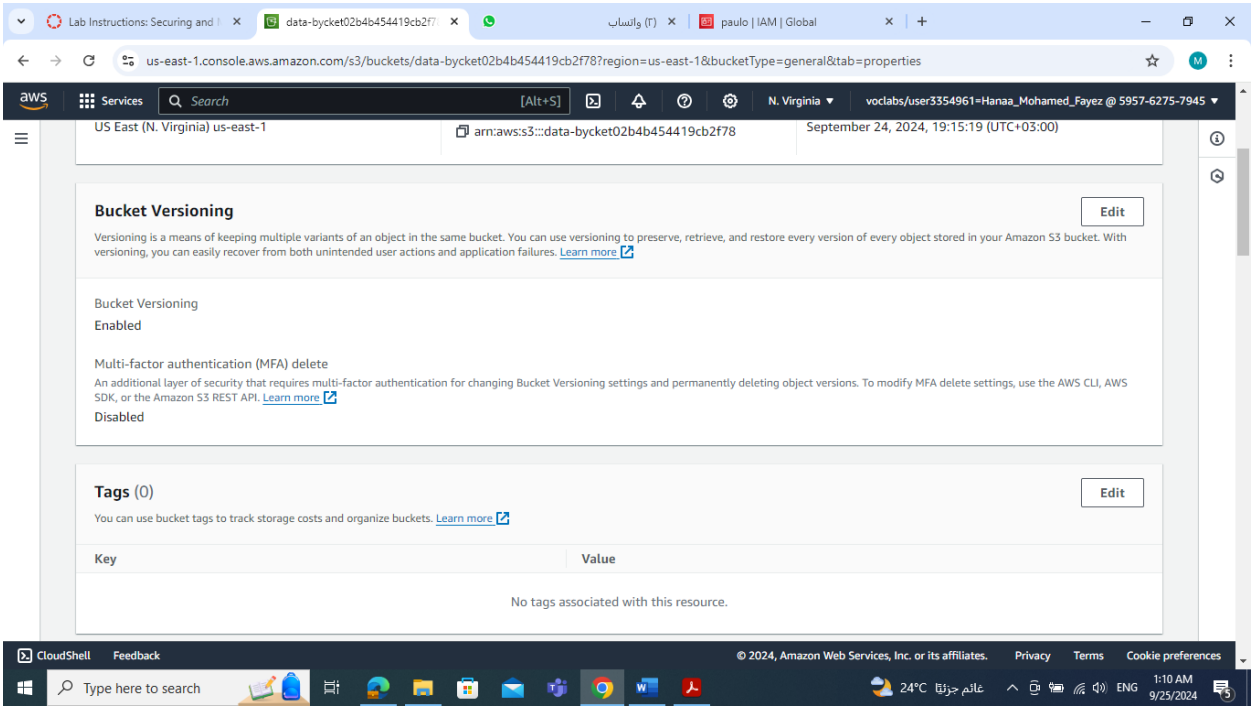
Verify the S3 access level of both the paulo and mary user logins



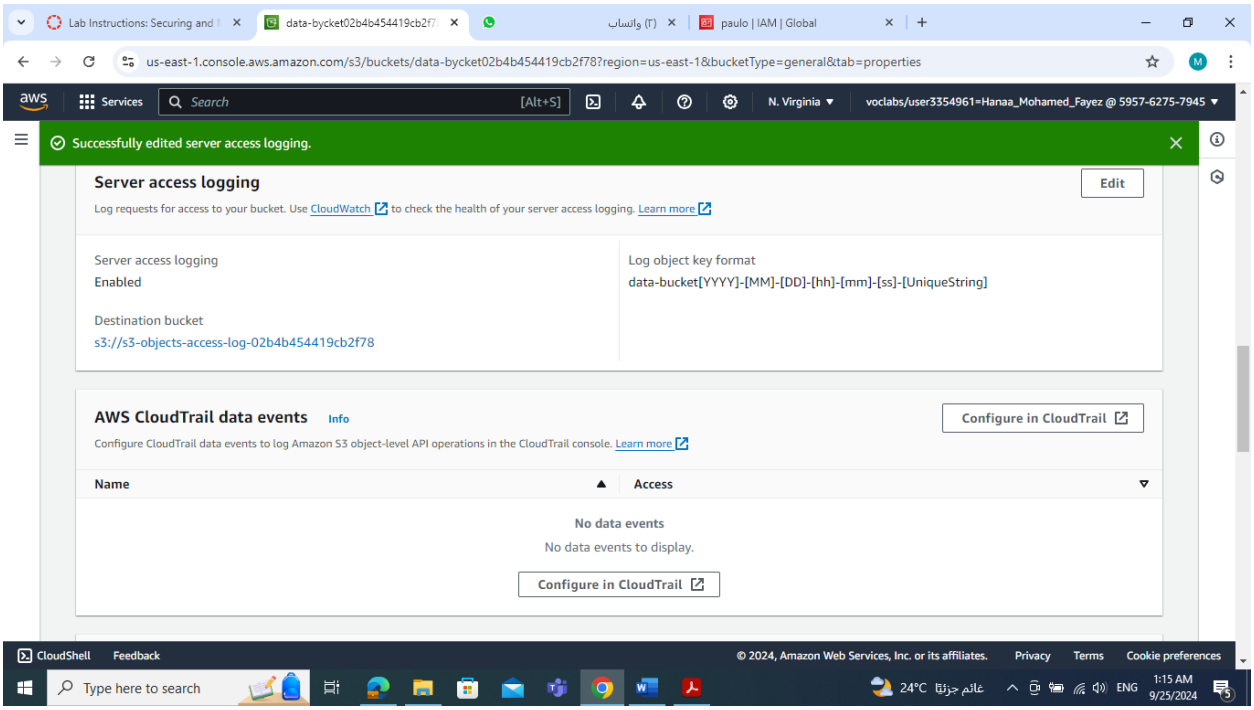


Task 1.2: Enable versioning and object-level logging on a bucket

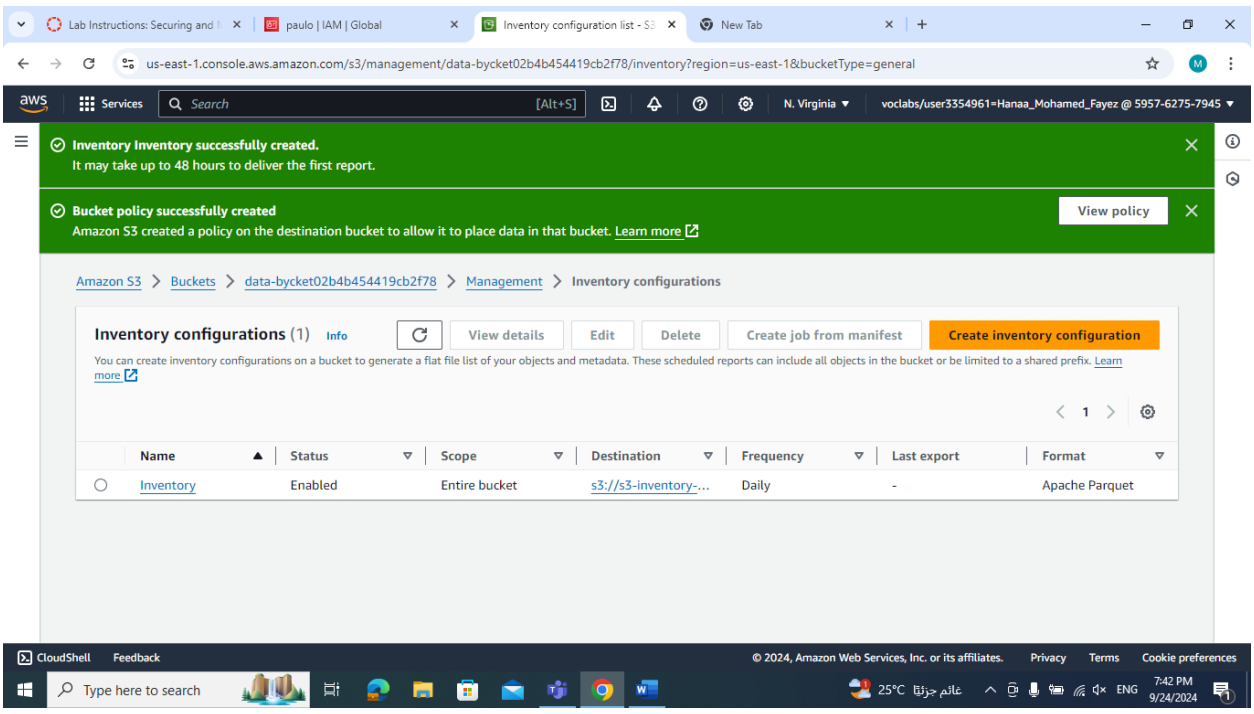
Enable versioning on the *data-bucket*



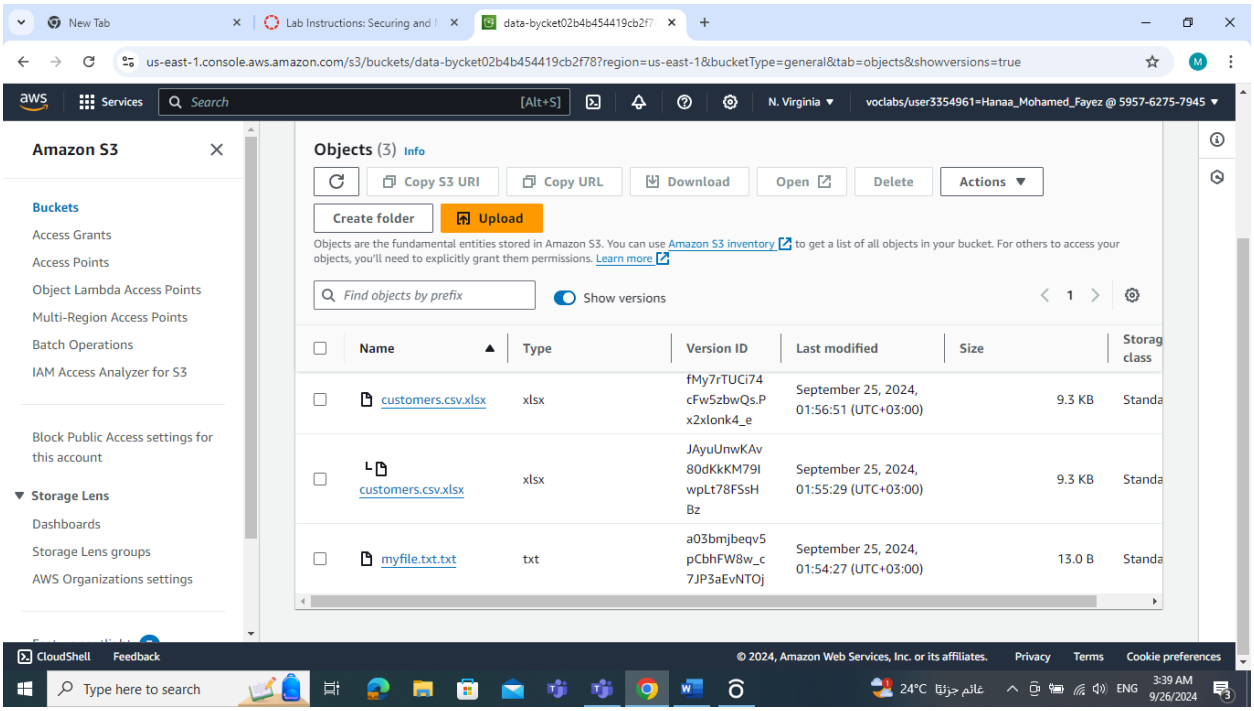
Enable server access logging on the *data-bucket*



Task 1.3: Implement the S3 Inventory feature on a bucket

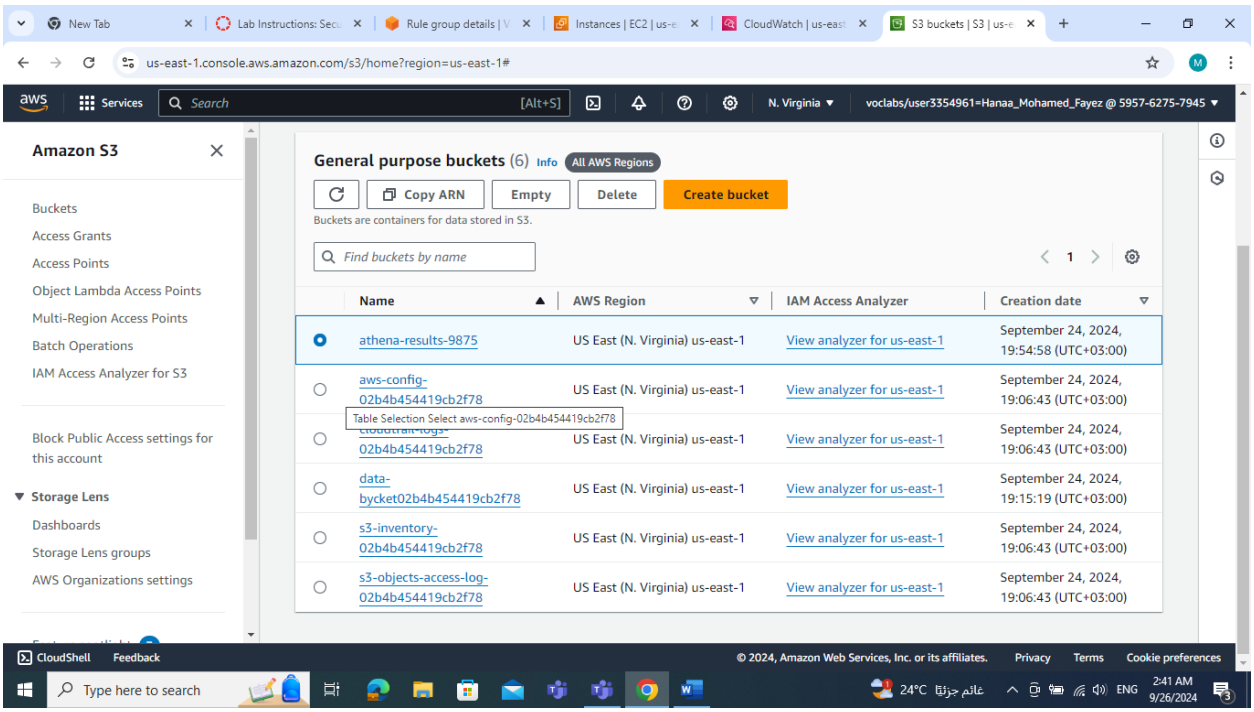


Task 1.4: Confirm that versioning works as intended

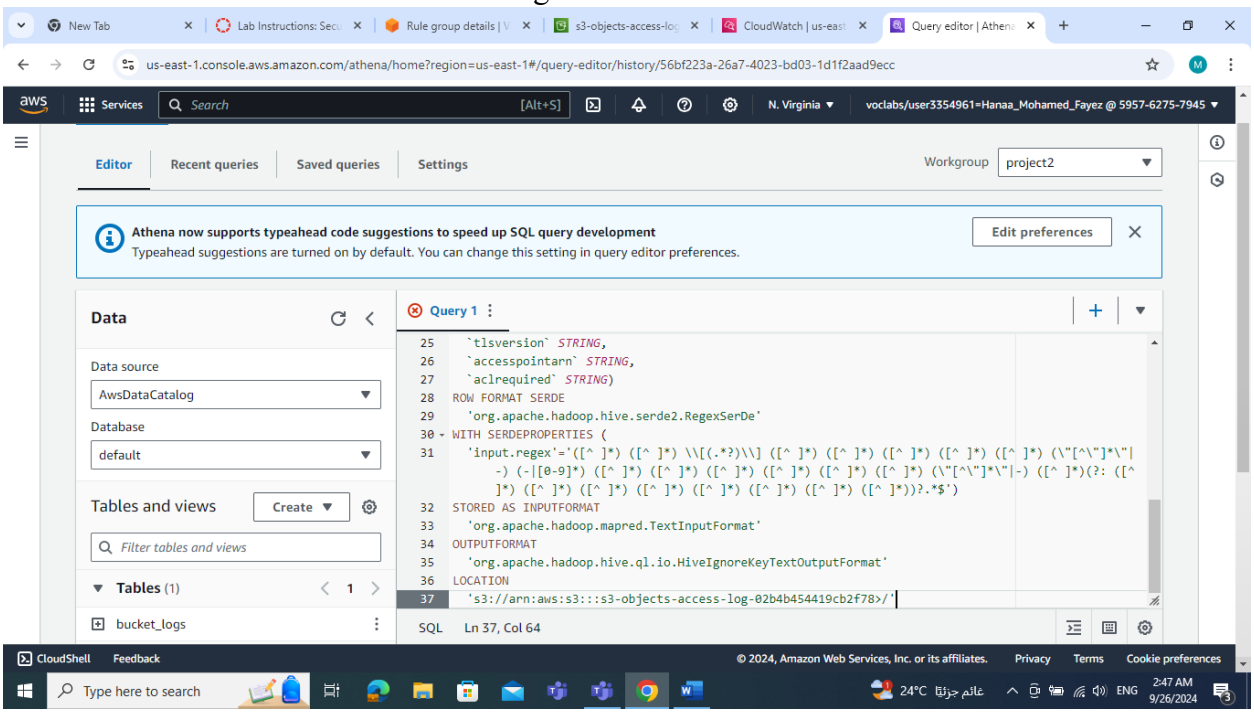


Task 1.5: Confirm object-level logging and query the access logs by using Athena

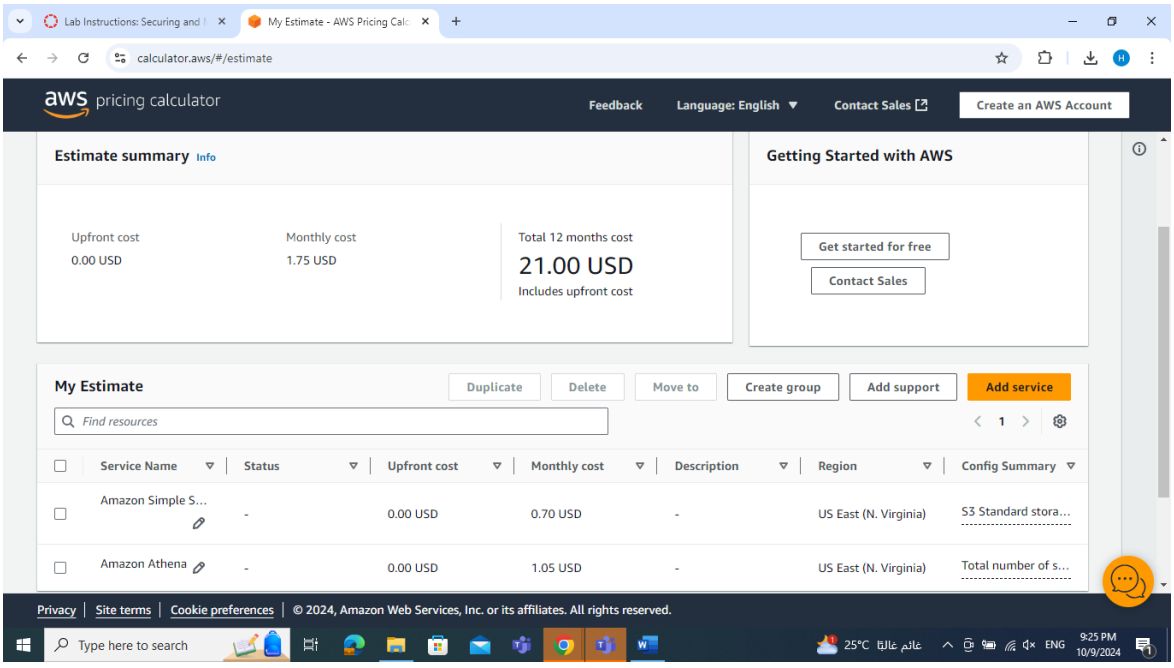
Create an S3 bucket named athena-results-9875

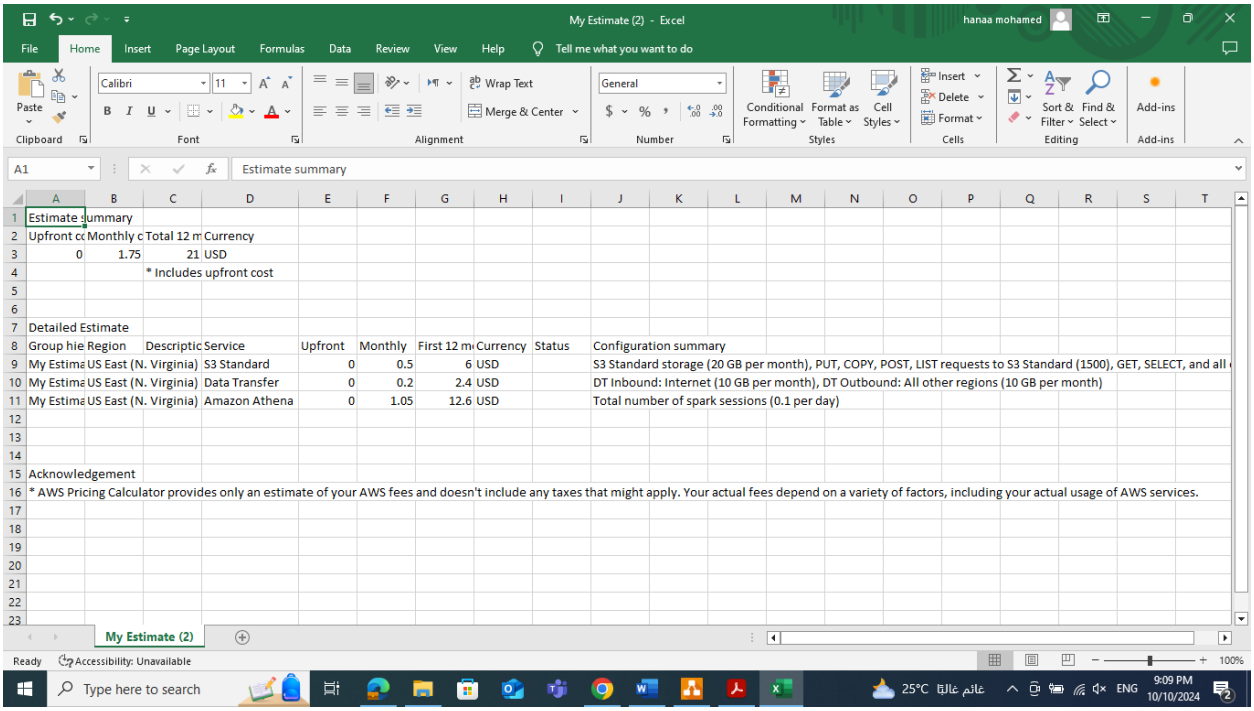


Create an Athena table from the access logs



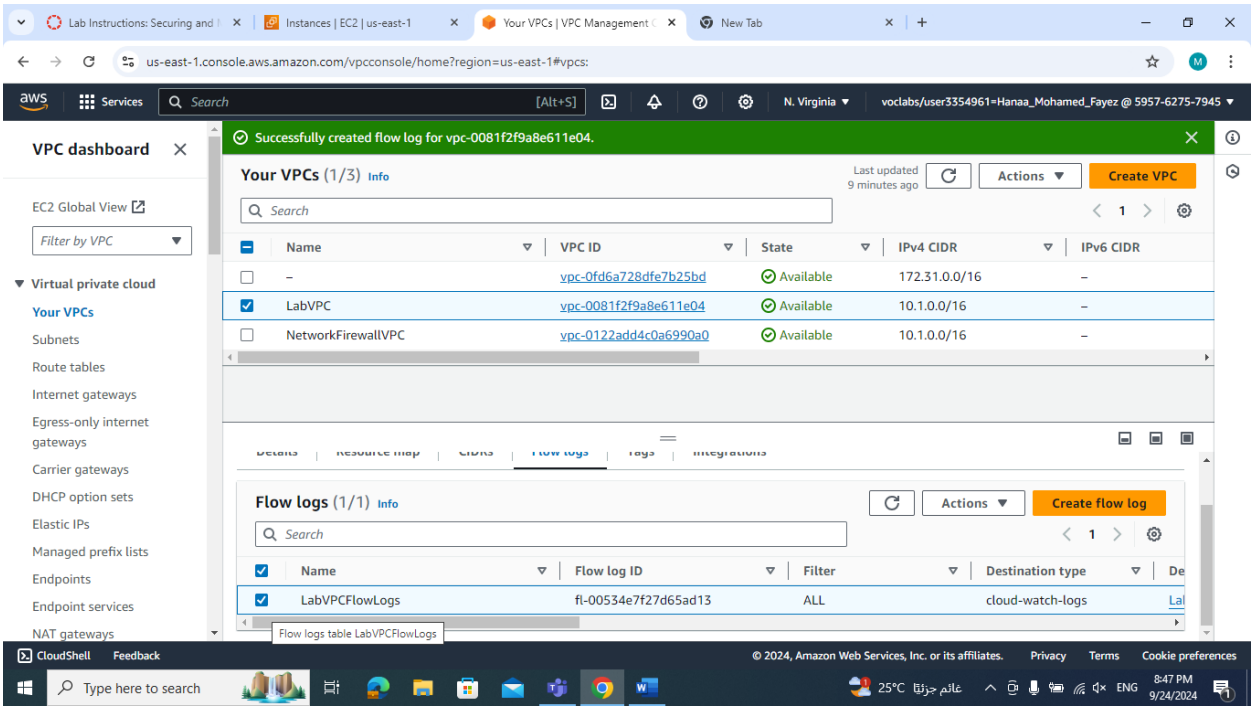
Estimate cost of S3and Athena

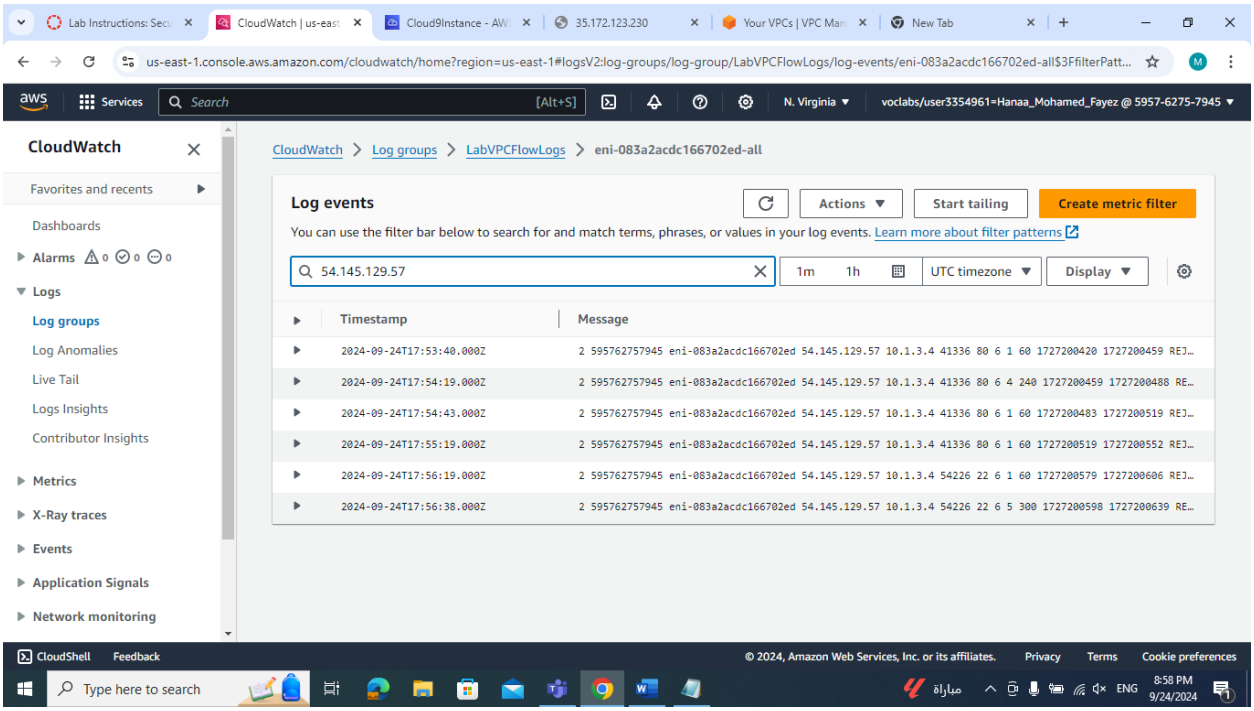




Phase 2: Securing VPCs

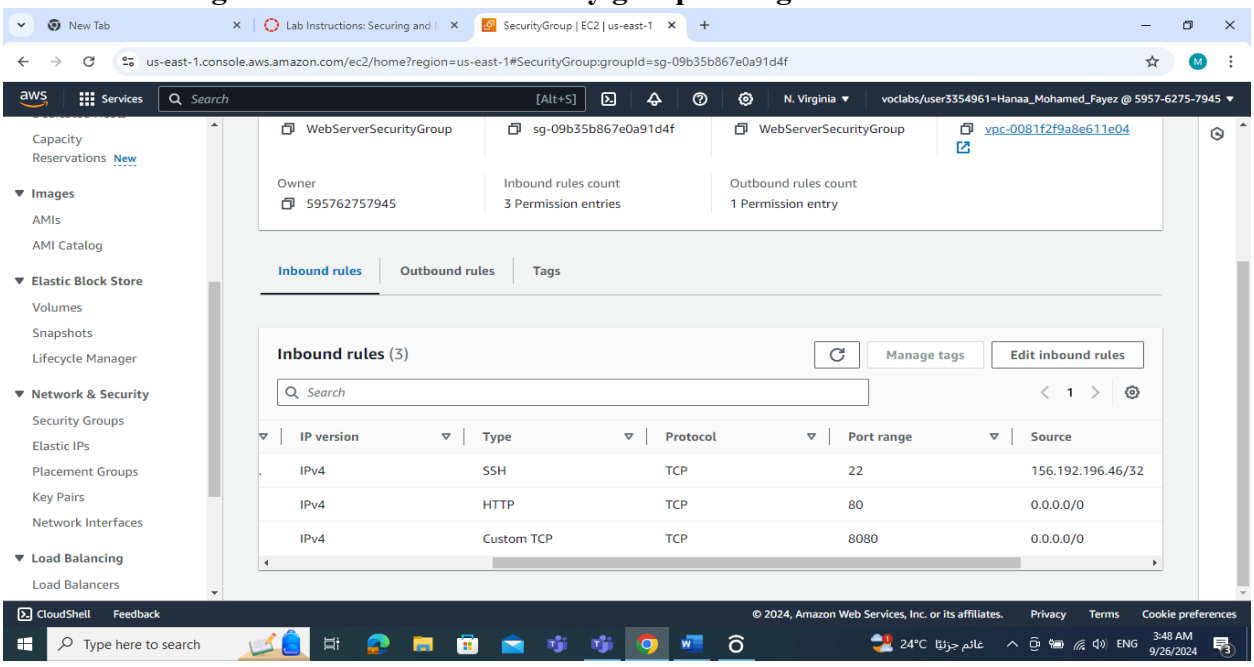
Task 2.2: Create a VPC flow log



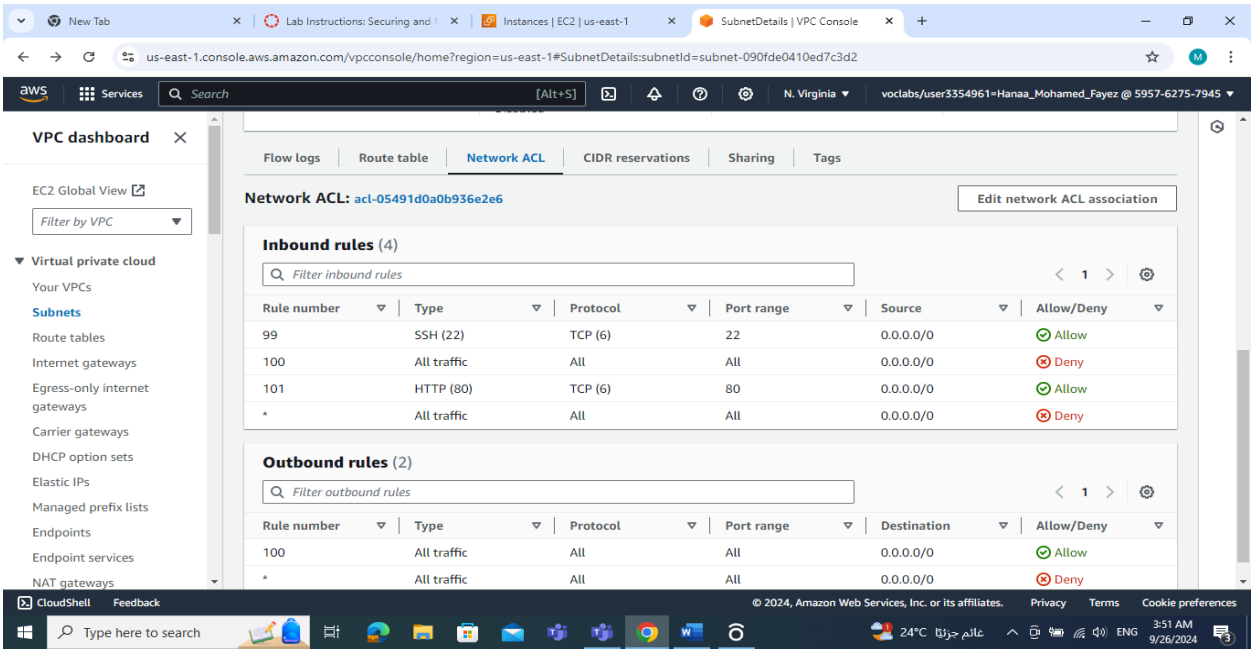


Task 2.3: Access the WebServer instance from the internet and review VPC flow logs in CloudWatch

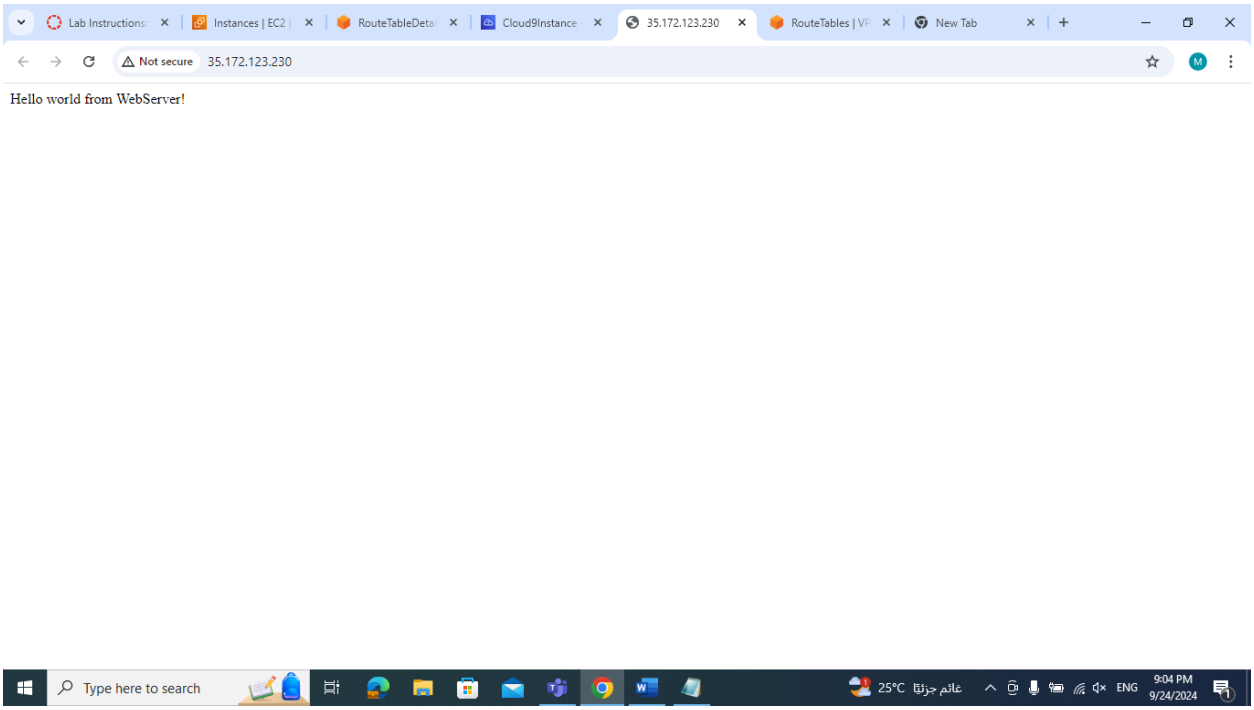
Task 2.4: Configure route table and security group settings



Task 2.5: Secure the WebServerSubnet with a network ACL

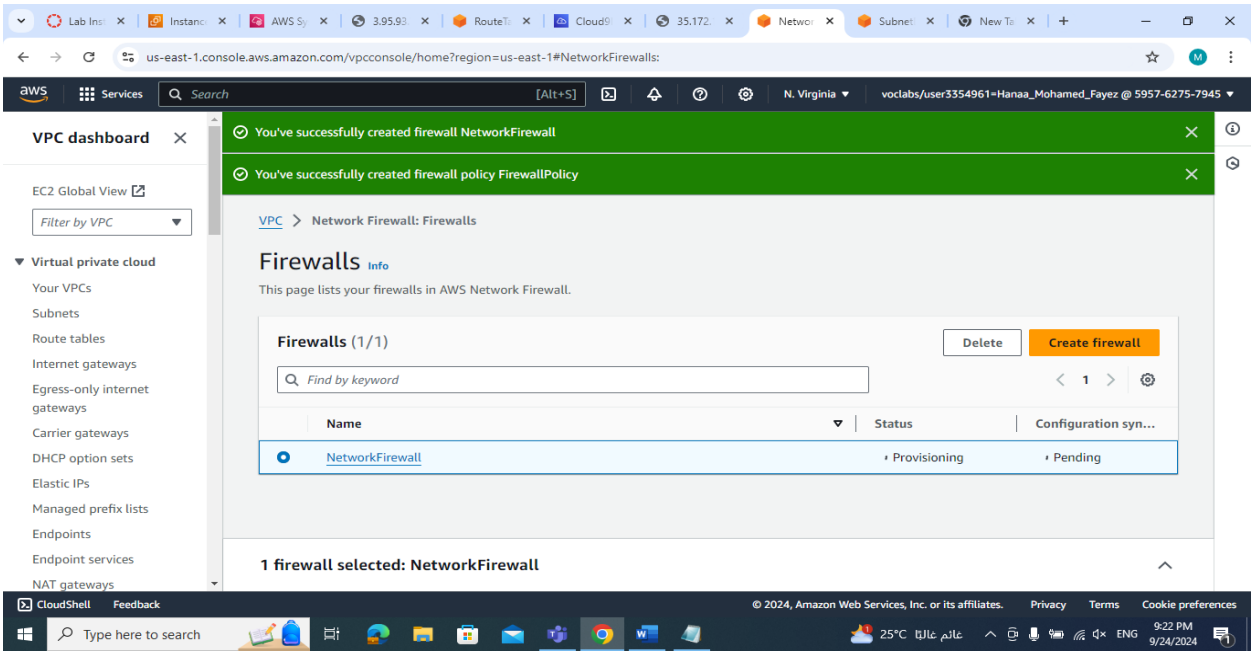


Access the webpage



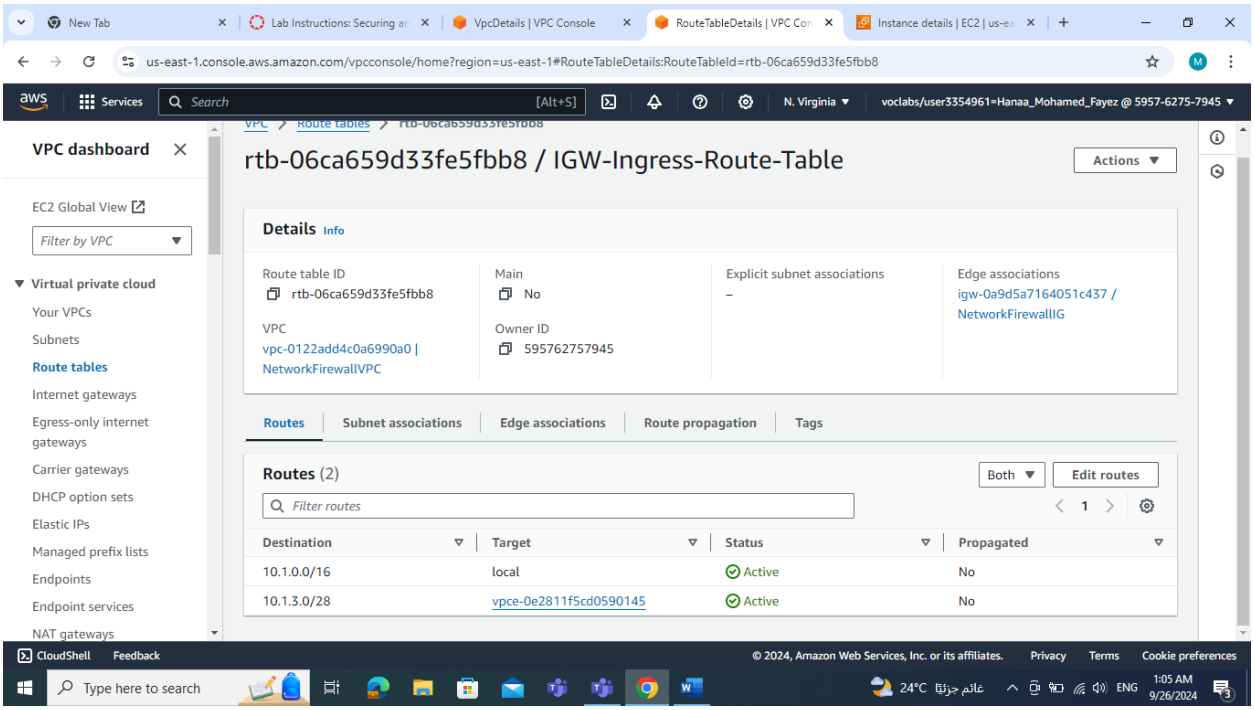
Task 2.7: Create a network firewall

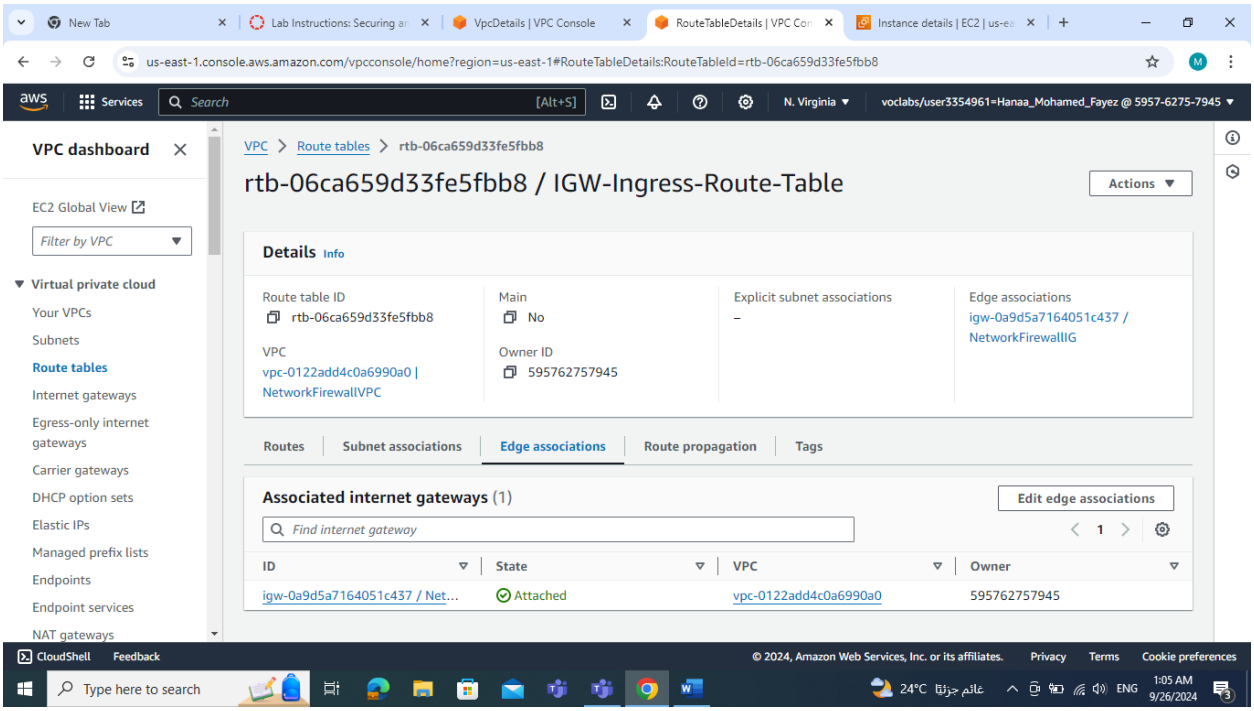
Create a firewall named NetworkFirewall



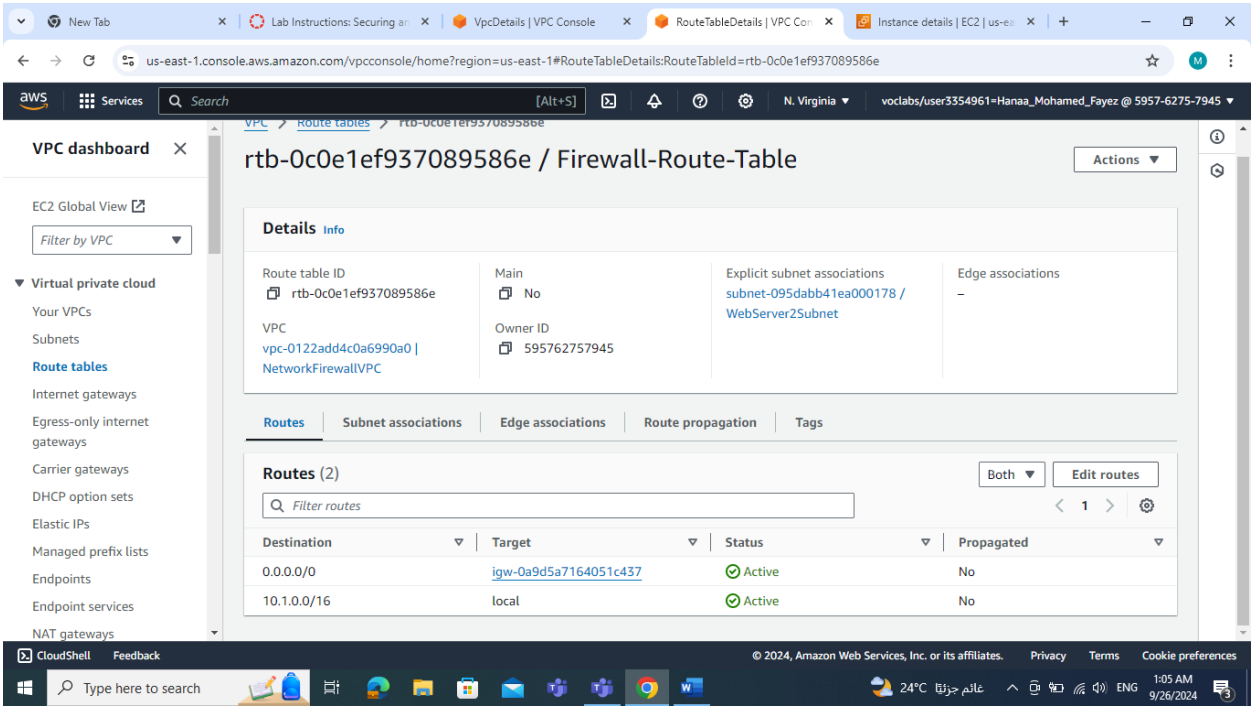
Task 2.8: Create route tables

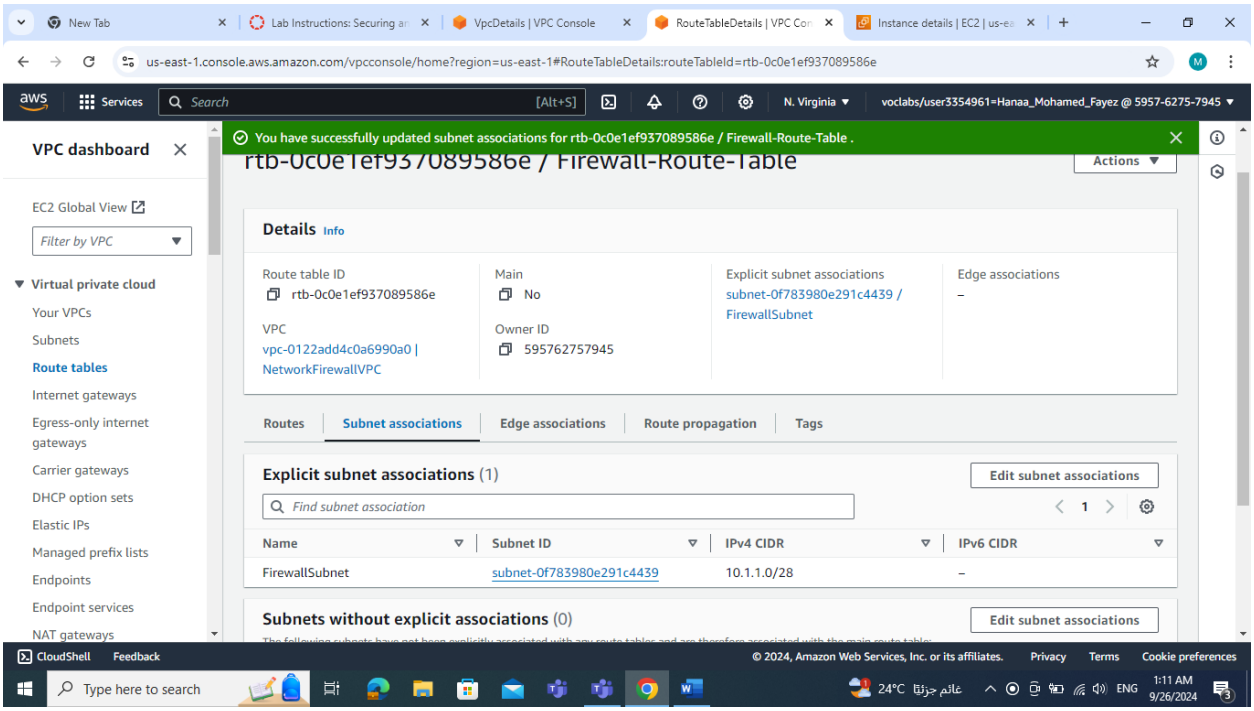
Create a new route table named IGW-Ingress-Route-Table in the *NetworkFirewallVPC*.



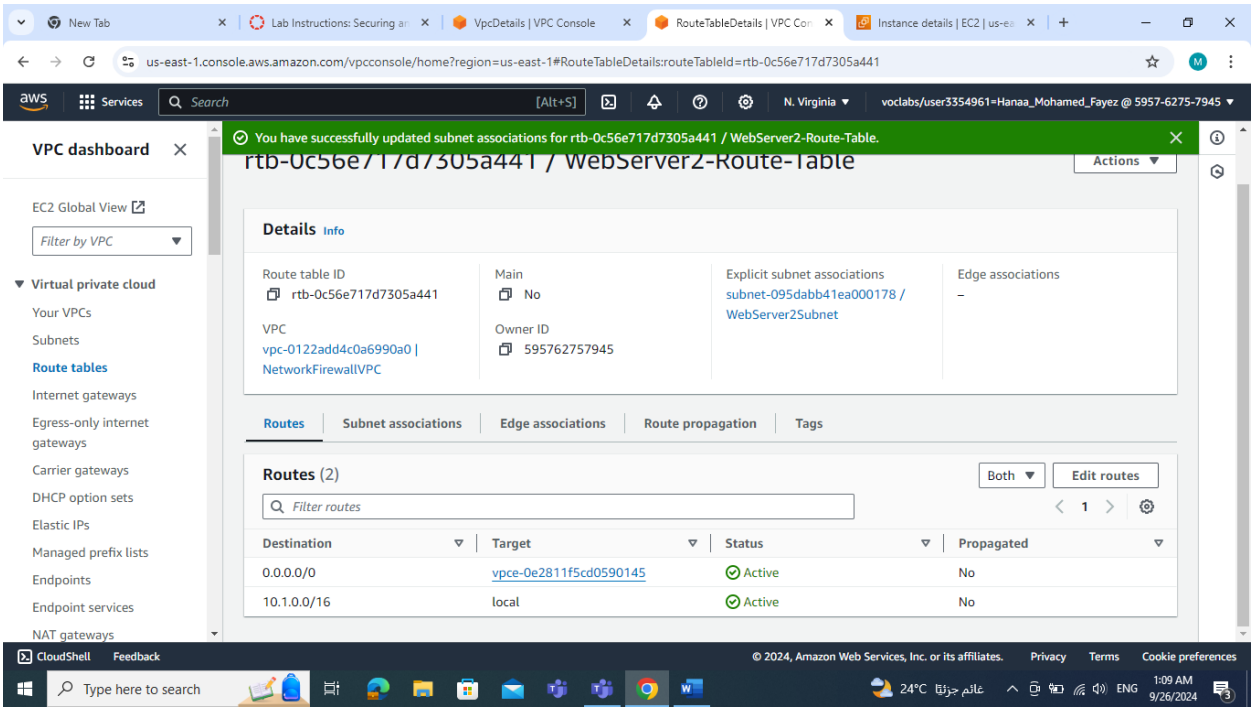


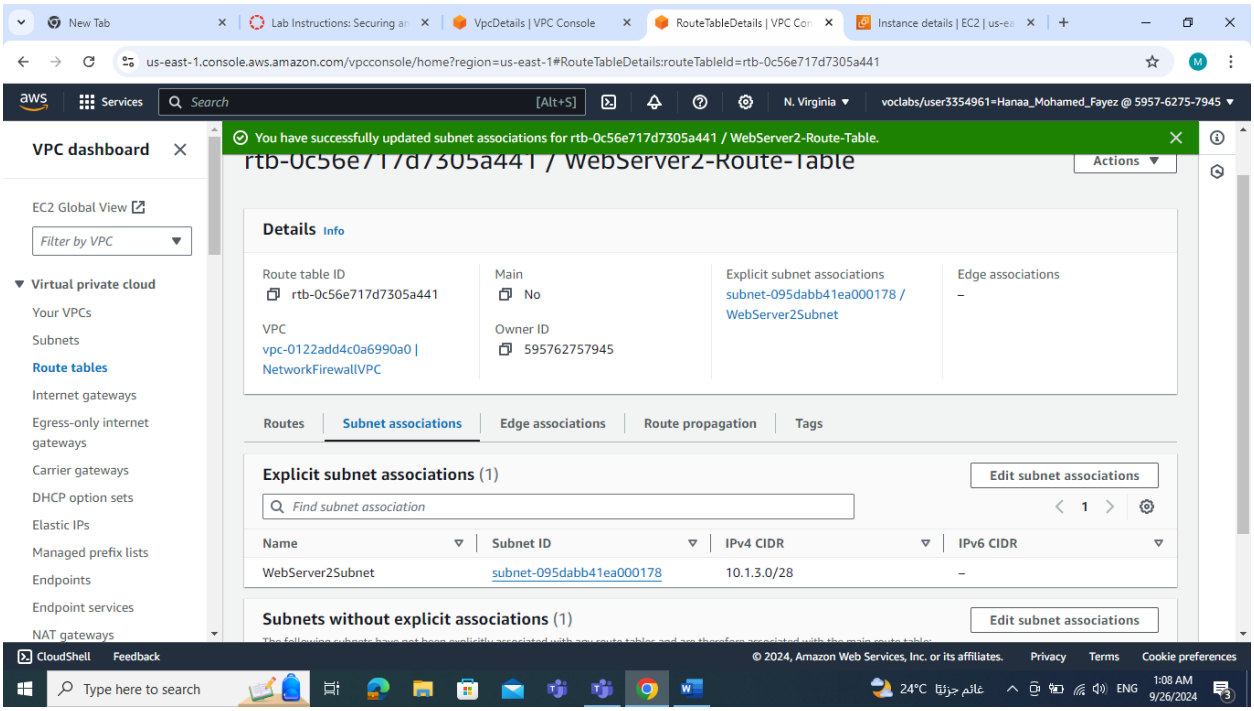
Create another route table in *NetworkFirewallVPC* for the *FirewallSubnet*.





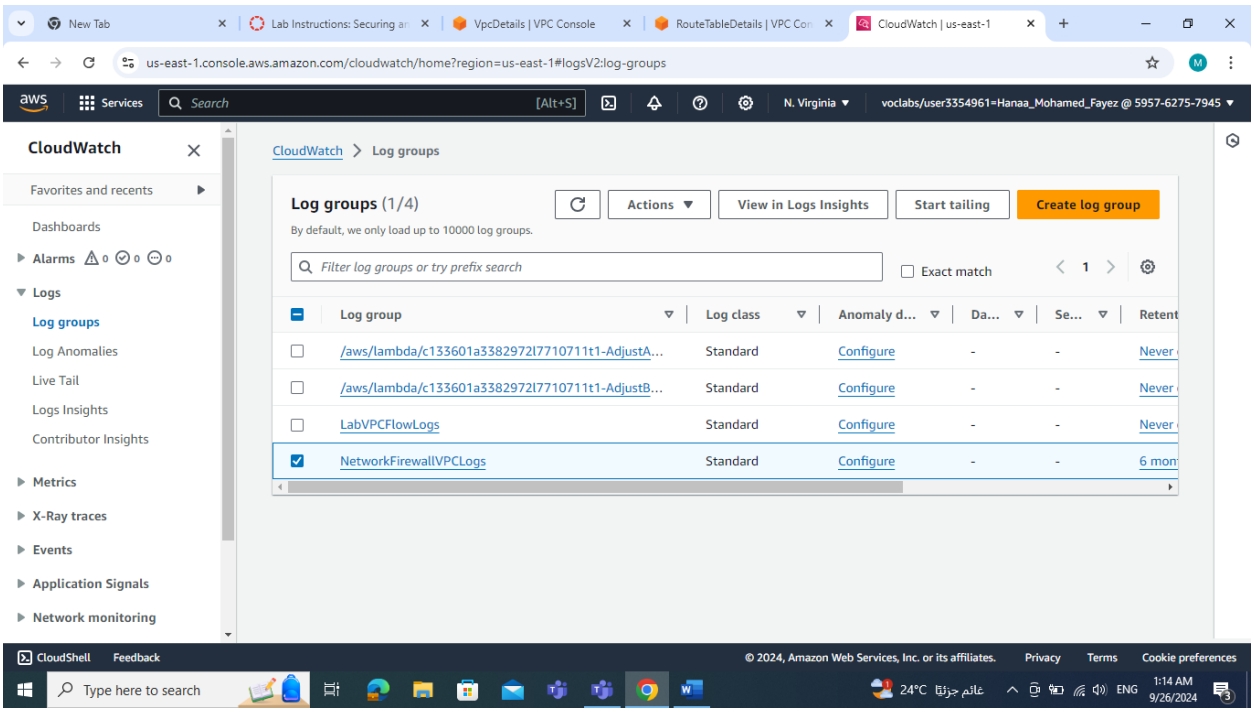
Create another route table in *NetworkFirewallVPC* for the *Webserver2Subnet*.

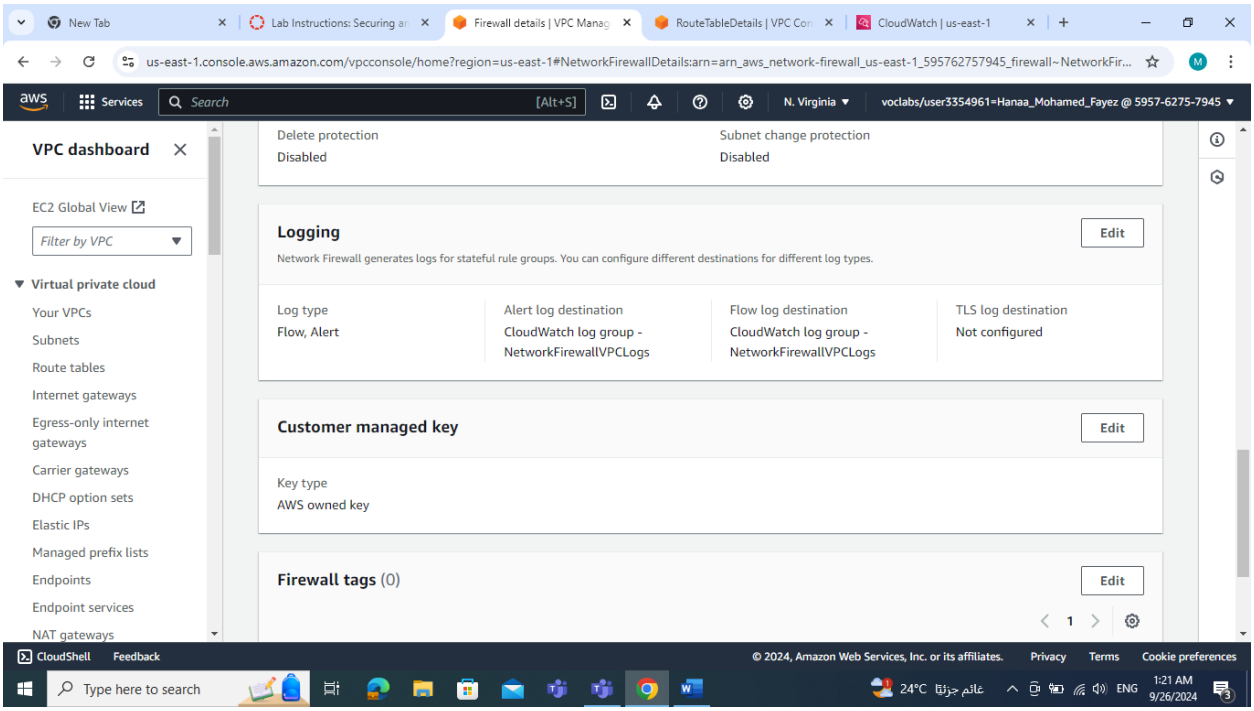


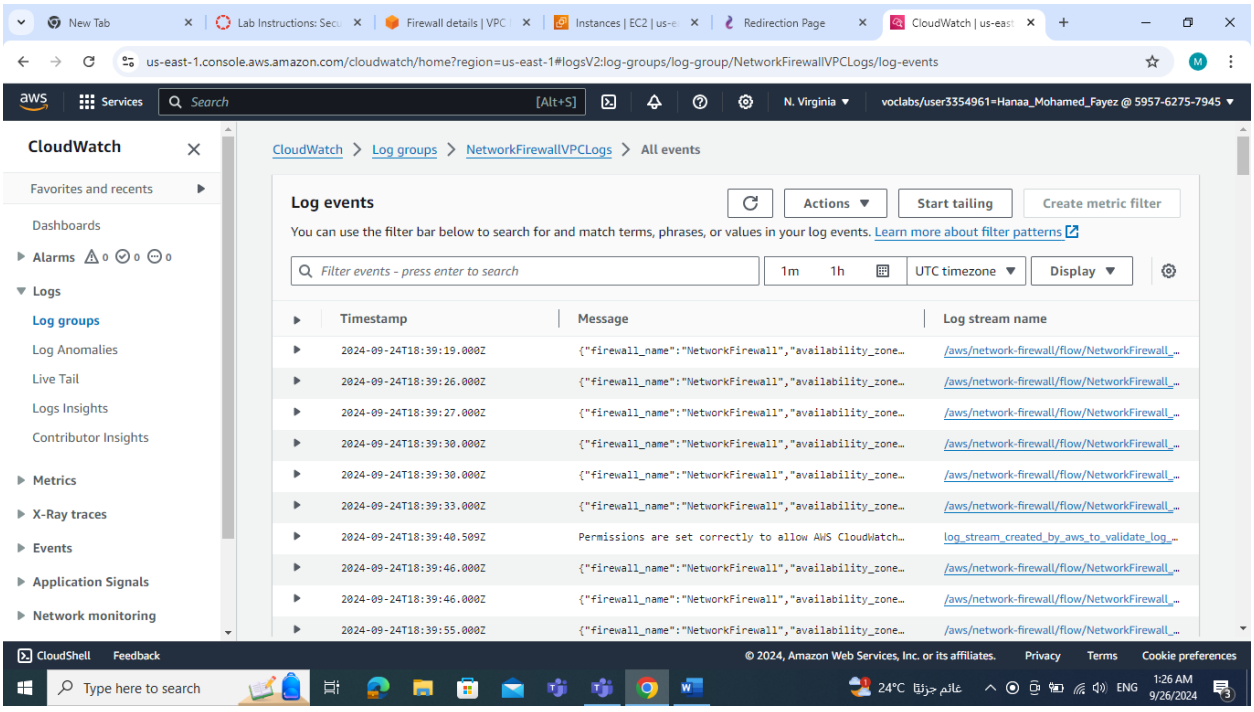


Task 2.9: Configure logging for the network firewall

Create a CloudWatch log group named NetworkFirewallVPCLogs

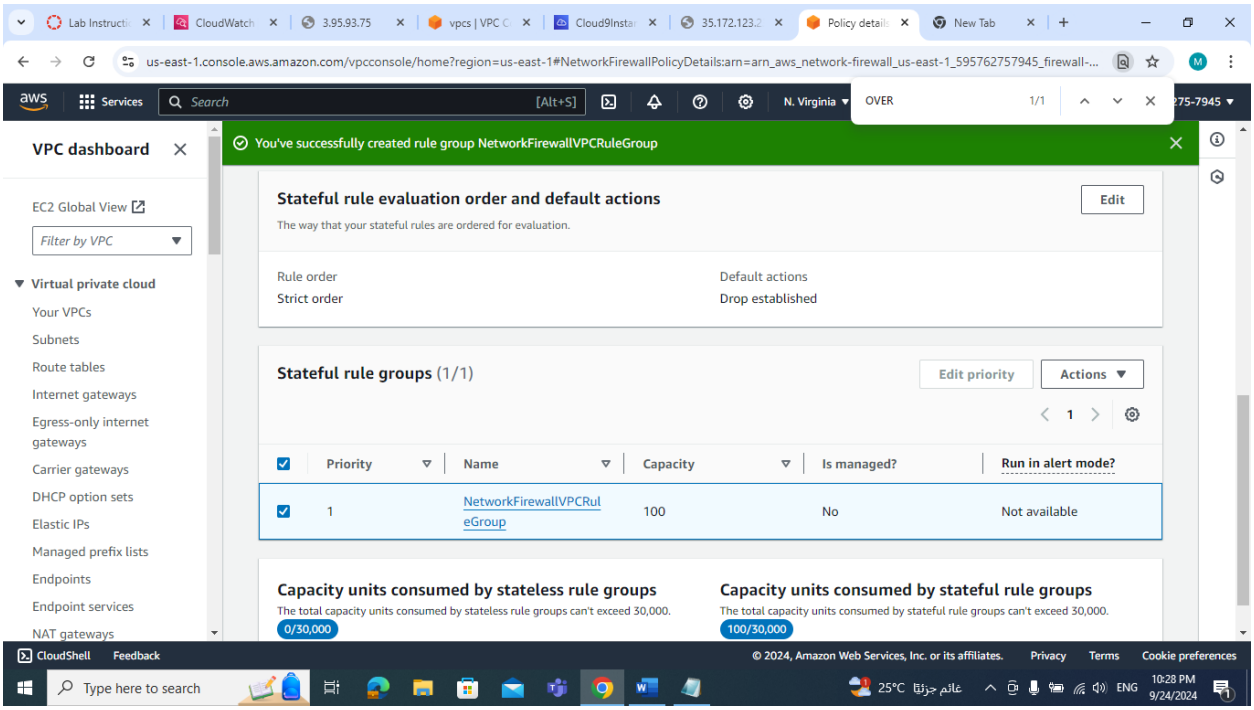


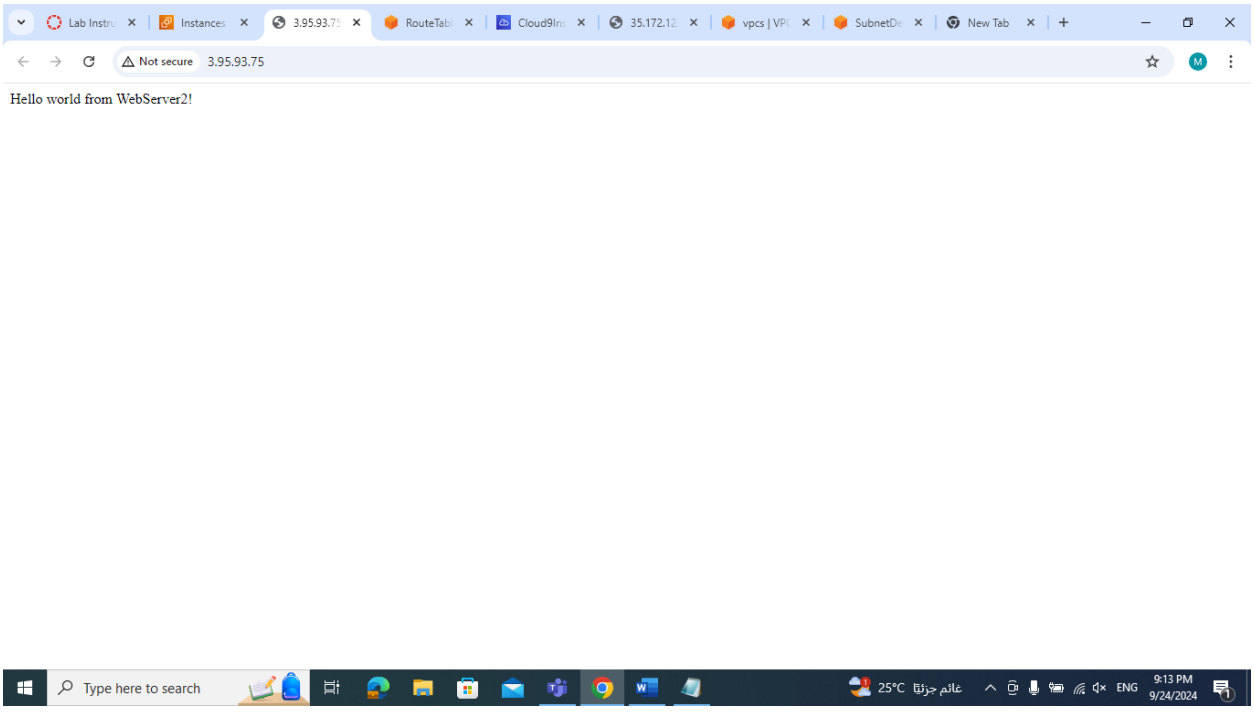

Delete protection
Disabled
Subnet change protection
Disabled
Logging
Edit
Network Firewall generates logs for stateful rule groups. You can configure different destinations for different log types.
Log type
Flow, Alert
Alert log destination
CloudWatch log group - NetworkFirewallVPCLogs
Flow log destination
CloudWatch log group - NetworkFirewallVPCLogs
TLS log destination
Not configured
Customer managed key
Edit
Key type
AWS owned key
Firewall tags (0)
Edit
VPC dashboard
EC2 Global View
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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


CloudWatch
Log groups
NetworkFirewallVPCLogs
All events
Log events
Actions
Start tailing
Create metric filter
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
Filter events - press enter to search
1m
1h
UTC timezone
Display
Timestamp
Message
Log stream name
2024-09-24T18:39:19.000Z
2024-09-24T18:39:26.000Z
2024-09-24T18:39:27.000Z
2024-09-24T18:39:30.000Z
2024-09-24T18:39:30.000Z
2024-09-24T18:39:33.000Z
2024-09-24T18:39:40.509Z
Permissions are set correctly to allow AWS CloudWatch...
2024-09-24T18:39:46.000Z
2024-09-24T18:39:46.000Z
2024-09-24T18:39:55.000Z
{"firewall_name":"NetworkFirewall","availability_zone...
/aws/network-firewall/flow/NetworkFirewall_...
log_stream_created_by_aws_to_validate_log_...
Favorites and recents
Dashboards
Alarms
Logs
Log groups
Log Anomalies
Live Tail
Logs Insights
Contributor Insights
Metrics
X-Ray traces
Events
Application Signals
Network monitoring
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

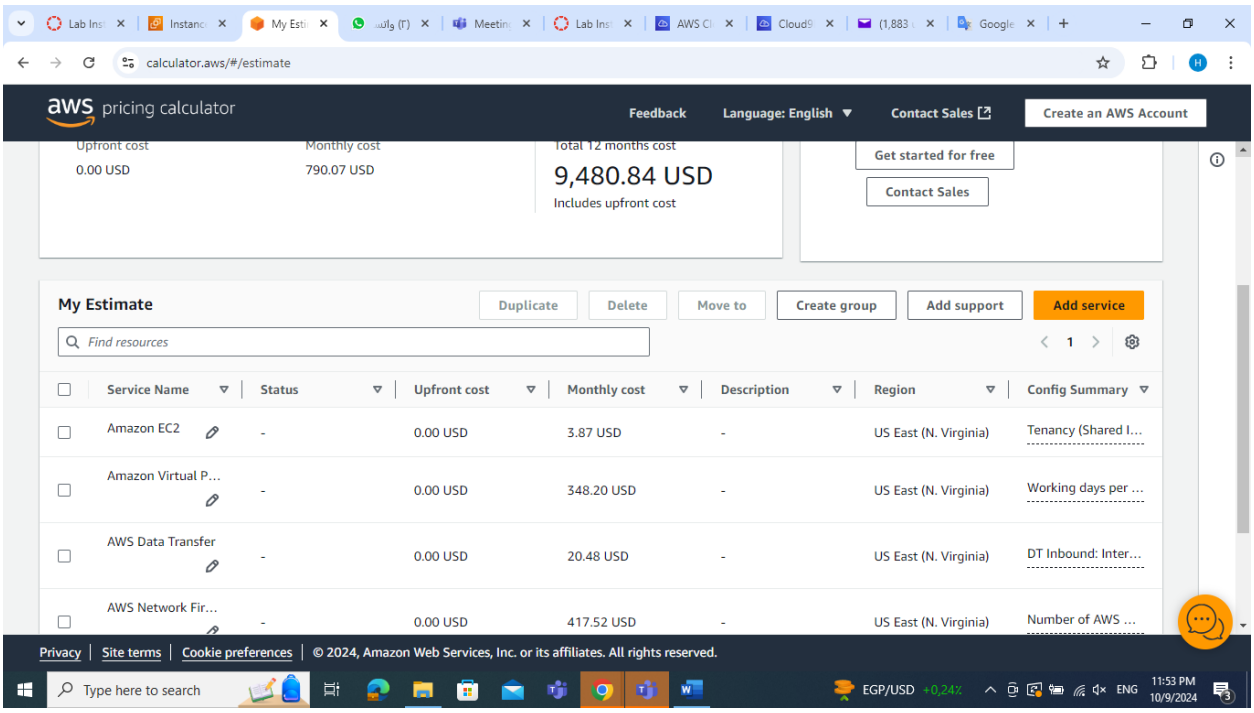
Task 2.10: Configure the firewall policy and test access

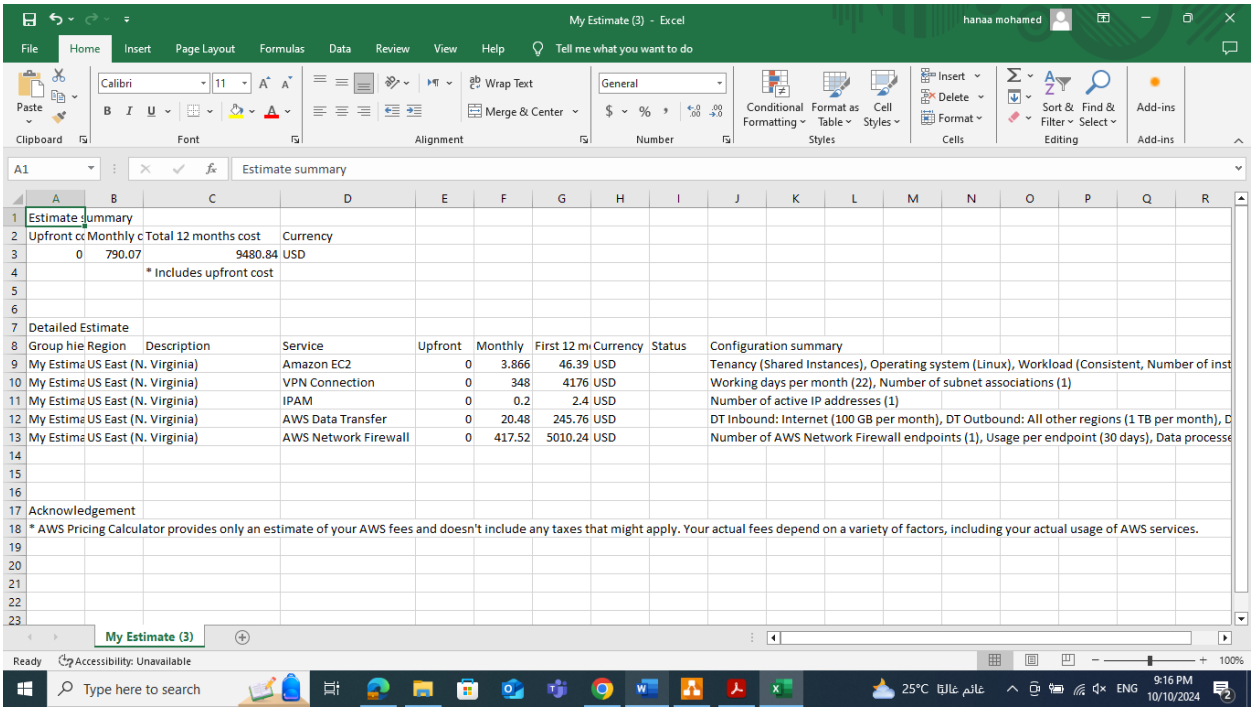
Configure the stateful rule group with the name NetworkFirewallVPCRuleGroup





Cost estimate to secure a VPC with a network firewall

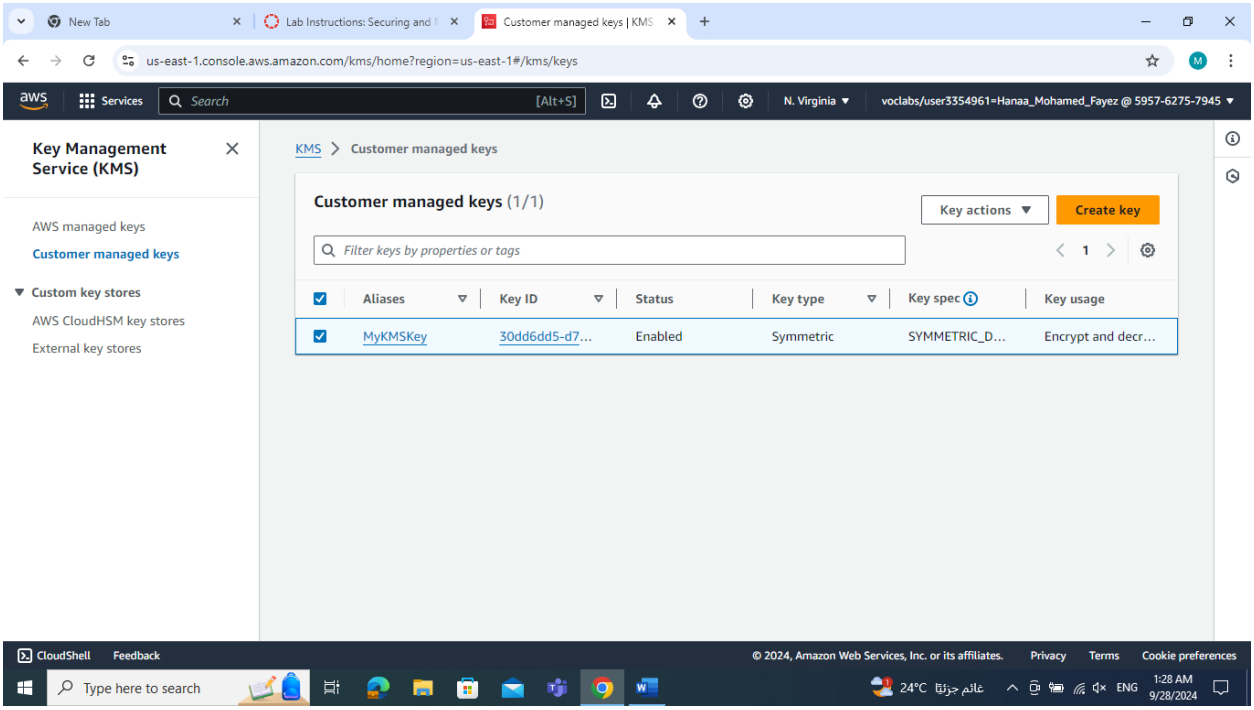


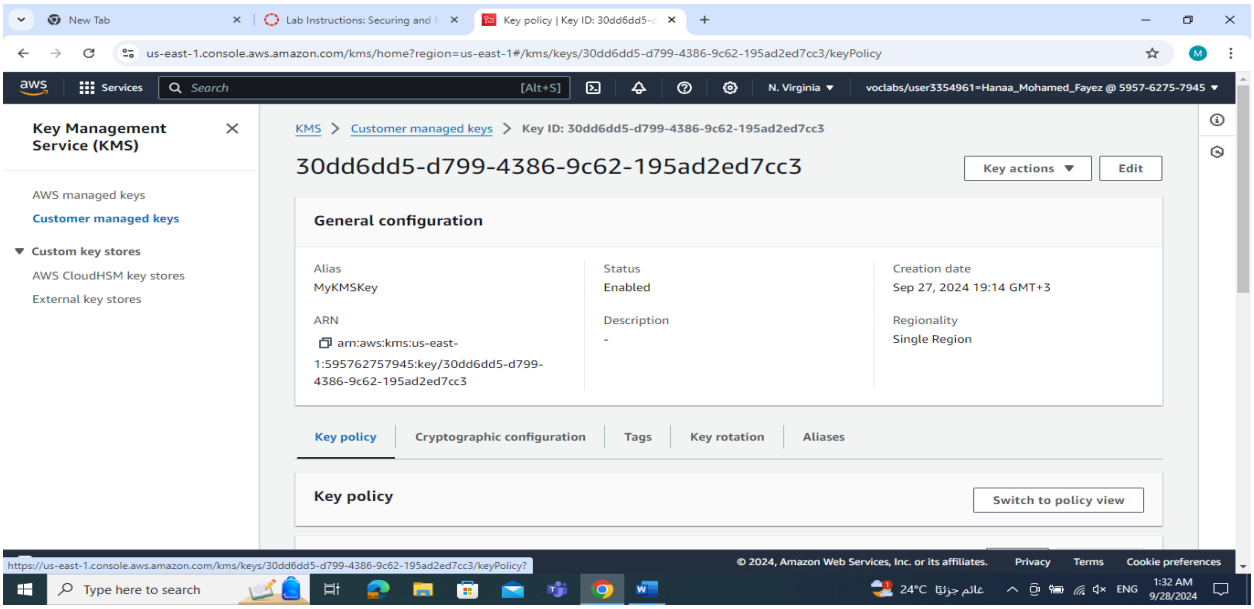


Phase 3: Securing AWS resources by using AWS KMS

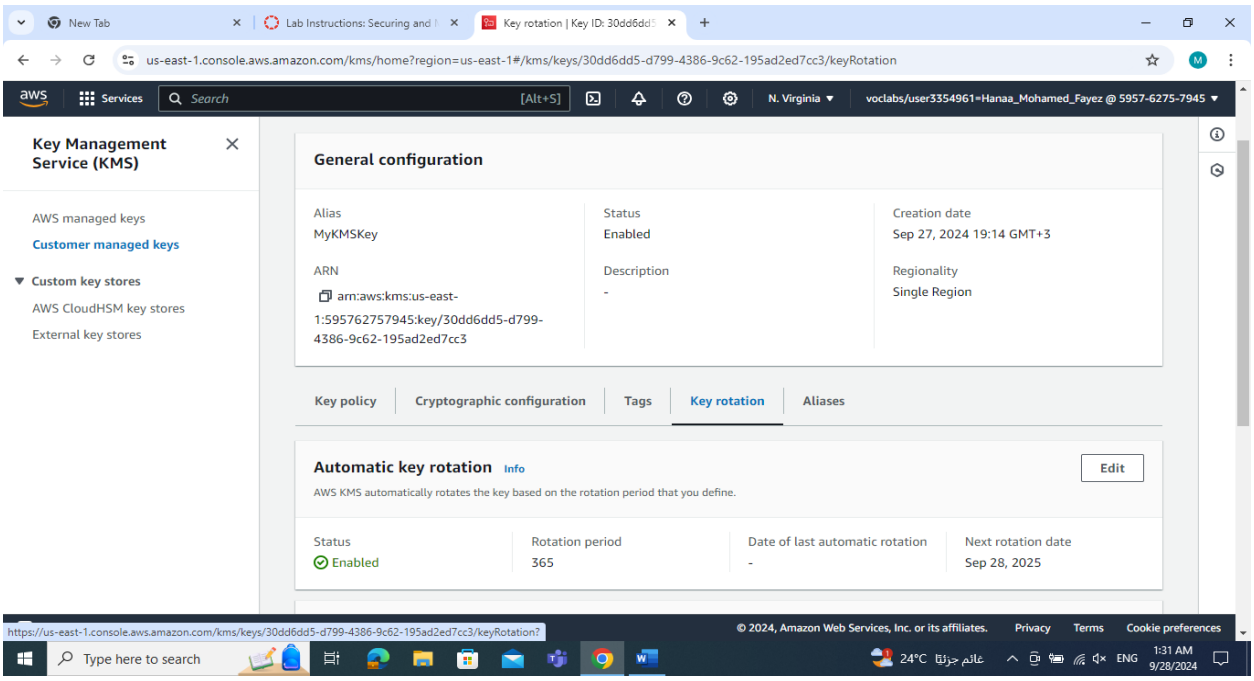
Task 3.1: Create a customer managed key and configure key rotation

Create an AWS KMS with the alias (name) of MyKMSKey



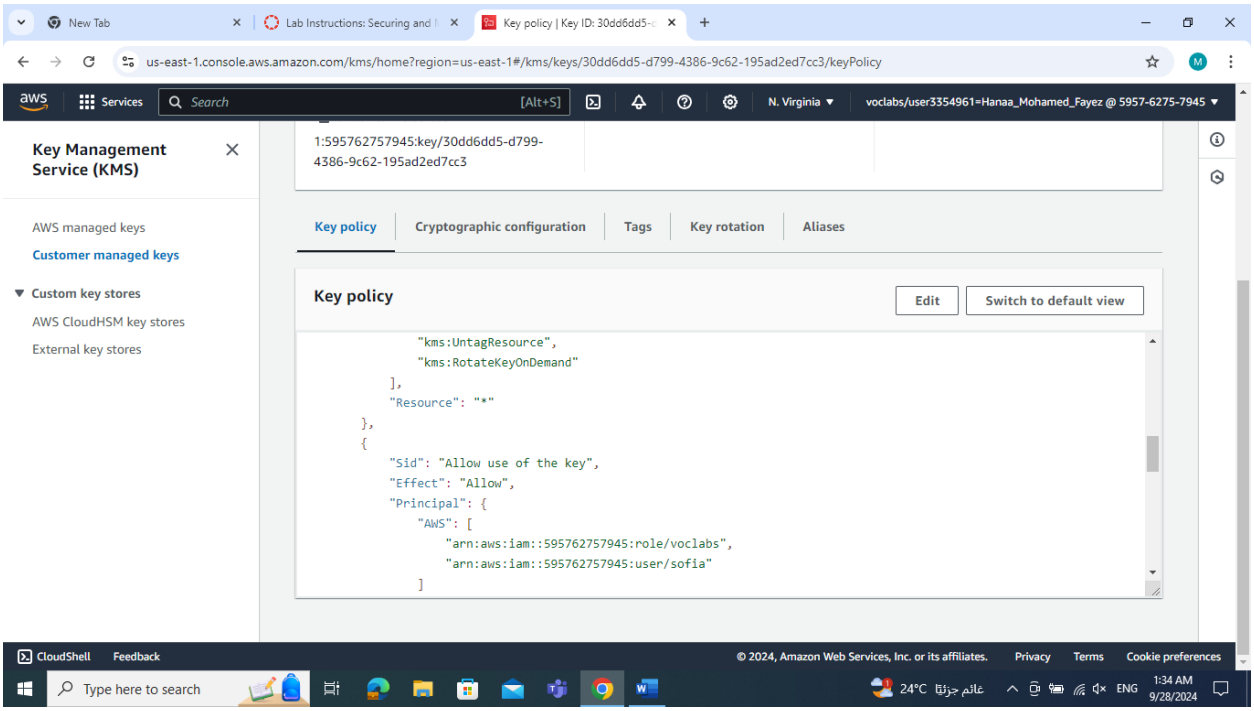


Configure AWS KMS key rotation on the new key so that it is automatically rotated every year

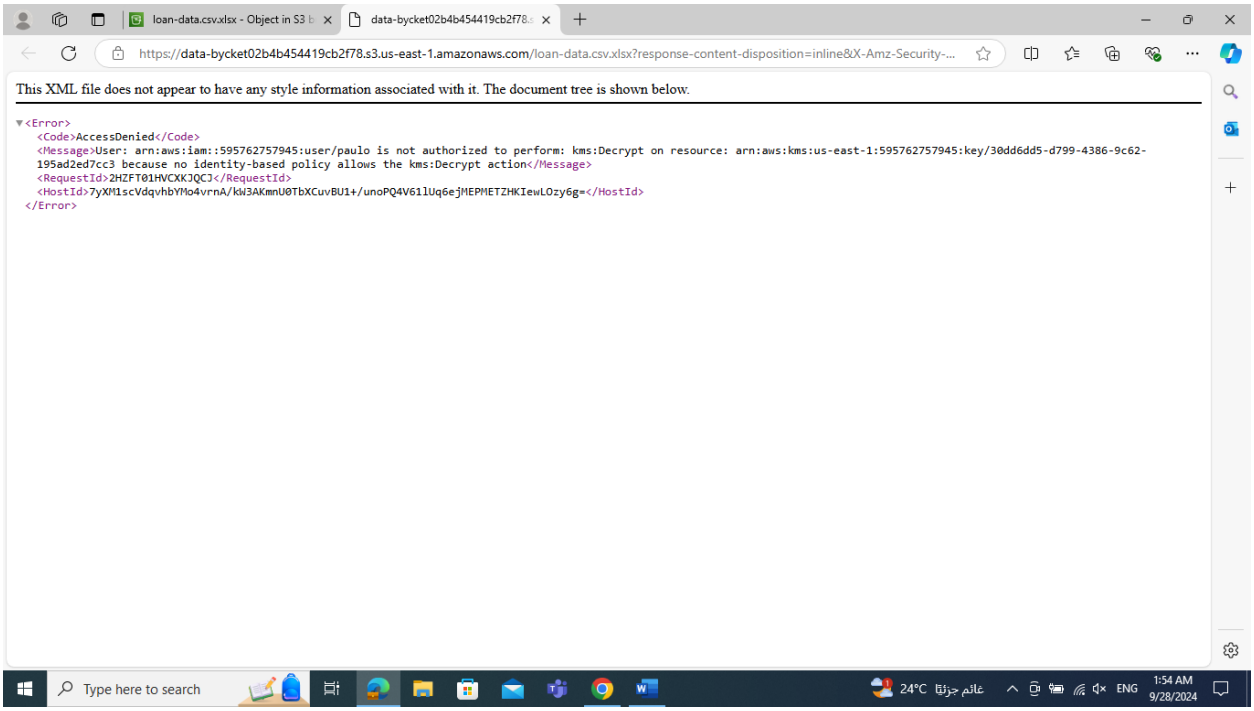


Task 3.2: Update the AWS KMS key policy and analyze an IAM policy

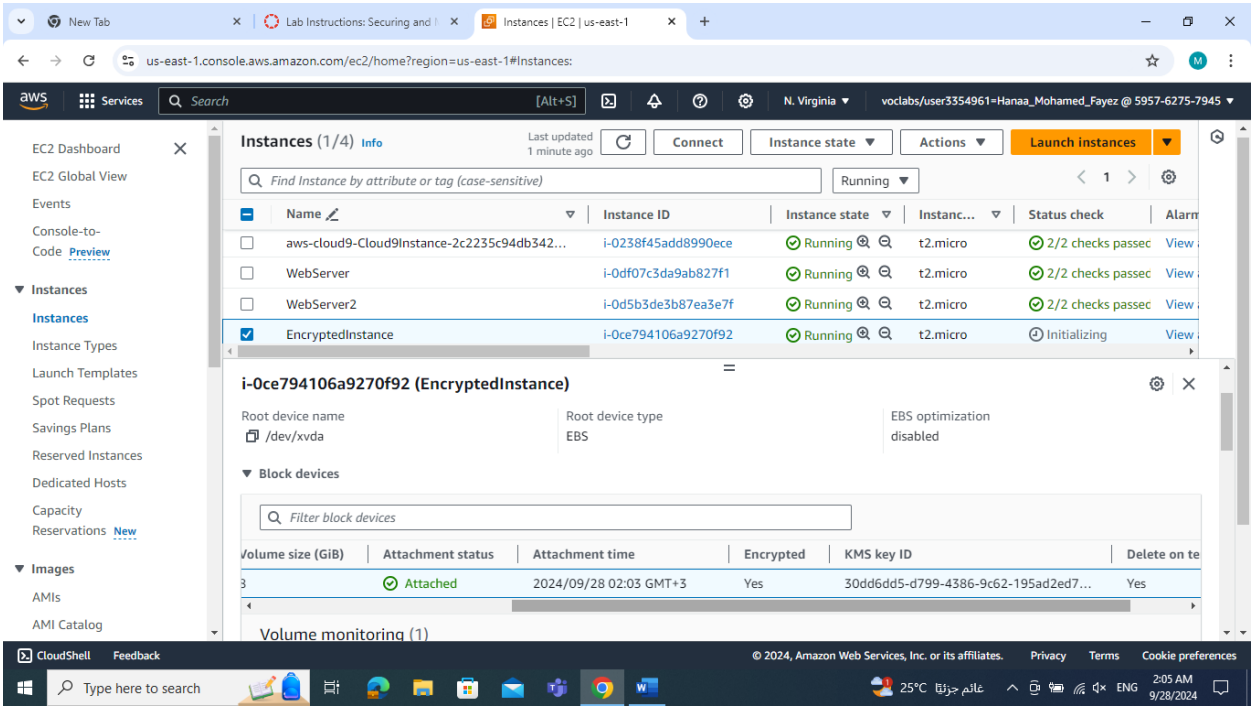
Modify the key policy for *MyKMSKey* so that it allows the *sofia* IAM user to use the key



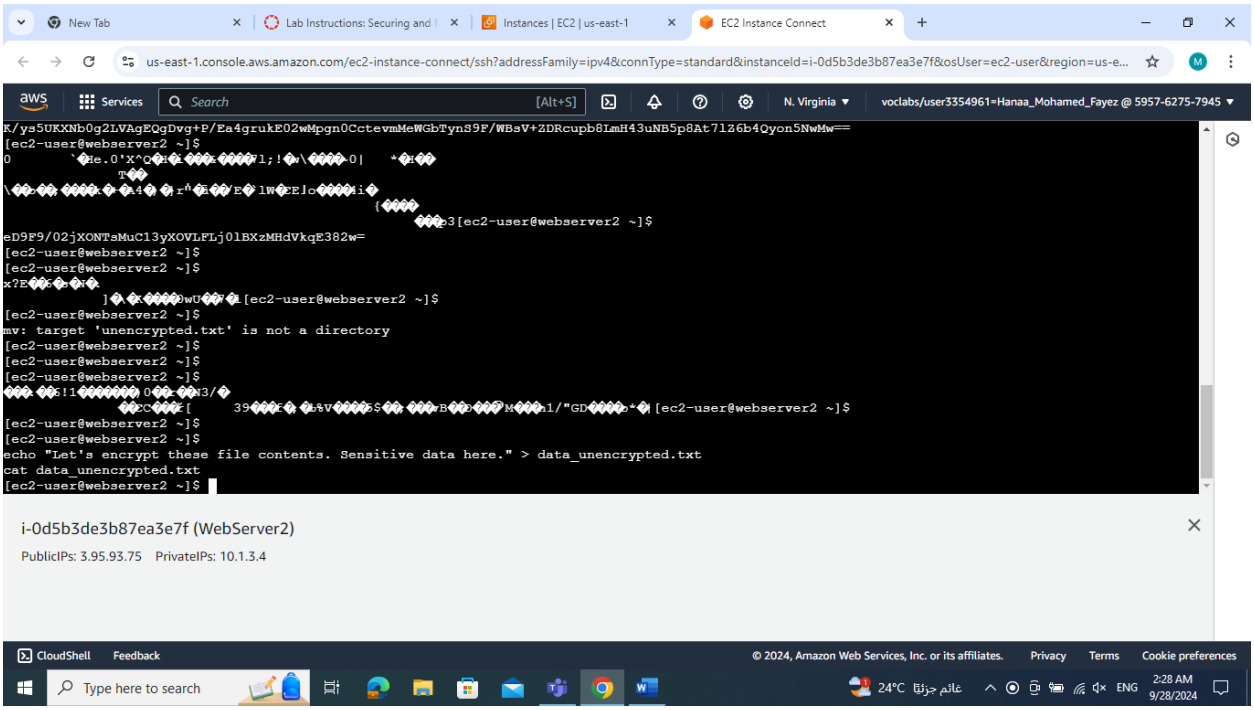
Task 3.3: Use AWS KMS to encrypt data in Amazon S3



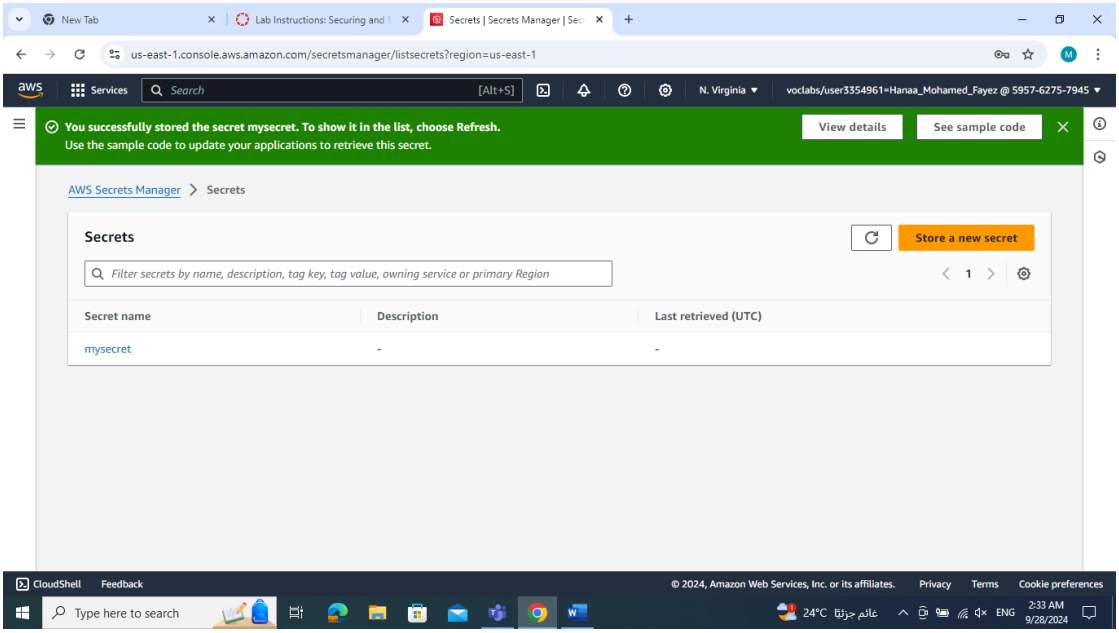
Task 3.4: Use AWS KMS to encrypt the root volume of an EC2 instance

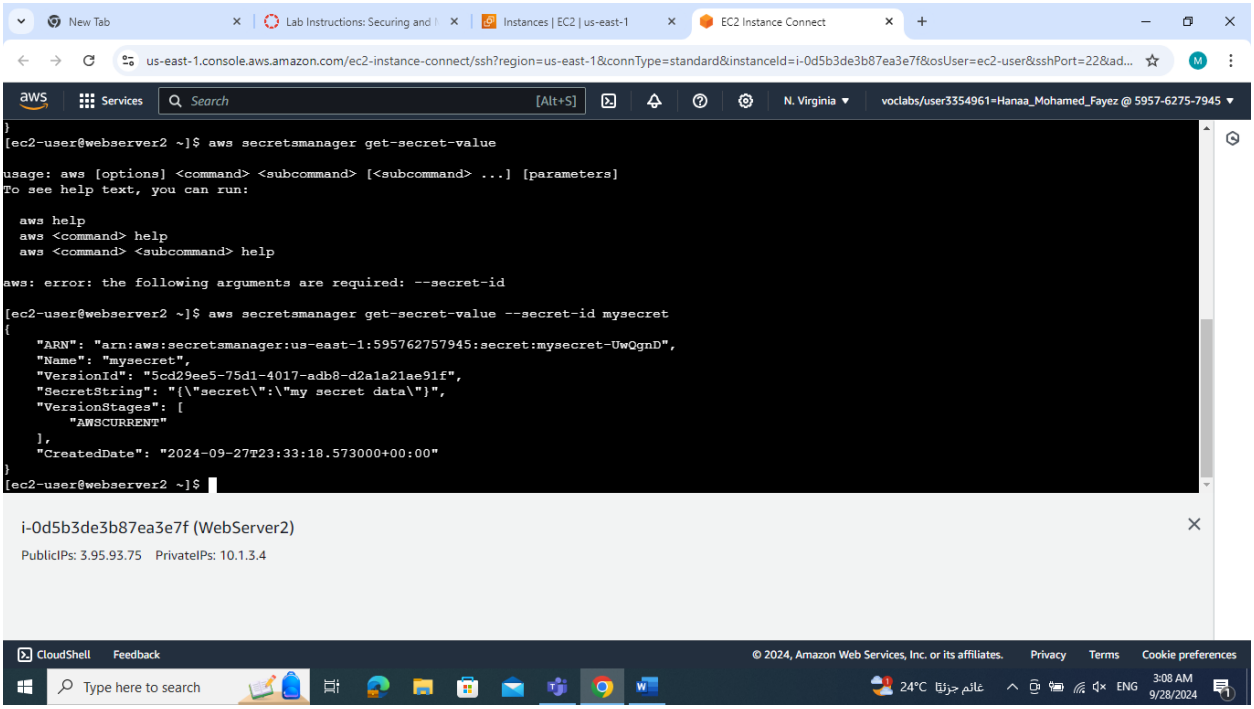


Task 3.5: Use AWS KMS envelope encryption to encrypt data in place

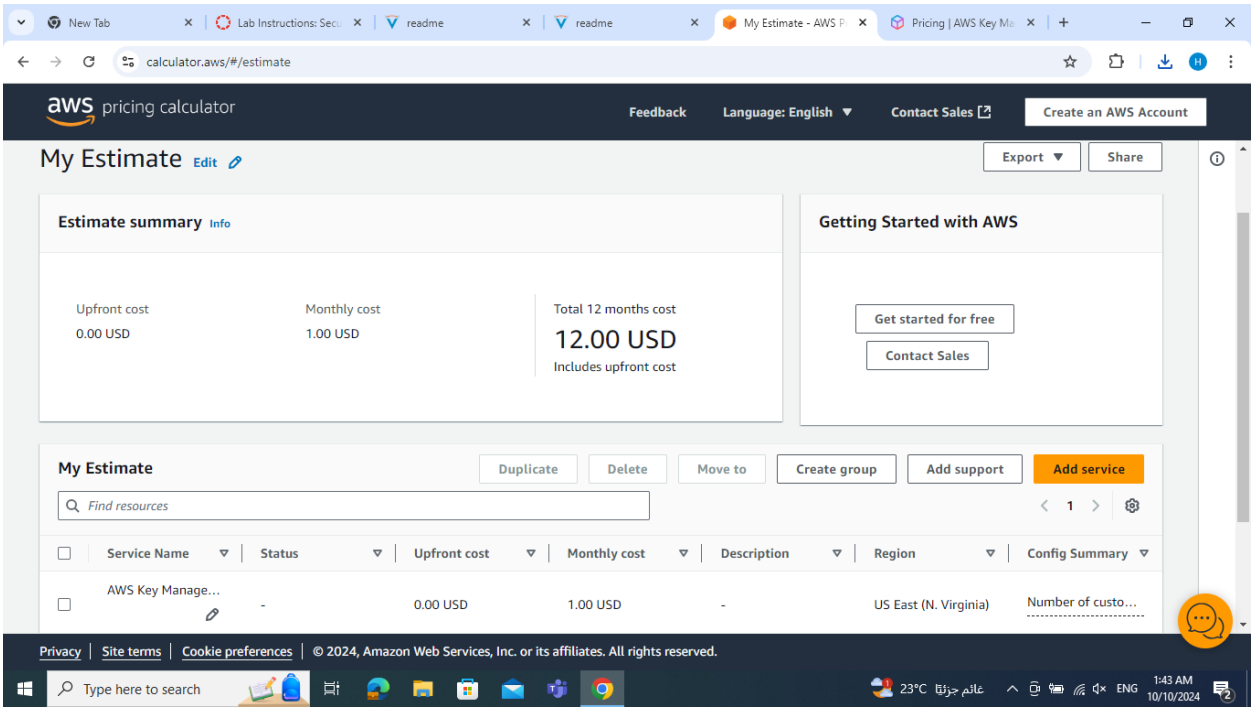


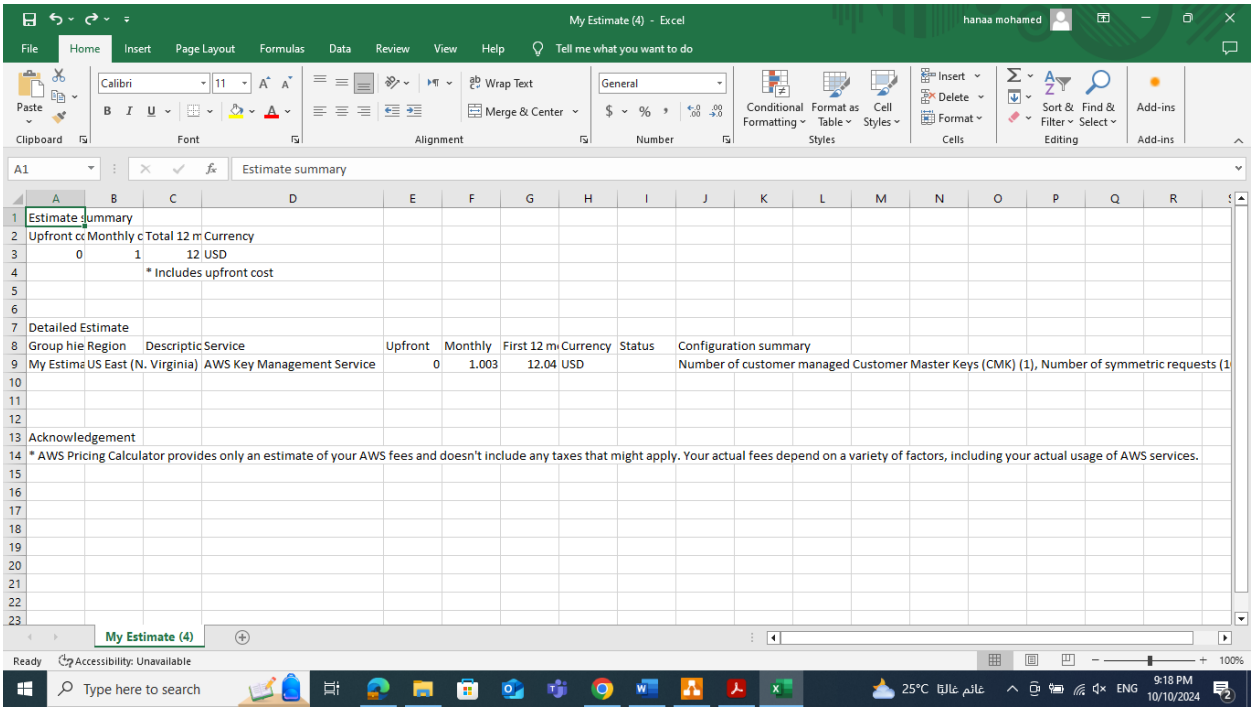
Task 3.6: Use AWS KMS to encrypt a Secrets Manager secret





Estimate Cost for using AWS KMS

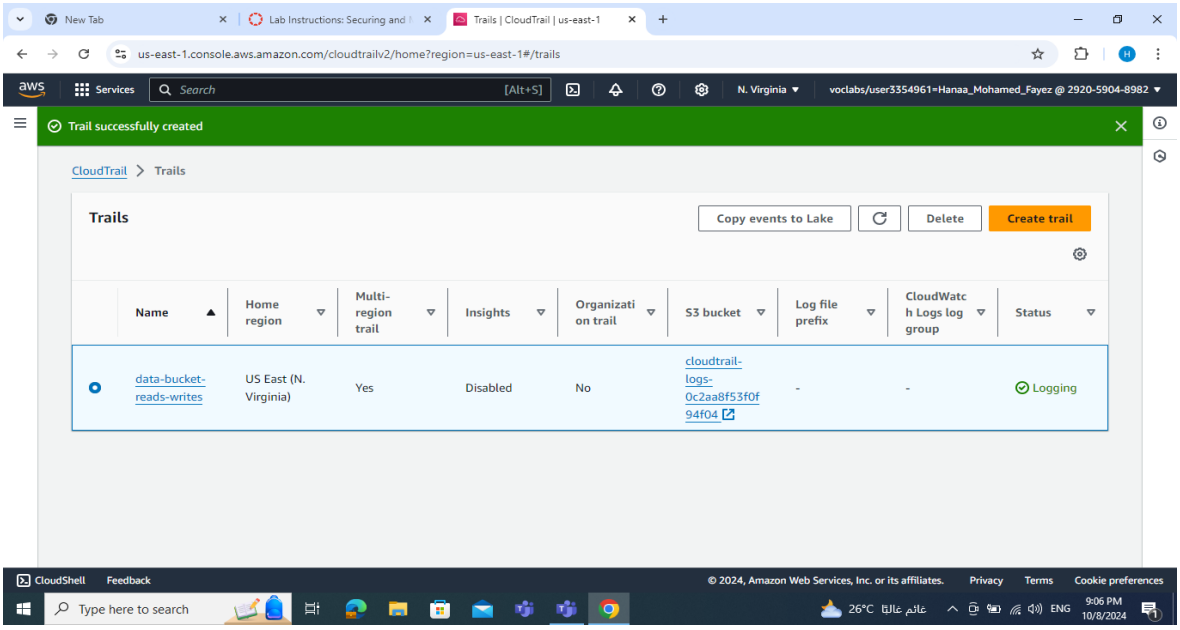




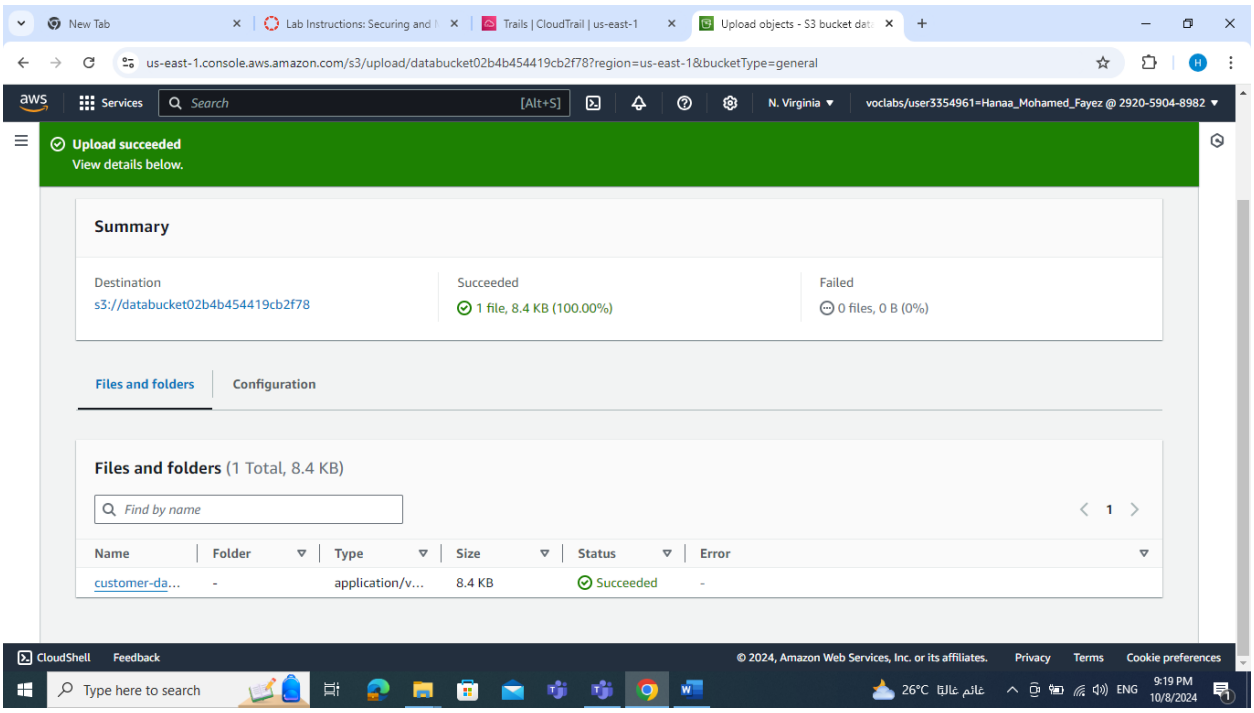
Phase 4: Monitoring and logging

Task 4.1: Use CloudTrail to record Amazon S3 API calls

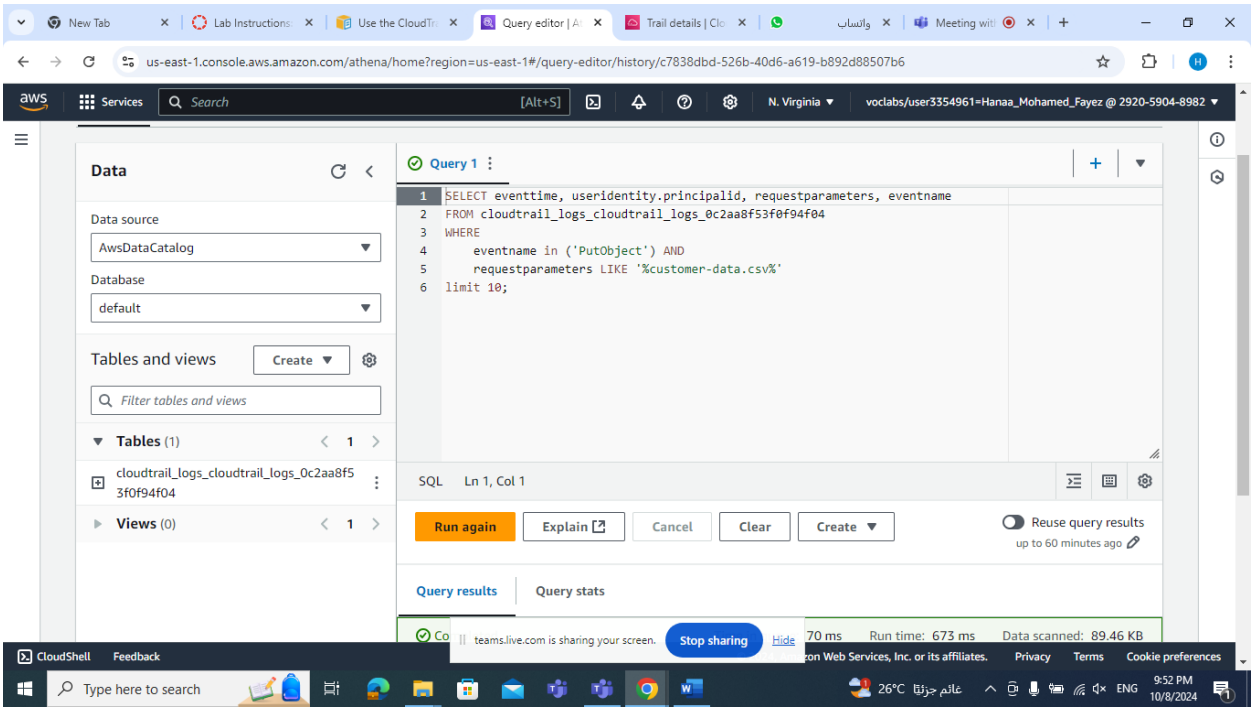
Create trail (data-bucket-reads-writes)

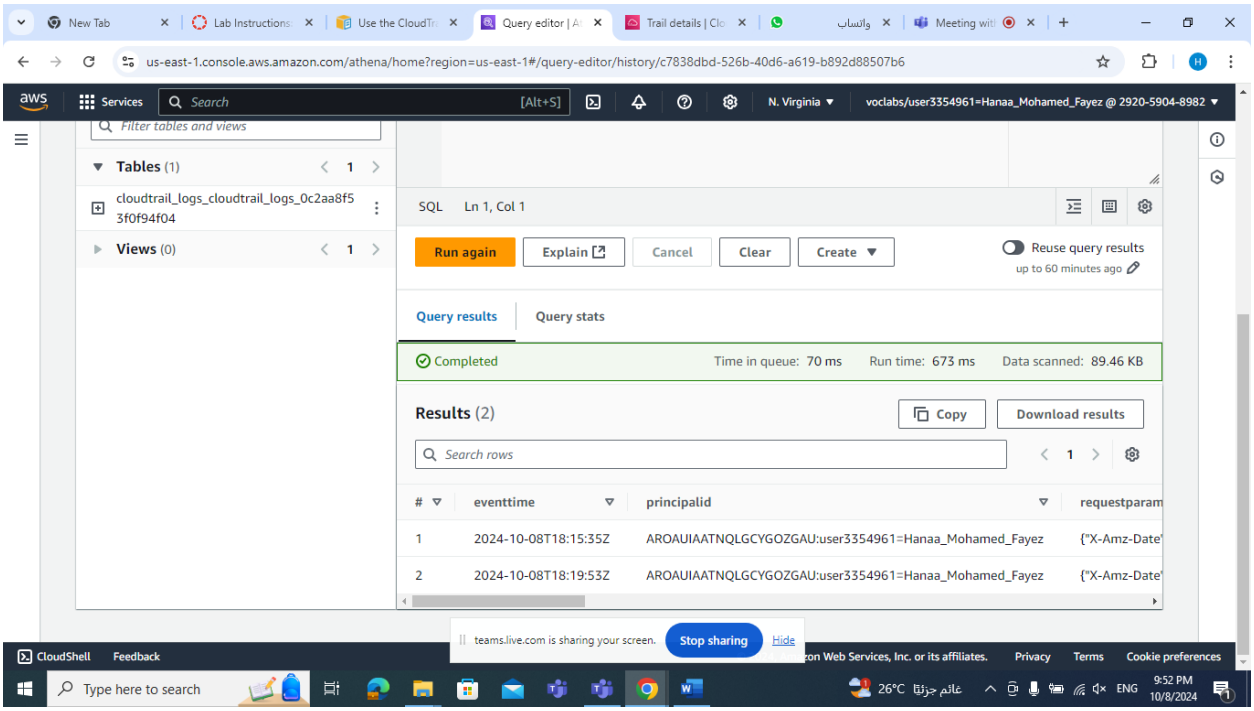


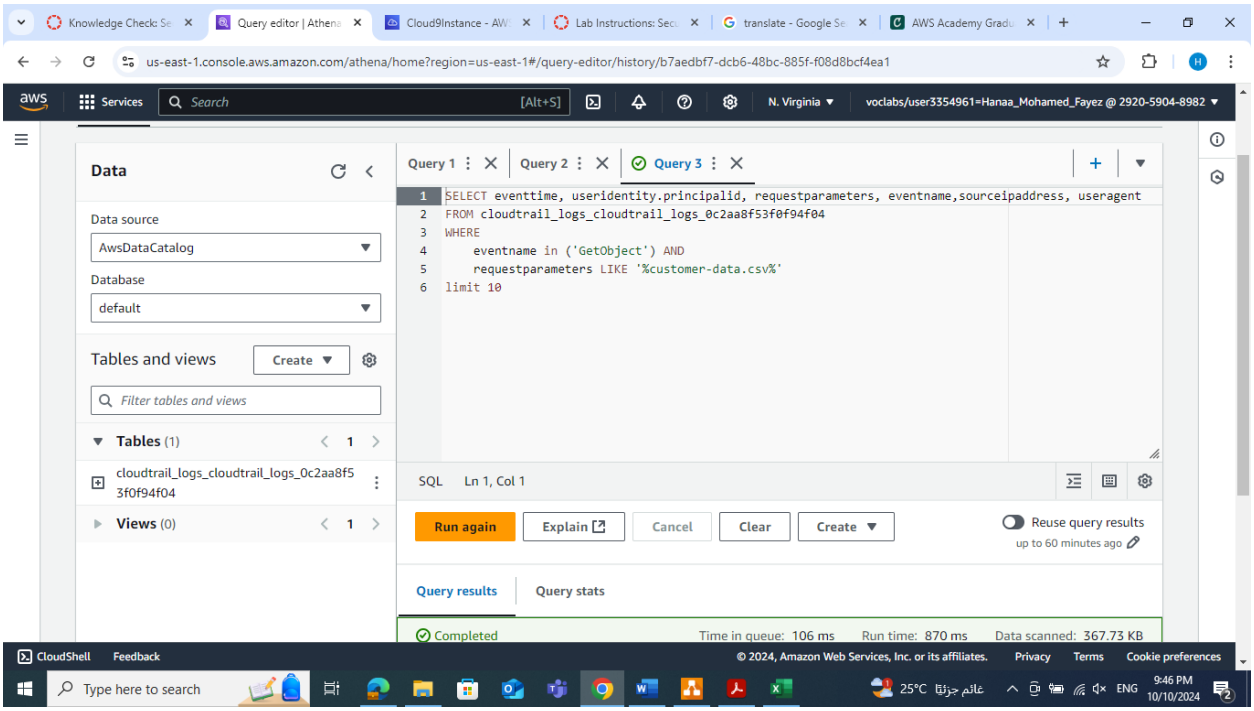
Upload the *customer-data.csv* file to *data-bucket*

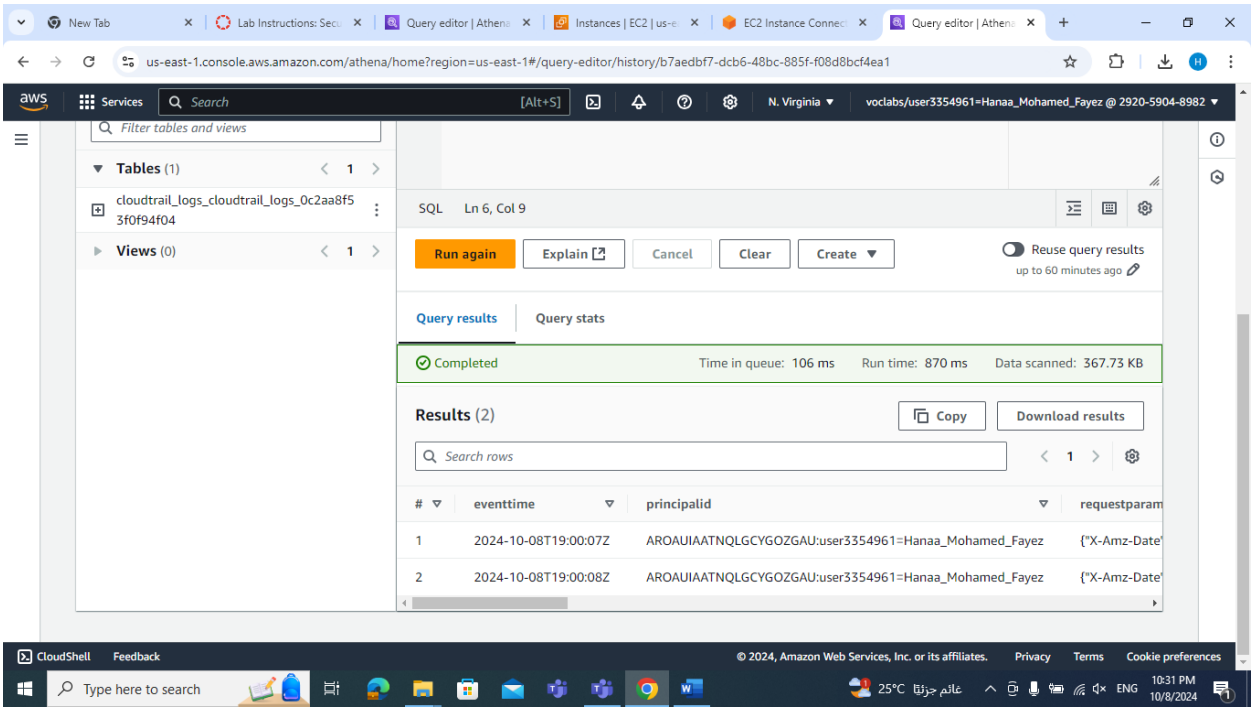


Use the CloudTrail console to create an Athena table that describes the format of the data in the *cloudtrail-logs* S3 bucket.



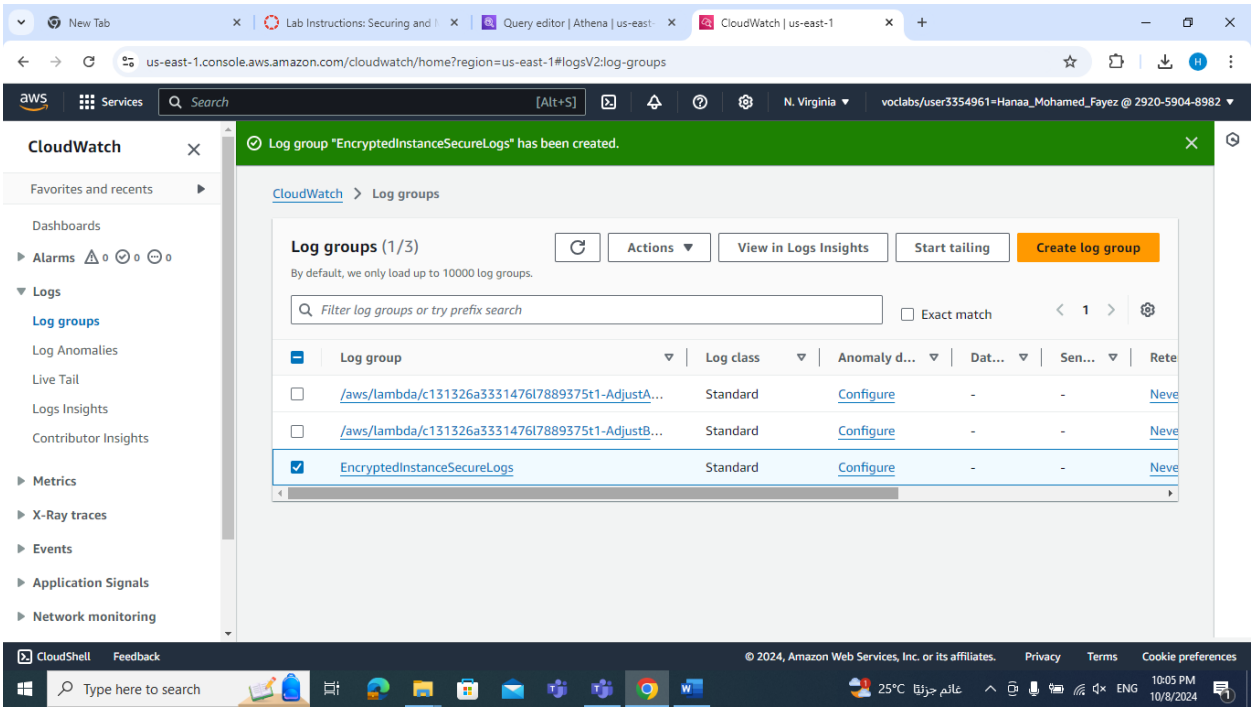

us-east-1.console.aws.amazon.com/athena/home?region=us-east-1#/query-editor/history/c7838dbd-526b-40d6-a619-b892d88507b6
Tables (1)
cloudtrail_logs_cloudtrail_logs_0c2aa8f53f0f94f04
Views (0)
SQL Ln 1, Col 1
Run again
Explain
Cancel
Clear
Create
Reuse query results
up to 60 minutes ago
Query results
Query stats
Completed
Time in queue: 70 ms
Run time: 673 ms
Data scanned: 89.46 KB
Results (2)
Copy
Download results
Search rows
eventtime principalid requestparam
1 2024-10-08T18:15:35Z AROAUIAATNQLGCYGOZGAU:user3354961=Hanaa_Mohamed_Fayez {"X-Amz-Date"
2 2024-10-08T18:19:53Z AROAUIAATNQLGCYGOZGAU:user3354961=Hanaa_Mohamed_Fayez {"X-Amz-Date"
teams.live.com is sharing your screen.
Stop sharing
Hide
CloudShell
Feedback
Privacy
Terms
Cookie preferences
Type here to search
9:52 PM
10/8/2024

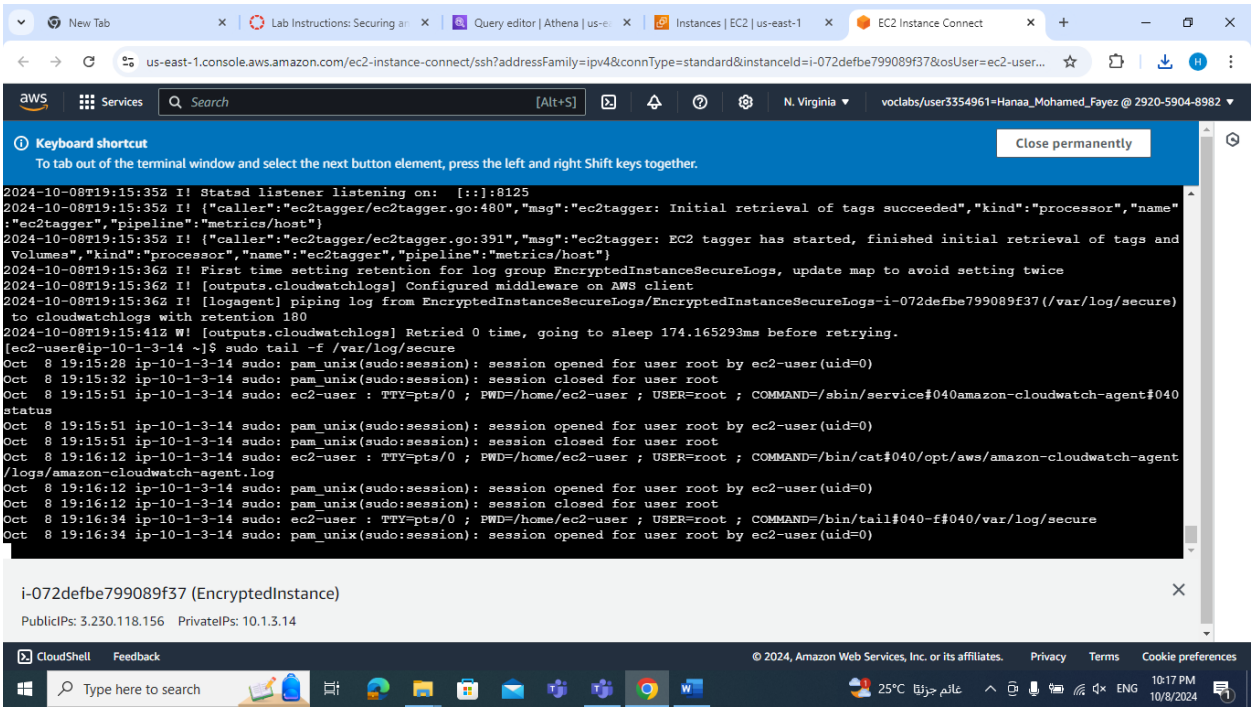

us-east-1.console.aws.amazon.com/athena/home?region=us-east-1#/query-editor/history/b7aedbf7-dcb6-48bc-885f-f08d8bcf4ea1
Data
Data source
AwsDataCatalog
Database
default
Tables and views
Create
Filter tables and views
Tables (1)
cloudtrail_logs_cloudtrail_logs_0c2aa8f53f0f94f04
Views (0)
Query 1
Query 2
Query 3
SELECT eventtime, useridentity.principalid, requestparameters, eventname,sourceipaddress, useragent
FROM cloudtrail_logs_cloudtrail_logs_0c2aa8f53f0f94f04
WHERE
eventname in ('GetObject') AND
requestparameters LIKE '%customer-data.csv%'
limit 10
SQL Ln 1, Col 1
Run again
Explain
Cancel
Clear
Create
Reuse query results
up to 60 minutes ago
Query results
Query stats
Completed
Time in queue: 106 ms
Run time: 870 ms
Data scanned: 367.73 KB
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
9:46 PM
10/10/2024

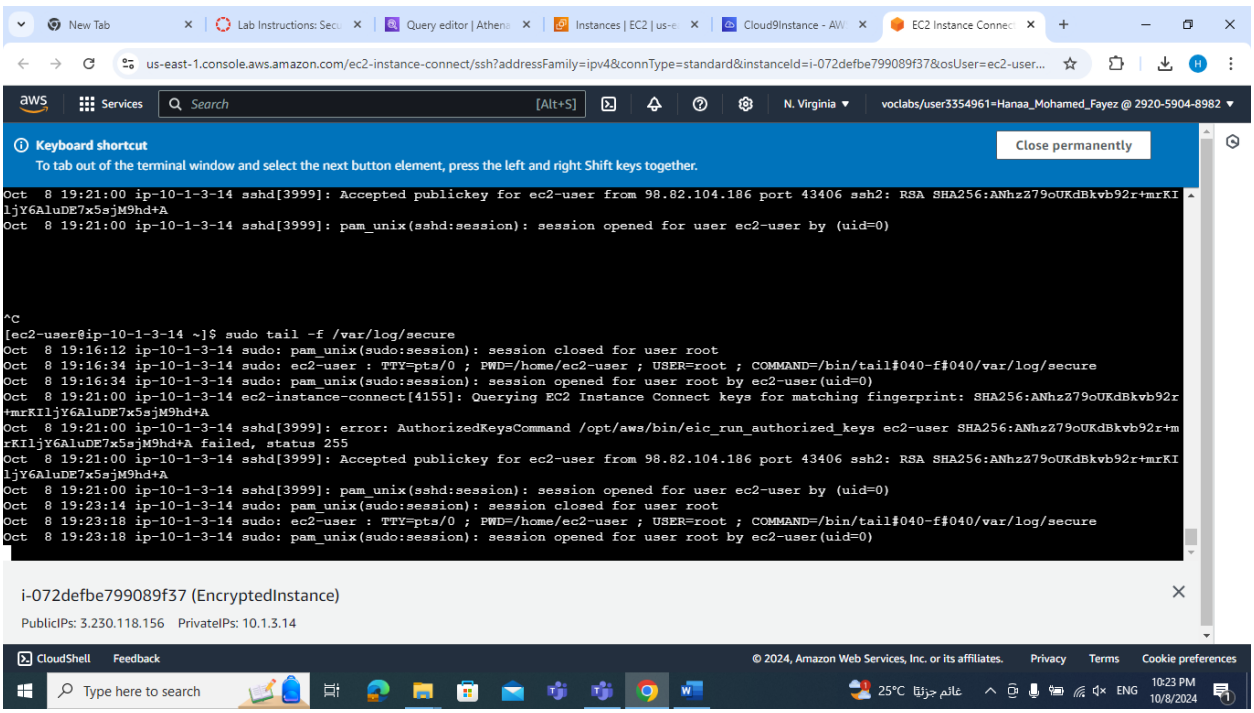


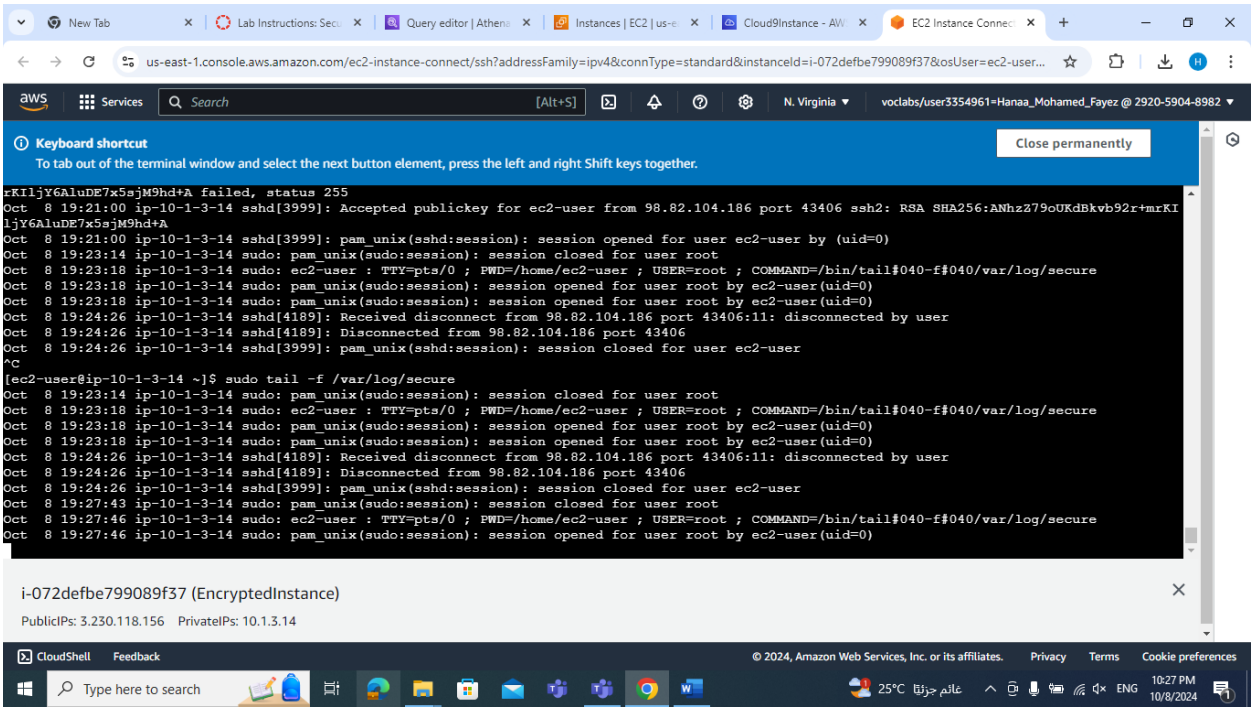
Task 4.2: Use CloudWatch Logs to monitor secure logs

Create a CloudWatch log group named EncryptedInstanceSecureLogs with all default settings.

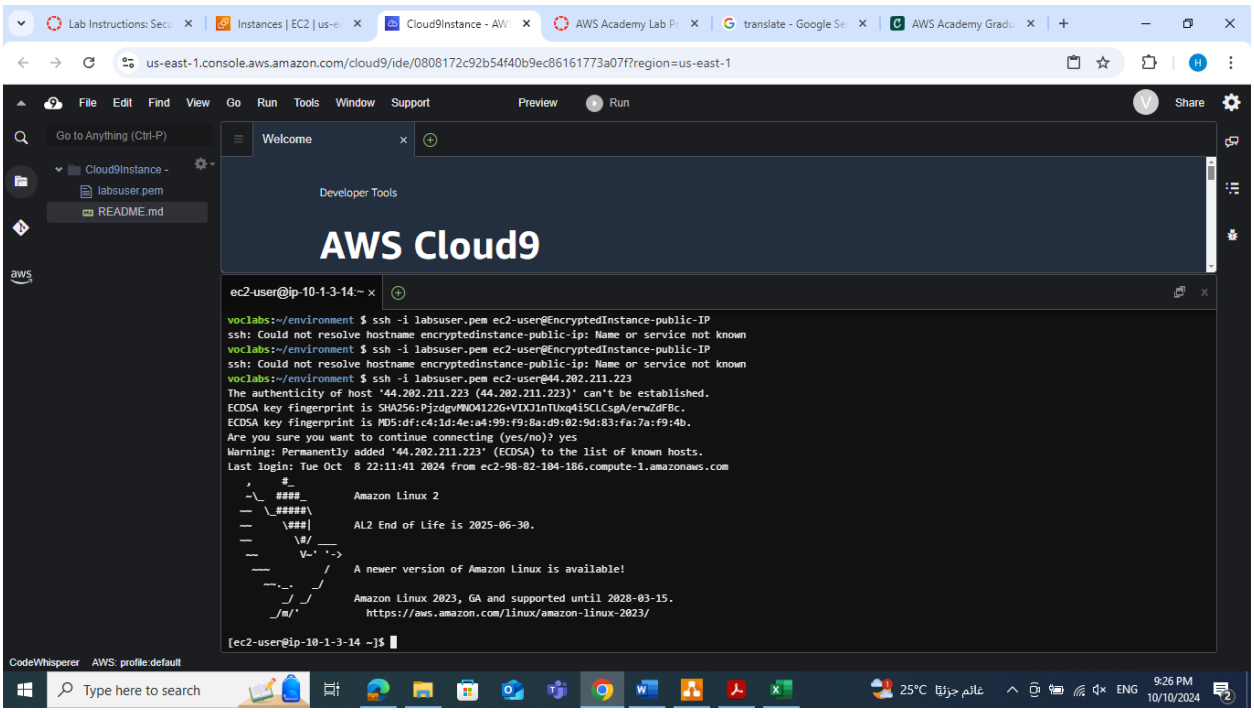


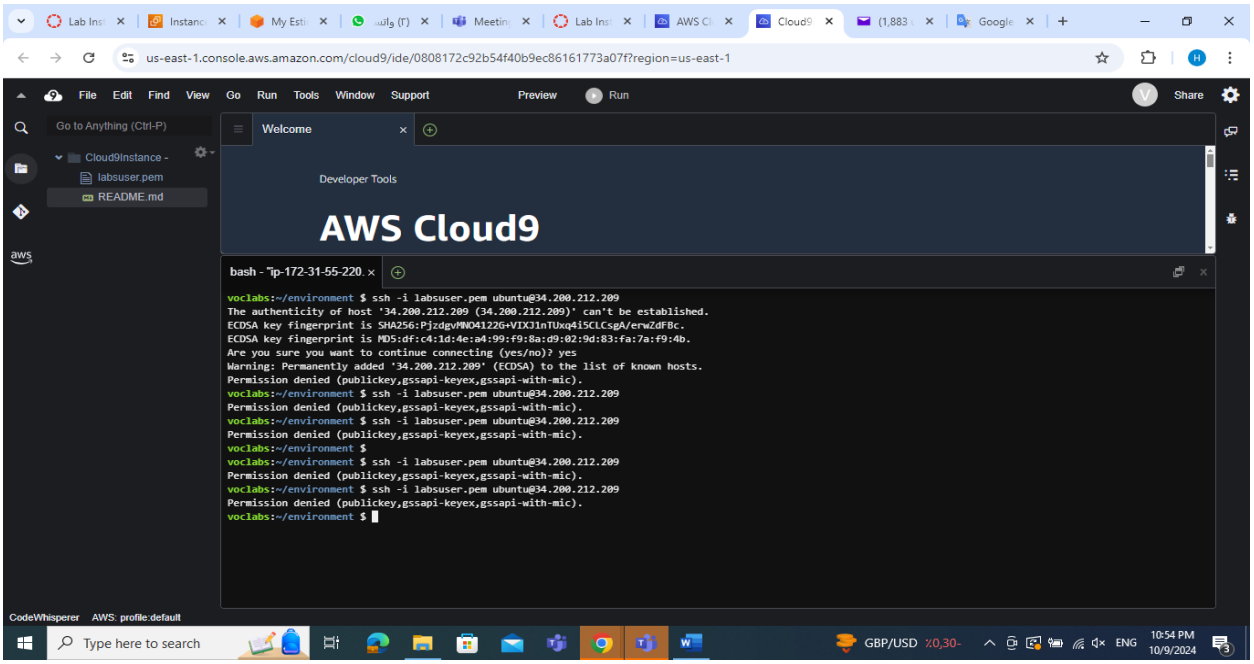

New Tab
Lab Instructions: Securing ar
Query editor | Athena | us-e
Instances | EC2 | us-east-1
EC2 Instance Connect
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?addressFamily=ipv4&connType=standard&instanceId=i-072defbe799089f37&osUser=ec2-user...
aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3354961=Hanaa_Mohamed_Fayez @ 2920-5904-8982
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
2024-10-08T19:15:35Z I! Statsd listener listening on: [::]:8125
2024-10-08T19:15:35Z I! {"caller":"ec2tagger/ec2tagger.go:480","msg":"ec2tagger: Initial retrieval of tags succeeded","kind":"processor","name":"ec2tagger","pipeline":"metrics/host"}
2024-10-08T19:15:35Z I! {"caller":"ec2tagger/ec2tagger.go:391","msg":"ec2tagger: EC2 tagger has started, finished initial retrieval of tags and Volumes","kind":"processor","name":"ec2tagger","pipeline":"metrics/host"}
2024-10-08T19:15:36Z I! First time setting retention for log group EncryptedInstanceSecureLogs, update map to avoid setting twice
2024-10-08T19:15:36Z I! [outputs.cloudwatchlogs] Configured middleware on AWS client
2024-10-08T19:15:36Z I! [logagent] piping log from EncryptedInstanceSecureLogs/EncryptedInstanceSecureLogs-i-072defbe799089f37 (/var/log/secure) to cloudwatchlogs with retention 180
2024-10-08T19:15:41Z W! [outputs.cloudwatchlogs] Retried 0 time, going to sleep 174.165293ms before retrying.
[ec2-user@ip-10-1-3-14 ~]$ sudo tail -f /var/log/secure
Oct 8 19:15:28 ip-10-1-3-14 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Oct 8 19:15:32 ip-10-1-3-14 sudo: pam_unix(sudo:session): session closed for user root
Oct 8 19:15:51 ip-10-1-3-14 sudo: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/sbin/service#040amazon-cloudwatch-agent#040status
Oct 8 19:15:51 ip-10-1-3-14 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Oct 8 19:15:51 ip-10-1-3-14 sudo: pam_unix(sudo:session): session closed for user root
Oct 8 19:16:12 ip-10-1-3-14 sudo: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/cat#040/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log
Oct 8 19:16:12 ip-10-1-3-14 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Oct 8 19:16:12 ip-10-1-3-14 sudo: pam_unix(sudo:session): session closed for user root
Oct 8 19:16:34 ip-10-1-3-14 sudo: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/tail#040-f#040/var/log/secure
Oct 8 19:16:34 ip-10-1-3-14 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
i-072defbe799089f37 (EncryptedInstance)
PublicIPs: 3.230.118.156 PrivateIPs: 10.1.3.14
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
25°C
ENG
10:17 PM
10/8/2024


New Tab
Lab Instructions: Secu
Query editor | Athena
Instances | EC2 | us-e
Cloud9Instance - AW
EC2 Instance Connec
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?addressFamily=ipv4&connType=standard&instanceId=i-072defbe799089f37&osUser=ec2-user...
aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3354961=Hanaa_Mohamed_Fayez @ 2920-5904-8982
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
Oct 8 19:21:00 ip-10-1-3-14 sshd[3999]: Accepted publickey for ec2-user from 98.82.104.186 port 43406 ssh2: RSA SHA256:ANhz279oUKdBkvb92r+mrKIljY6AluDE7x5sjM9hd+A
Oct 8 19:21:00 ip-10-1-3-14 sshd[3999]: pam_unix(sshd:session): session opened for user ec2-user by (uid=0)
^C
[ec2-user@ip-10-1-3-14 ~]$ sudo tail -f /var/log/secure
Oct 8 19:16:12 ip-10-1-3-14 sudo: pam_unix(sudo:session): session closed for user root
Oct 8 19:16:34 ip-10-1-3-14 sudo: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/tail#040-f#040/var/log/secure
Oct 8 19:16:34 ip-10-1-3-14 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Oct 8 19:21:00 ip-10-1-3-14 ec2-instance-connect[4155]: Querying EC2 Instance Connect keys for matching fingerprint: SHA256:ANhz279oUKdBkvb92r+mrKIljY6AluDE7x5sjM9hd+A
Oct 8 19:21:00 ip-10-1-3-14 sshd[3999]: error: AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys ec2-user SHA256:ANhz279oUKdBkvb92r+mrKIljY6AluDE7x5sjM9hd+A failed, status 255
Oct 8 19:21:00 ip-10-1-3-14 sshd[3999]: Accepted publickey for ec2-user from 98.82.104.186 port 43406 ssh2: RSA SHA256:ANhz279oUKdBkvb92r+mrKIljY6AluDE7x5sjM9hd+A
Oct 8 19:21:00 ip-10-1-3-14 sshd[3999]: pam_unix(sshd:session): session opened for user ec2-user by (uid=0)
Oct 8 19:23:14 ip-10-1-3-14 sudo: pam_unix(sudo:session): session closed for user root
Oct 8 19:23:18 ip-10-1-3-14 sudo: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/tail#040-f#040/var/log/secure
Oct 8 19:23:18 ip-10-1-3-14 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
i-072defbe799089f37 (EncryptedInstance)
PublicIPs: 3.230.118.156 PrivateIPs: 10.1.3.14
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
25°C
ENG
10:23 PM
10/8/2024

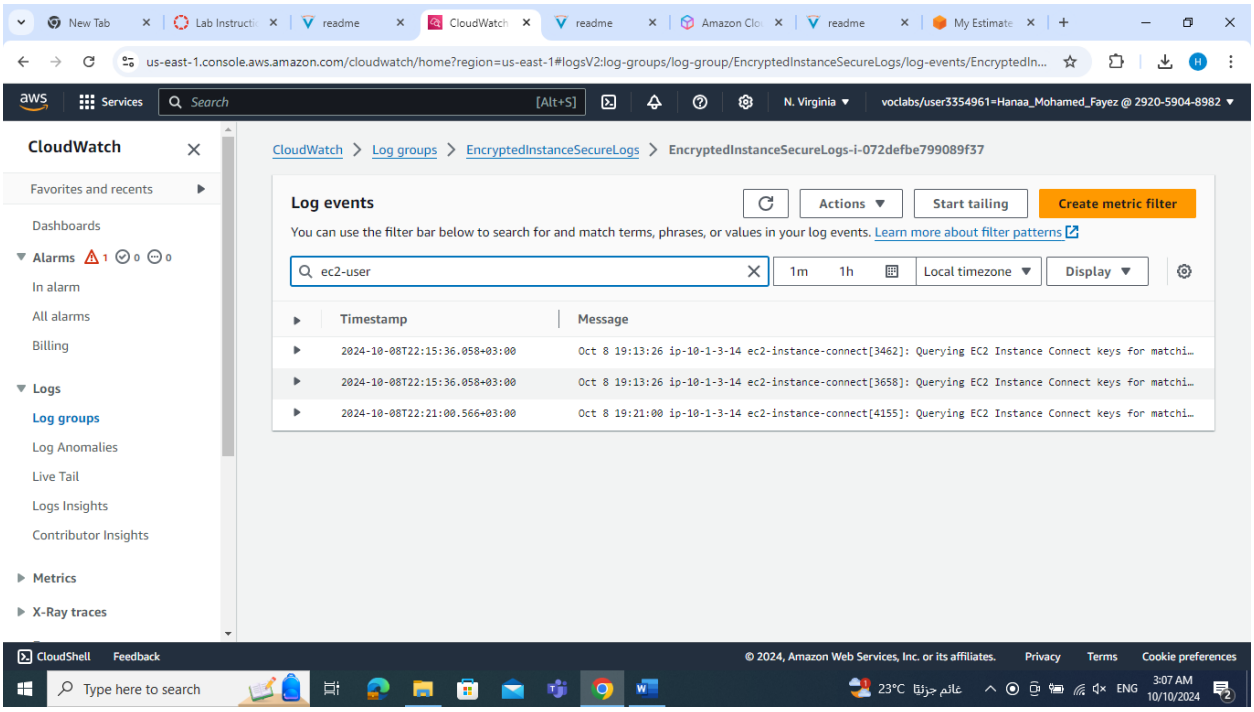


Create some security logs by successfully connecting and then failing to connect to the *EncryptedInstance* over SSH from your AWS Cloud9 IDE.



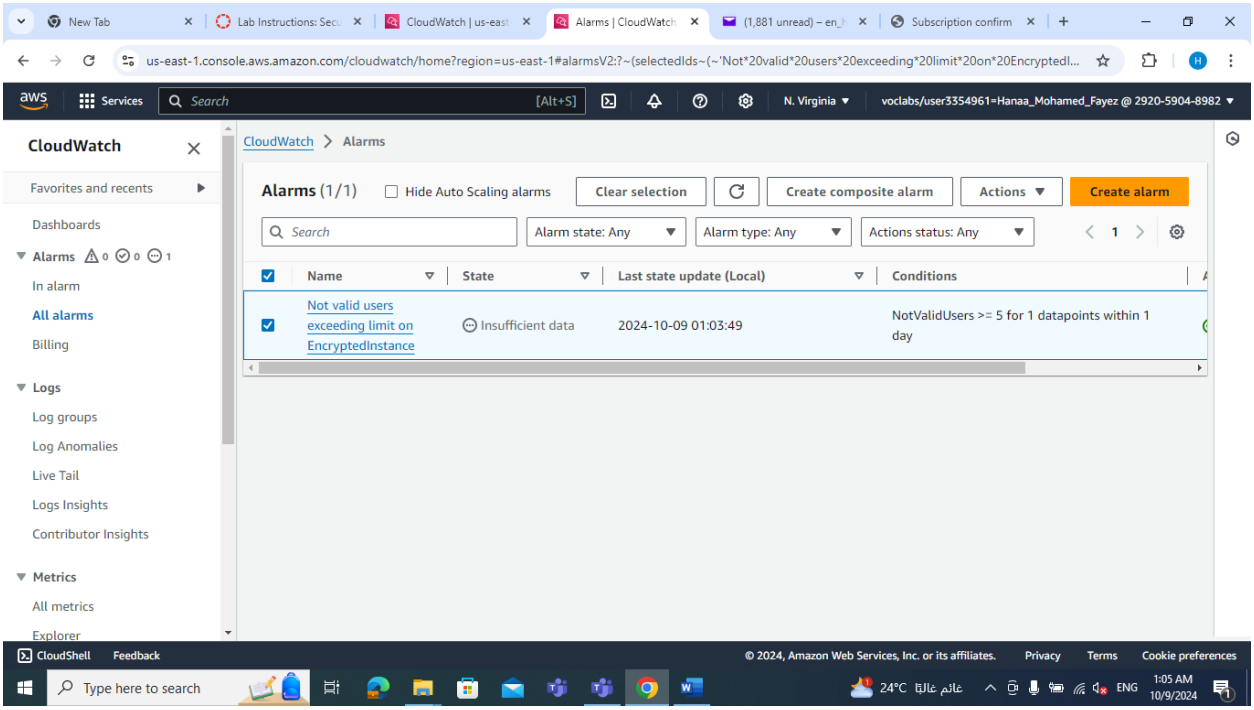


Verify that the secure logs are being written to the CloudWatch log group

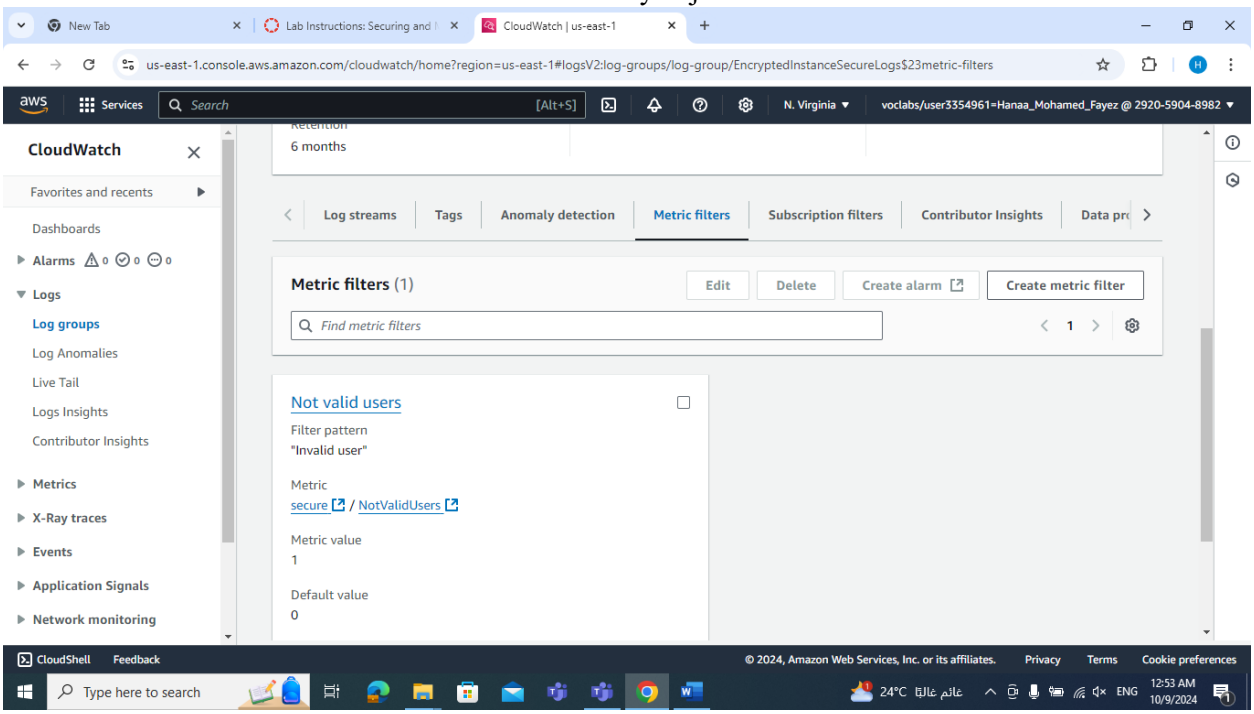


Task 4.3: Create a CloudWatch alarm to send notifications for security incidents

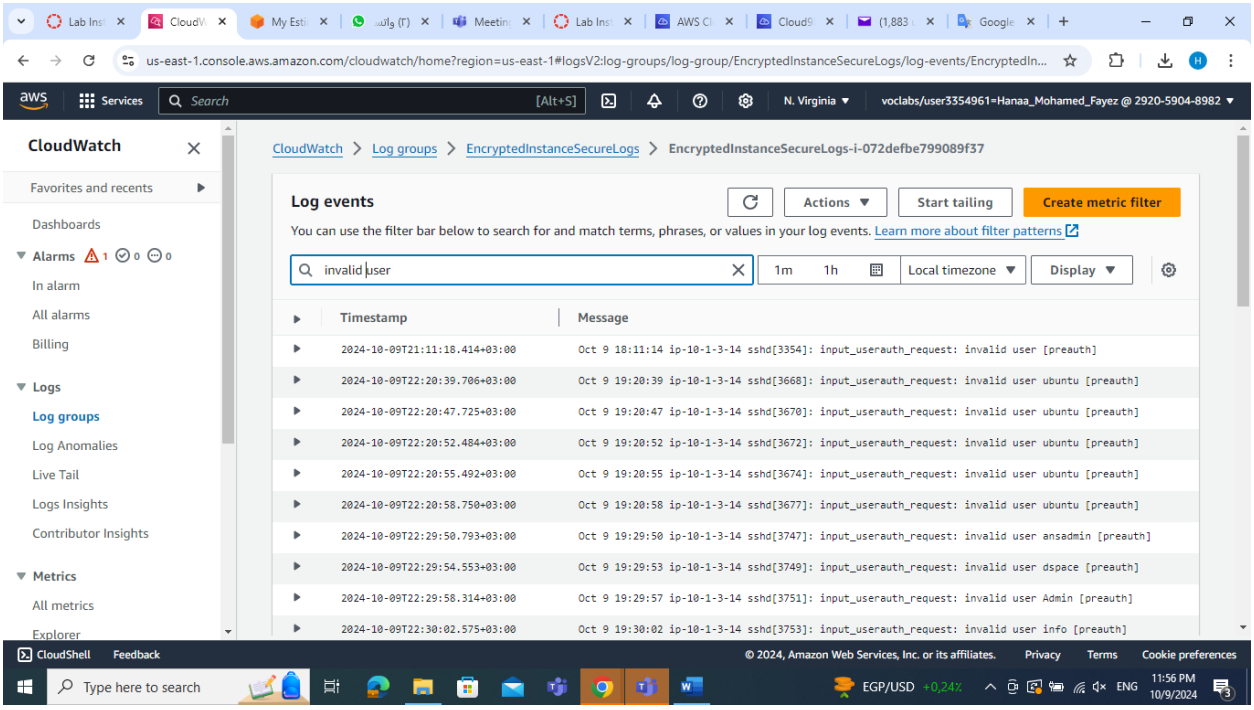
Go to the *EncryptedInstanceSecureLogs* CloudWatch log group



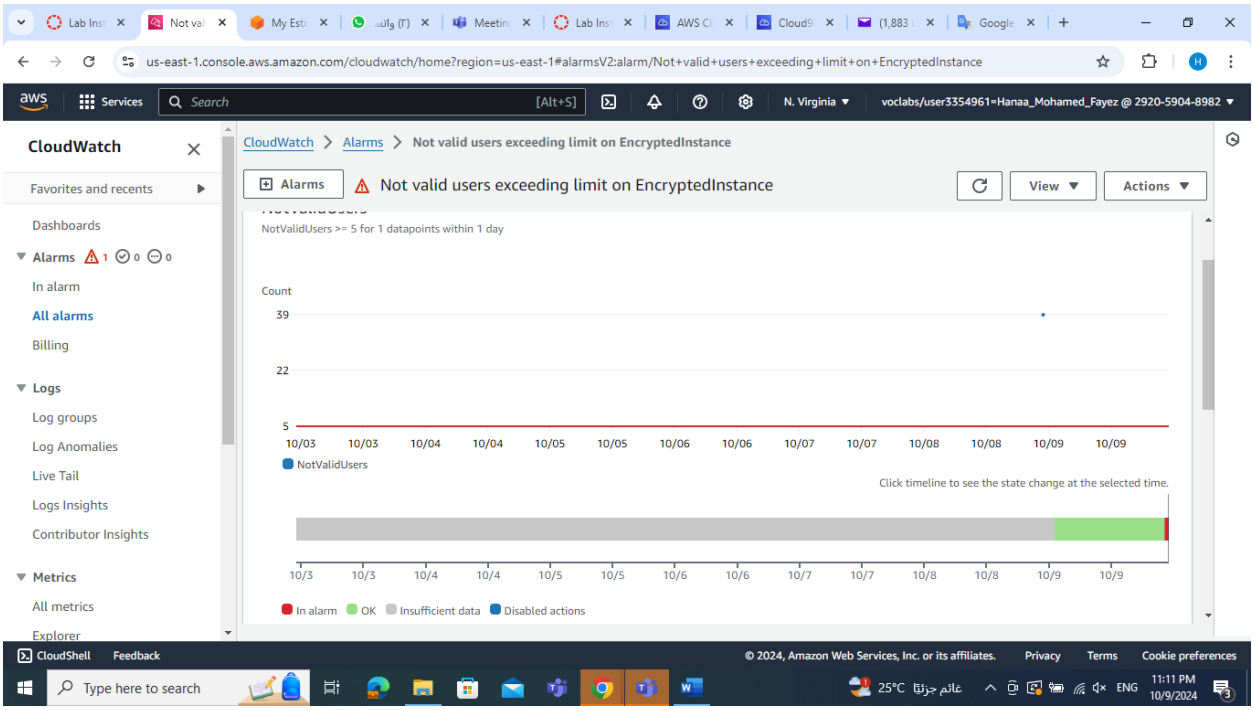
Create a CloudWatch alarm from the metric filter that you just created

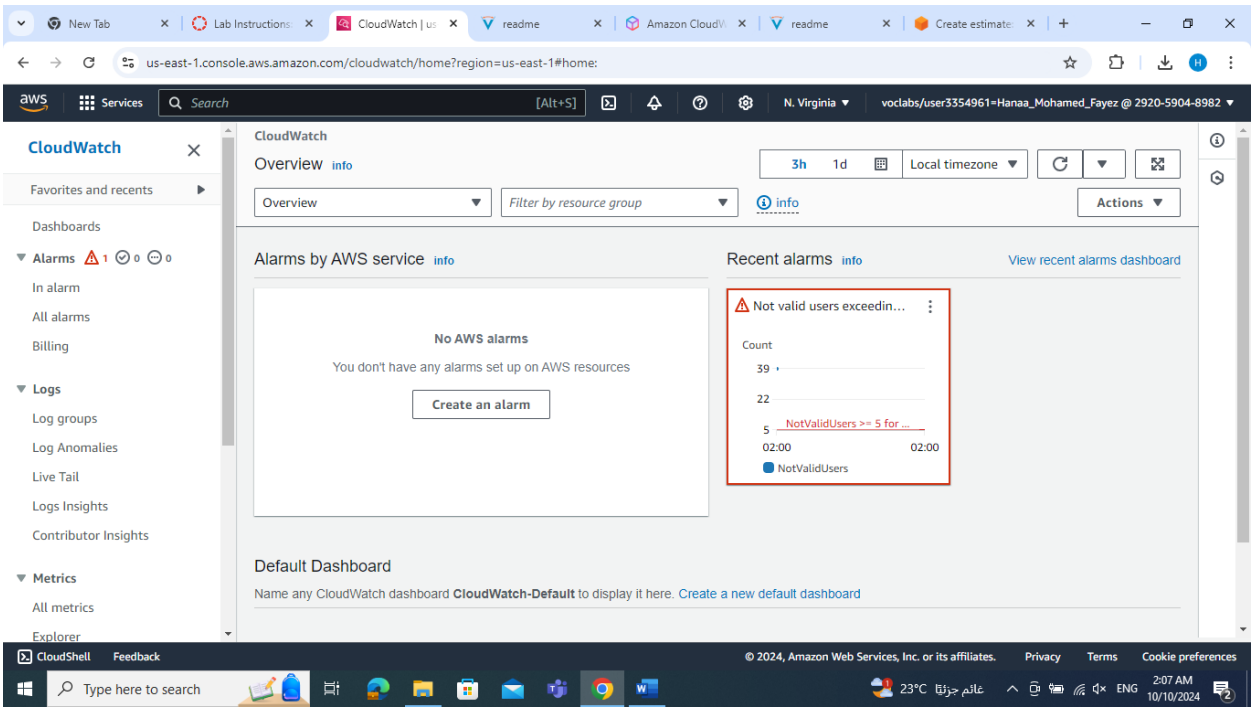


In the CloudWatch console, in the latest log stream for the *EncryptedInstanceSecureLogs* log group, filter the log events for Invalid user

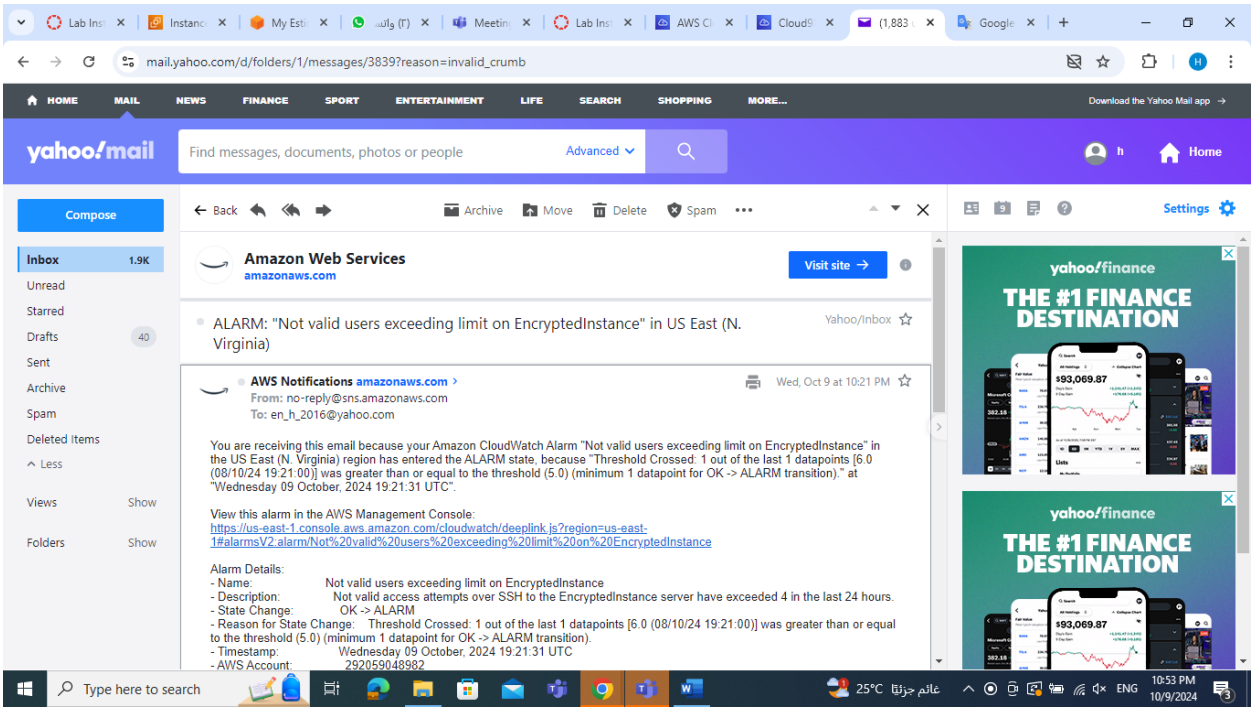


In the Alarms area of the CloudWatch console, confirm that the *Invalid users* alarm has a state of *In alarm*



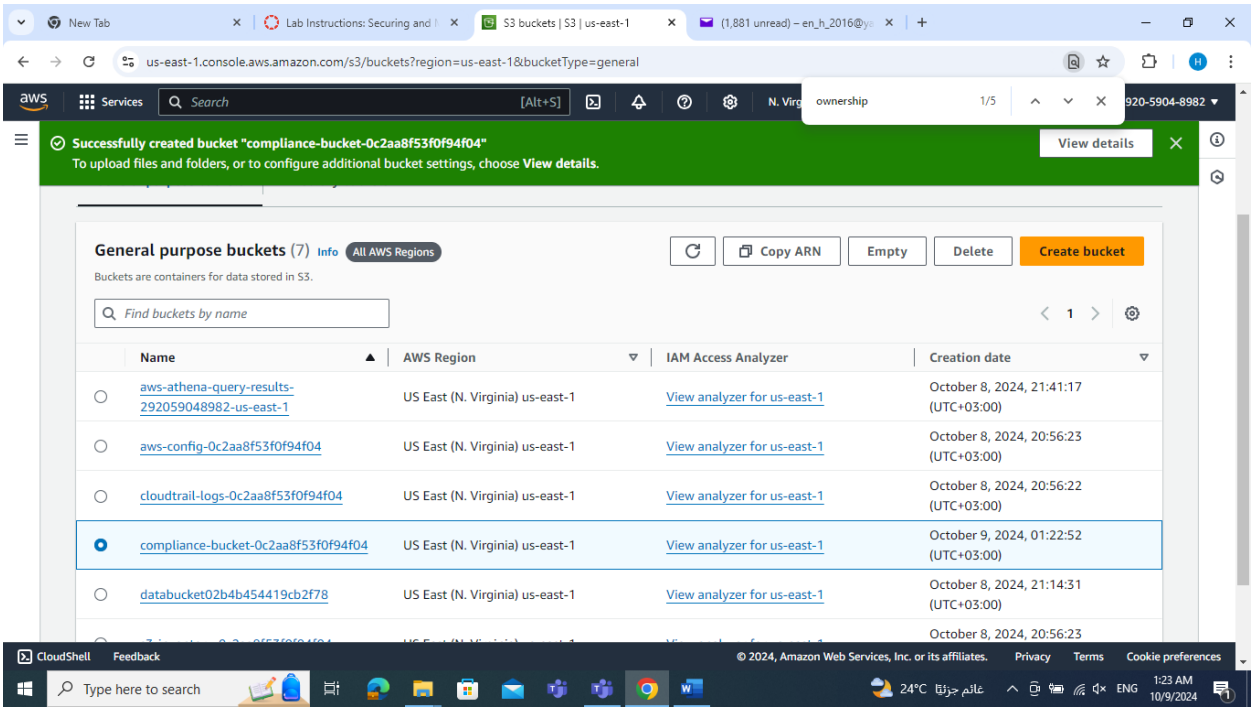


Go to the inbox for the email address

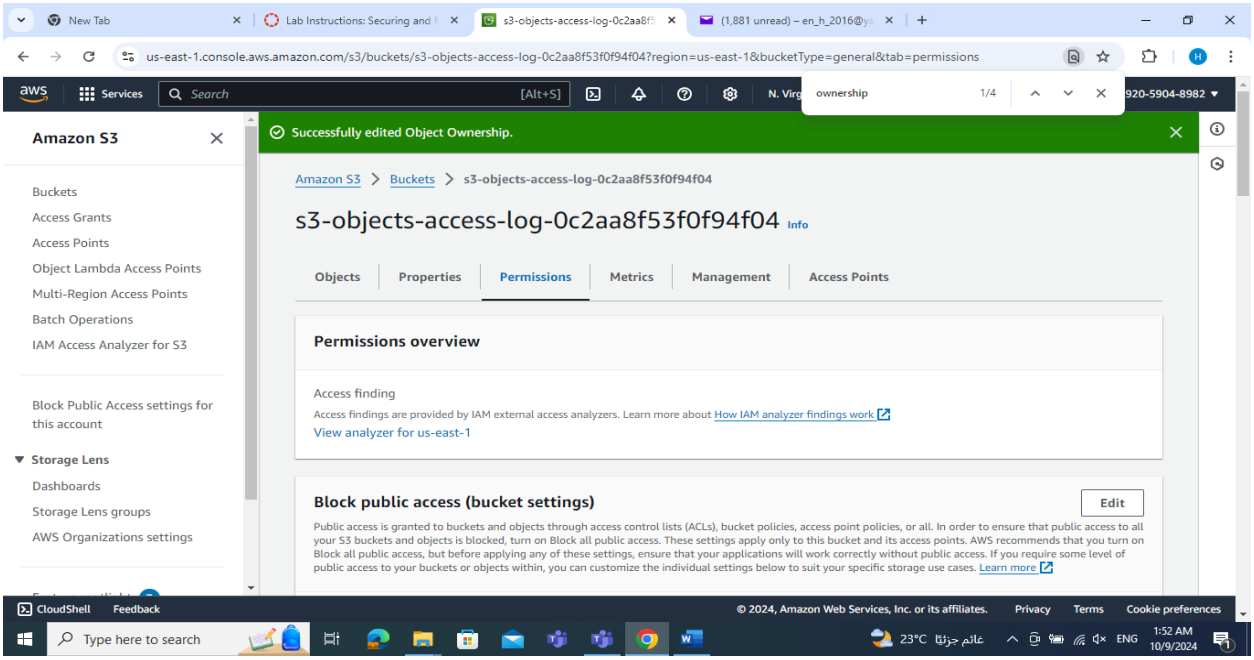


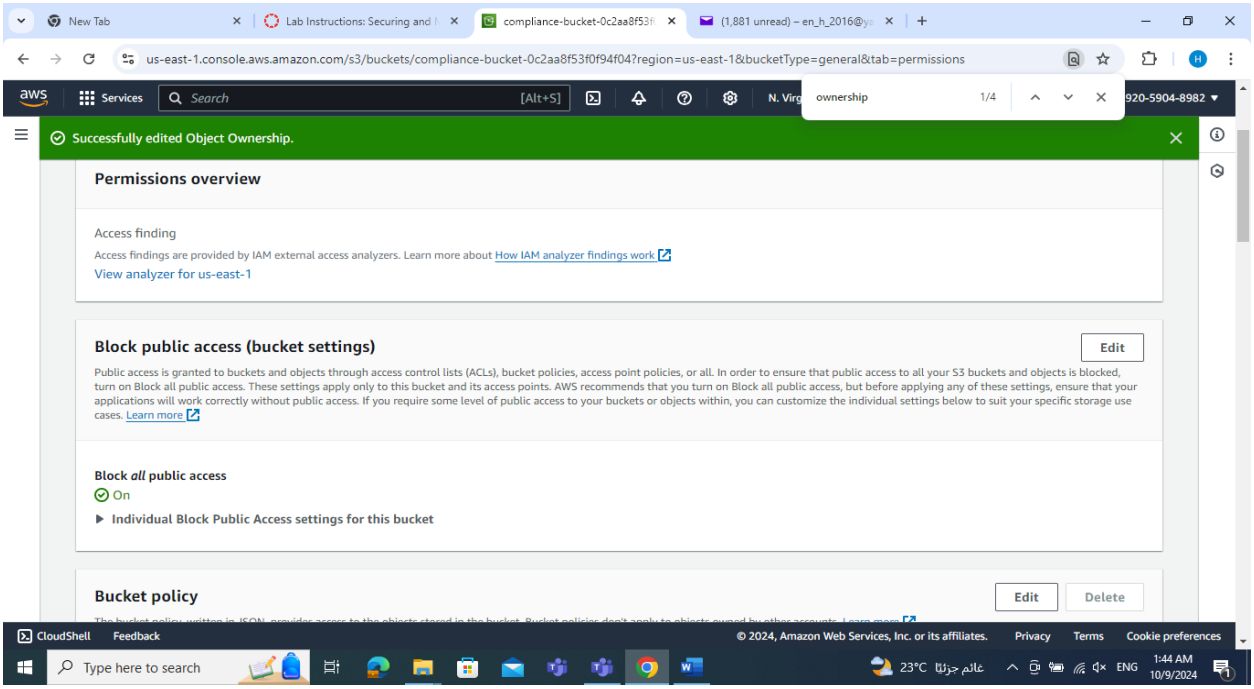
Task 4.4: Configure AWS Config to assess security settings and remediate the configuration of AWS resources

Create a new S3 bucket named compliance-bucket-unique-ID

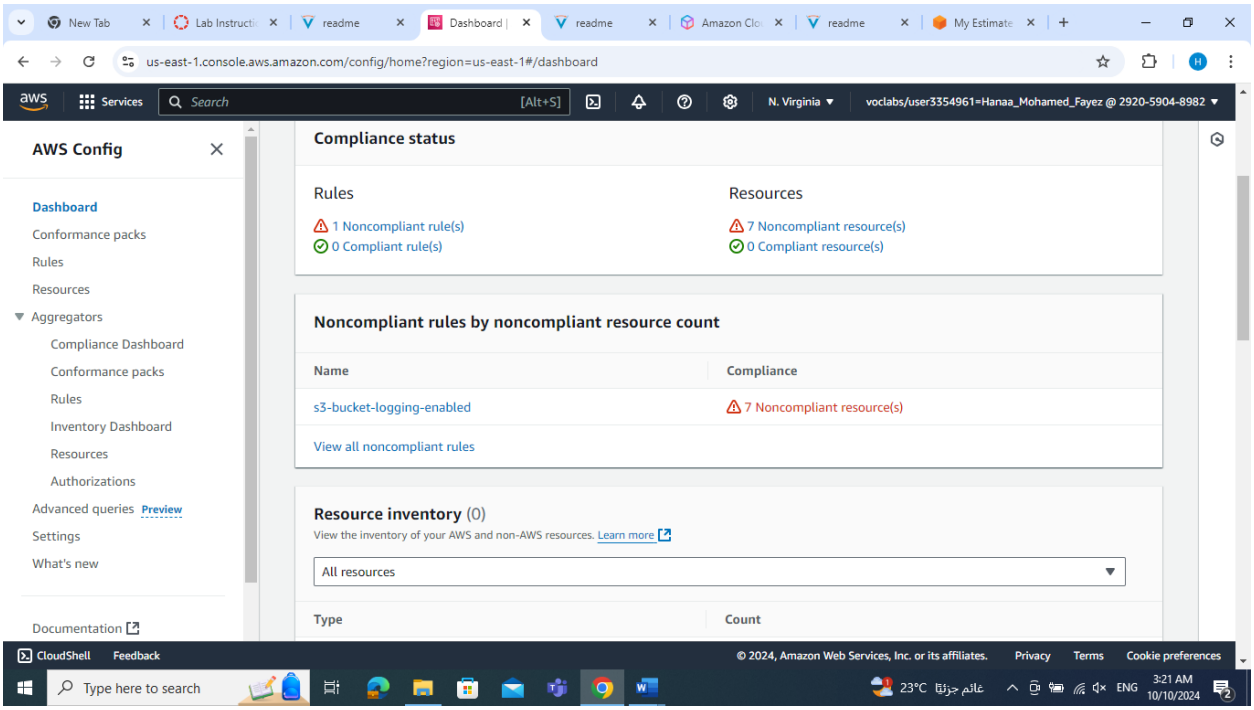


Enable object ownership on the *s3-objects-access-log* bucket

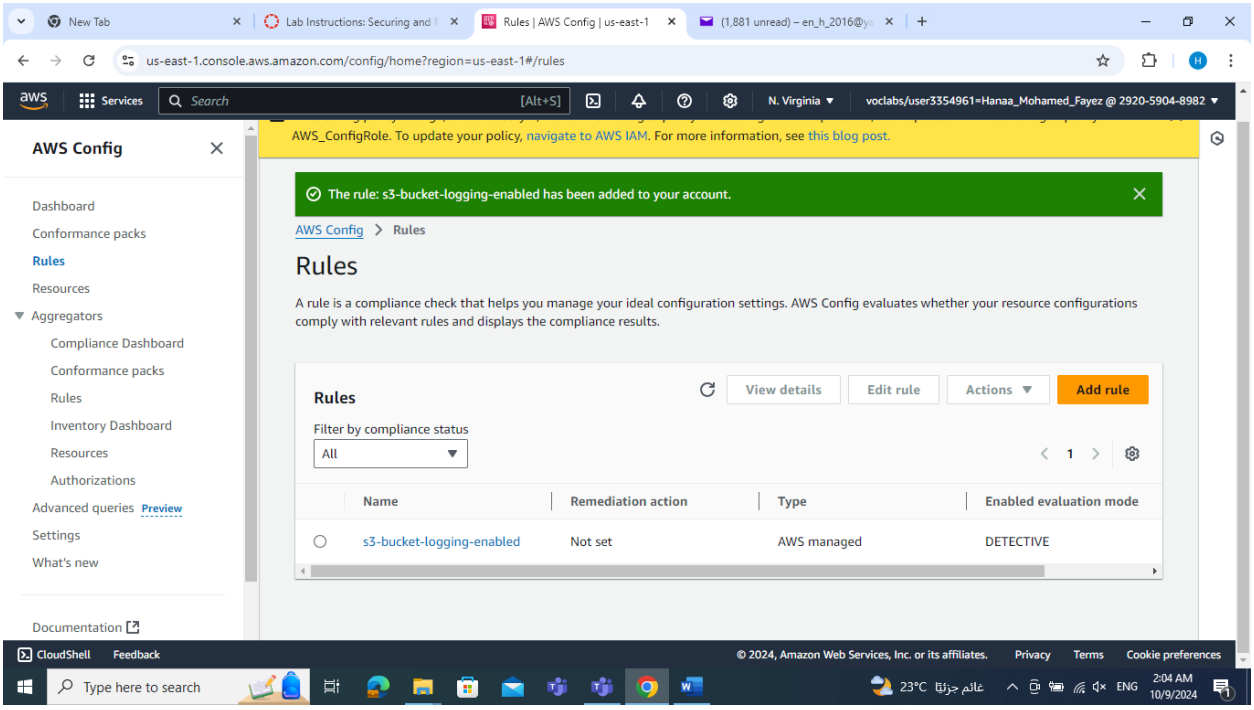




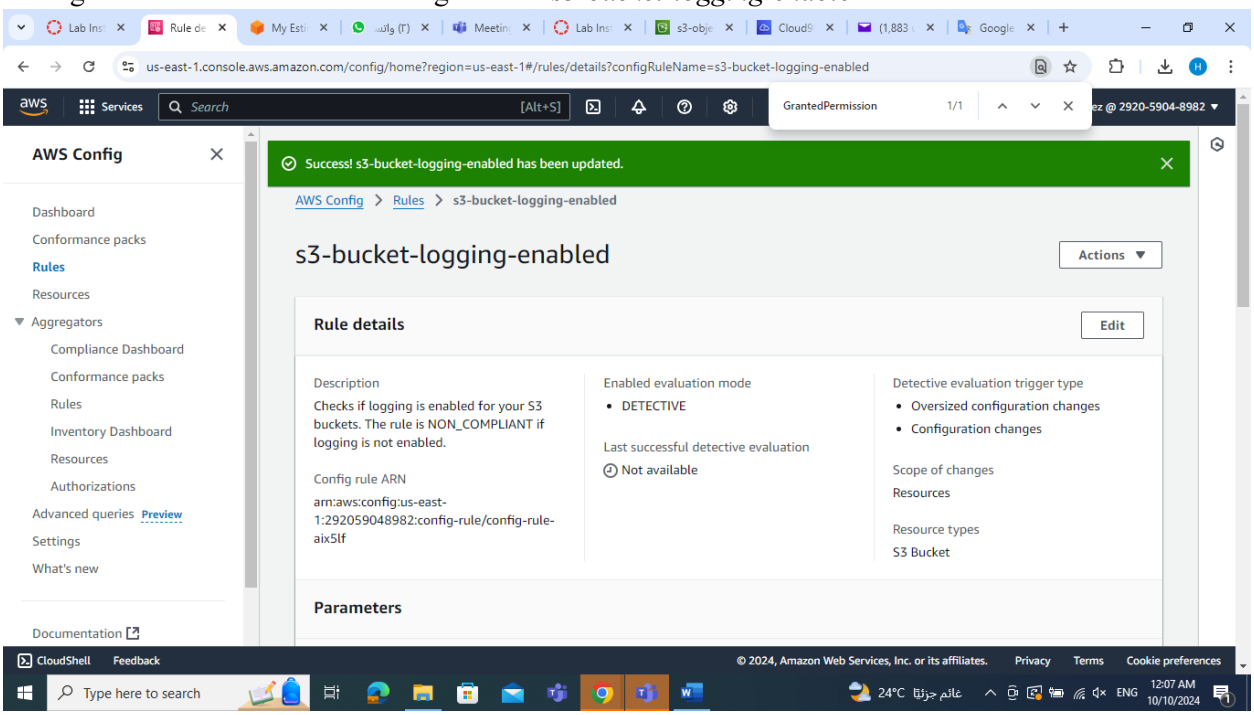
Navigate to the AWS Config console, and choose **Get started**

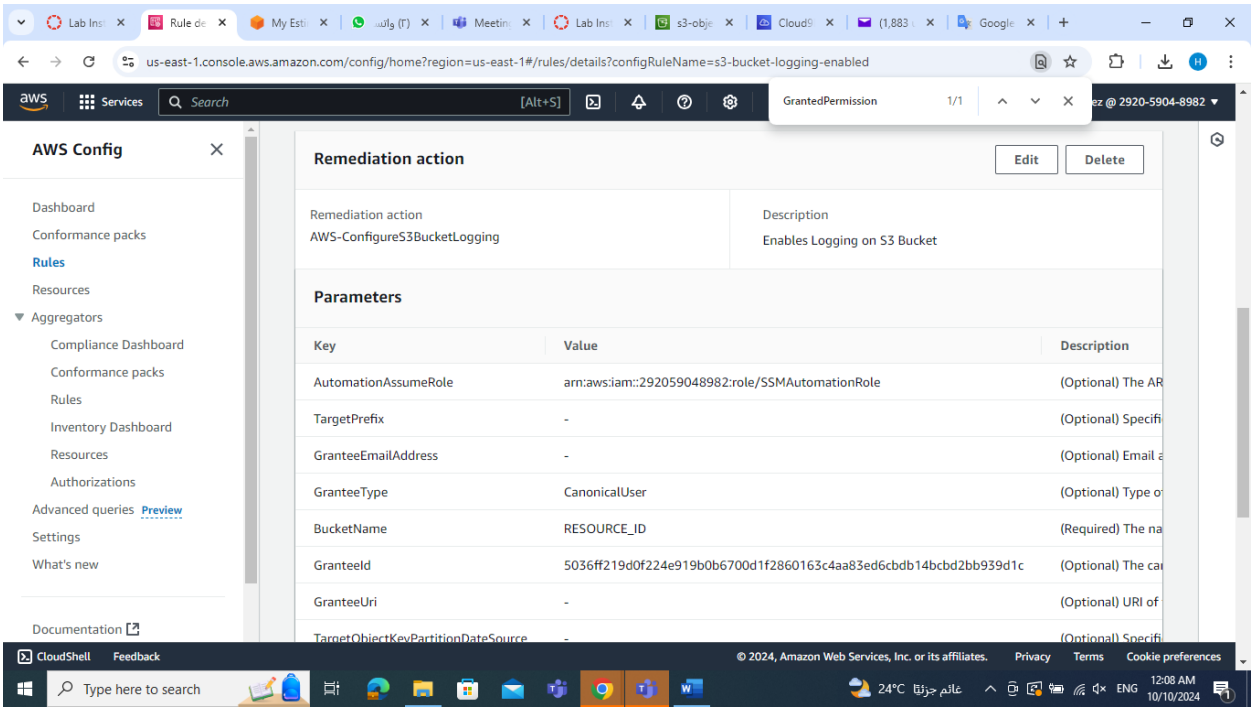


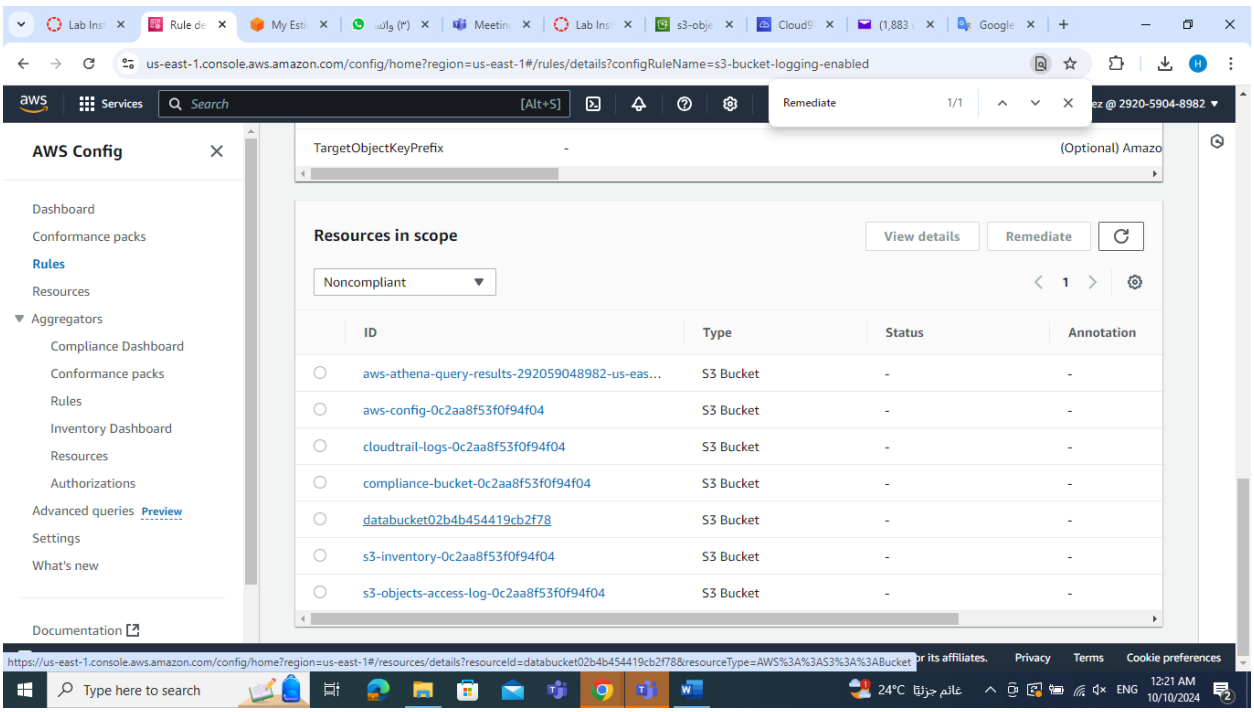
In the AWS Config console, add an AWS managed rule



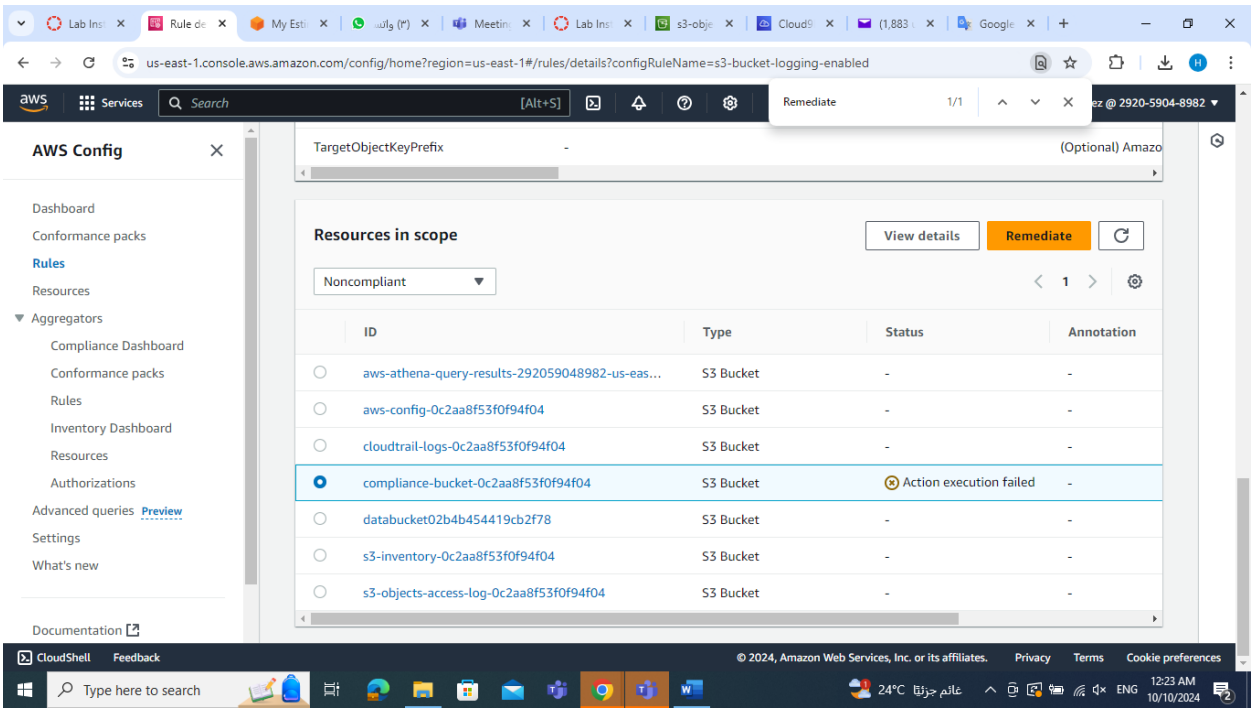
Configure manual remediation settings for the *s3-bucket-logging-enable* rule



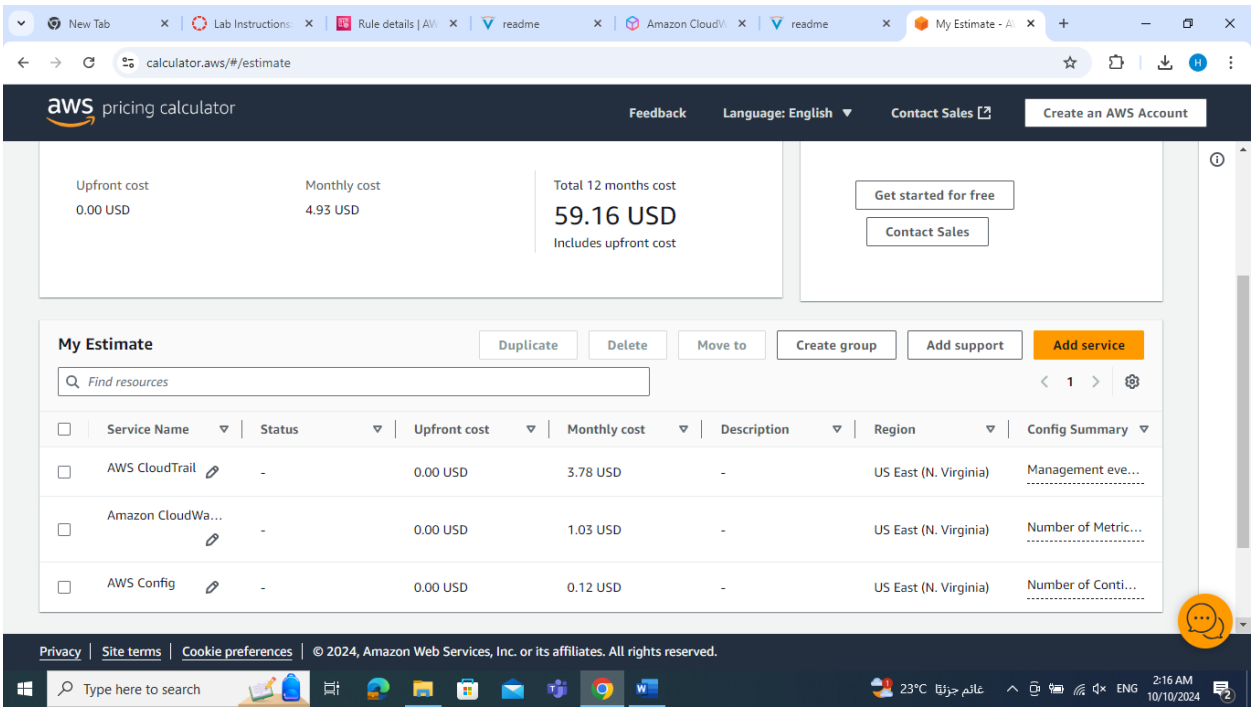

us-east-1.console.aws.amazon.com/config/home?region=us-east-1#/rules/details?configRuleName=s3-bucket-logging-enabled
Services
Search
[Alt+S]
GrantedPermission
1/1
AWS Config
Dashboard
Conformance packs
Rules
Resources
Aggregators
Compliance Dashboard
Conformance packs
Rules
Inventory Dashboard
Resources
Authorizations
Advanced queries Preview
Settings
What's new
Documentation
Remediation action
Edit
Delete
Remediation action
AWS-ConfigureS3BucketLogging
Description
Enables Logging on S3 Bucket
Parameters
Key
Value
Description
AutomationAssumeRole
arn:aws:iam::292059048982:role/SSMAutomationRole
(Optional) The AR
TargetPrefix
-
(Optional) Specifi
GranteeEmailAddress
-
(Optional) Email a
GranteeType
CanonicalUser
(Optional) Type o
BucketName
RESOURCE_ID
(Required) The na
GranteeId
5036ff219d0f224e919b0b6700d1f2860163c4aa83ed6cbdb14bcbd2bb939d1c
(Optional) The ca
GranteeUri
-
(Optional) URI of
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
12:08 AM
10/10/2024

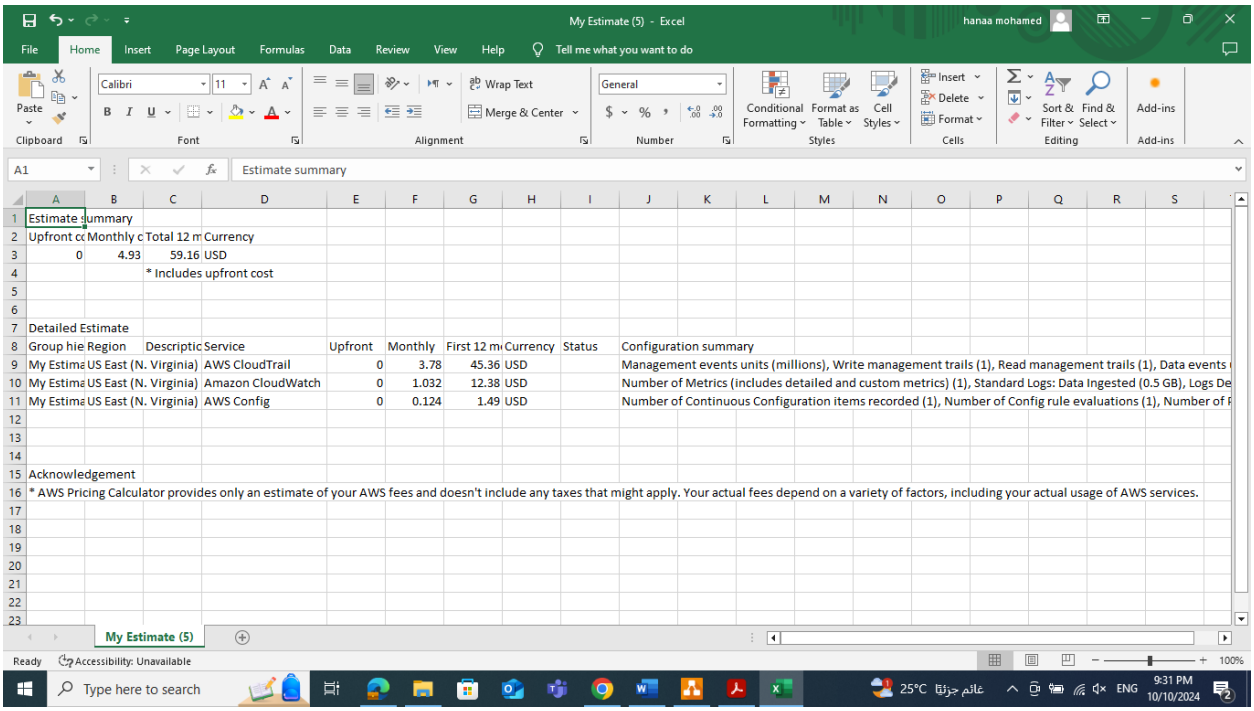

us-east-1.console.aws.amazon.com/config/home?region=us-east-1#/rules/details?configRuleName=s3-bucket-logging-enabled
Services
Search
[Alt+S]
Remediate
1/1
AWS Config
TargetObjectKeyPrefix
-
(Optional) Amazo
Resources in scope
View details
Remediate
Noncompliant
1
ID
Type
Status
Annotation
aws-athena-query-results-292059048982-us-eas...
S3 Bucket
aws-config-0c2aa8f53f0f94f04
S3 Bucket
cloudtrail-logs-0c2aa8f53f0f94f04
S3 Bucket
compliance-bucket-0c2aa8f53f0f94f04
S3 Bucket
databucket02b4b454419cb2f78
S3 Bucket
s3-inventory-0c2aa8f53f0f94f04
S3 Bucket
s3-objects-access-log-0c2aa8f53f0f94f04
S3 Bucket
https://us-east-1.console.aws.amazon.com/config/home?region=us-east-1#/resources/details?resourceId=databucket02b4b454419cb2f78&resourceType=AWS%3A%3AS3%3A%3ABucket
Privacy
Terms
Cookie preferences
Type here to search
12:21 AM
10/10/2024

Invoke the AWS Config remediation action so that object logging is enabled on the *compliance-bucket*



Estimate cost of CloudTrail, CloudWatch, and AWS Config

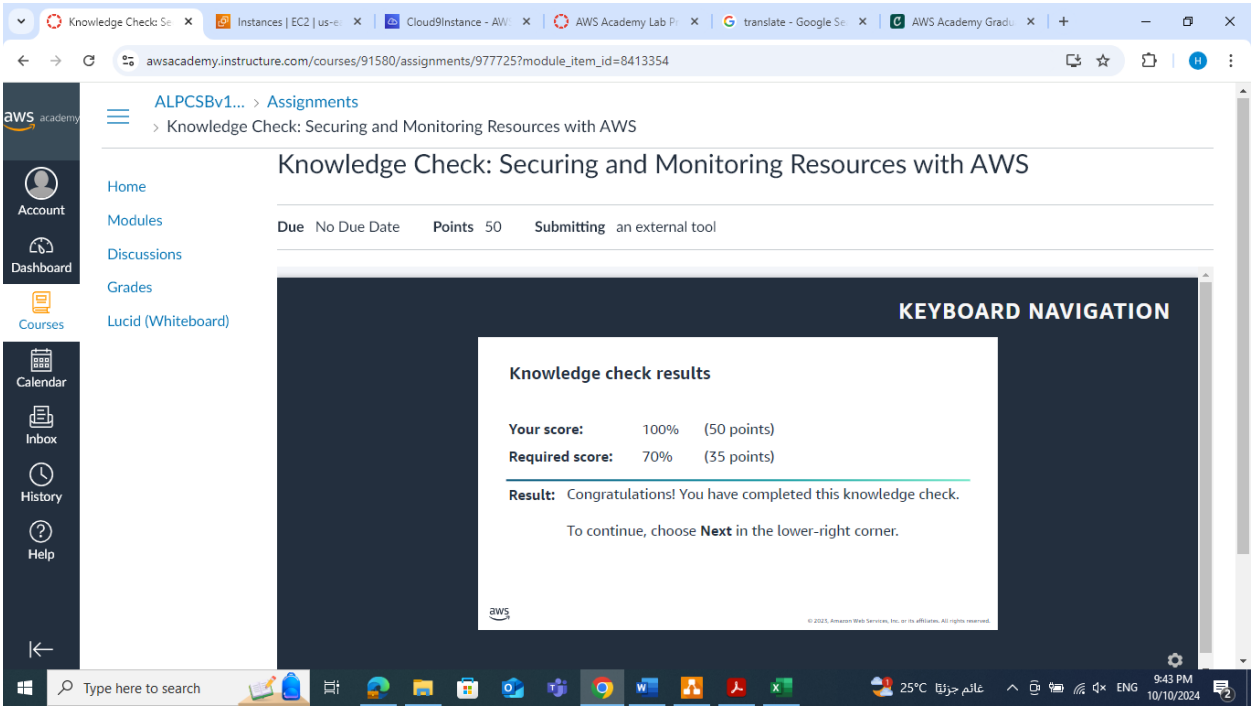




My Estimate (5) - Excel

hanaa mohamed

	A	B	C	D	E	F	G	H	I	J
1	Estimate summary									
2	Upfront co	Monthly c	Total 12 m	Currency						
3	0	4.93	59.16	USD						
4			* Includes upfront cost							
5										
6										
7	Detailed Estimate									
8	Group hie	Region	Descriptic	Service	Upfront	Monthly	First 12 m	Currency	Status	Configuration summary
9	My Estima	US East (N. Virginia)		AWS CloudTrail	0	3.78	45.36	USD		Management events units (millions), Write management trails (1), Read management trails (1), Data events
10	My Estima	US East (N. Virginia)		Amazon CloudWatch	0	1.032	12.38	USD		Number of Metrics (includes detailed and custom metrics) (1), Standard Logs: Data Ingested (0.5 GB), Logs De
11	My Estima	US East (N. Virginia)		AWS Config	0	0.124	1.49	USD		Number of Continuous Configuration items recorded (1), Number of Config rule evaluations (1), Number of
12										
13										
14										
15	Acknowledgement									
16	* 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.									



awsacademy.instructure.com/courses/91580/assignments/977725?module_item_id=8413354

ALPCSBv1... > Assignments

> Knowledge Check: Securing and Monitoring Resources with AWS

Knowledge Check: Securing and Monitoring Resources with AWS

Due No Due Date Points 50 Submitting an external tool

KEYBOARD NAVIGATION

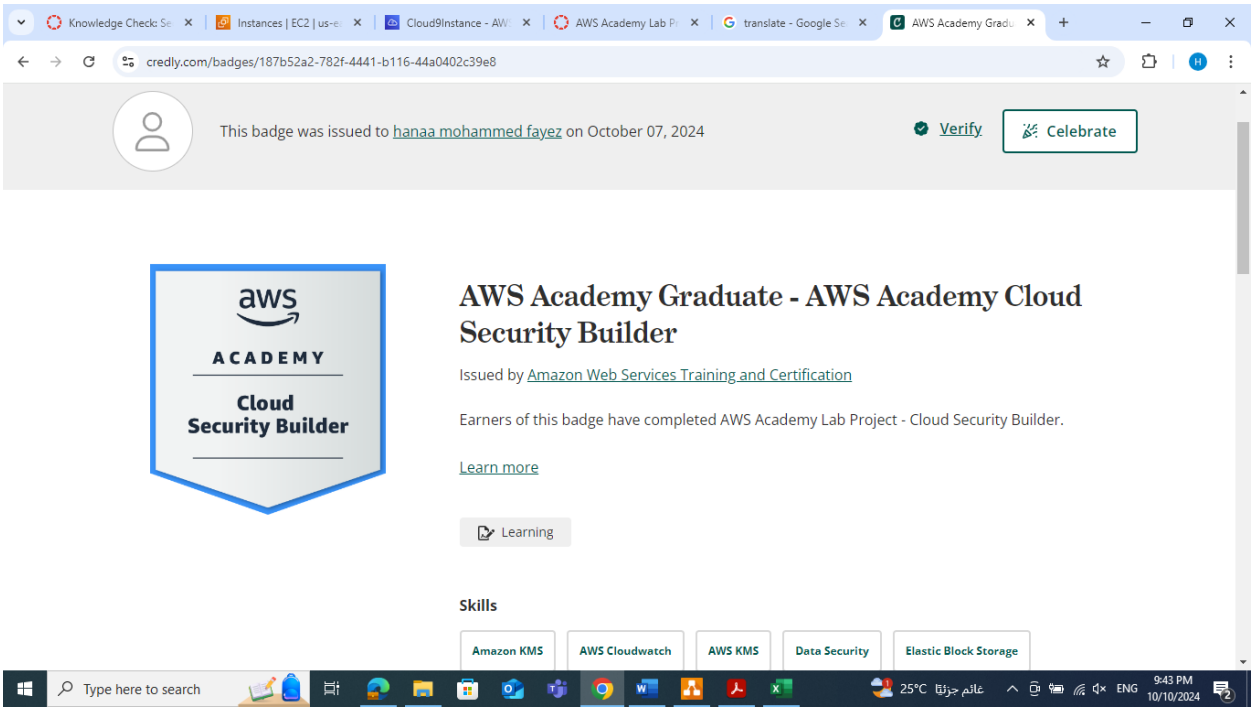
Knowledge check results

Your score: 100% (50 points)

Required score: 70% (35 points)

Result: Congratulations! You have completed this knowledge check.

To continue, choose **Next** in the lower-right corner.


credly.com/badges/187b52a2-782f-4441-b116-44a0402c39e8
This badge was issued to hanaa mohammed fayez on October 07, 2024
Verify
Celebrate
aws
ACADEMY
Cloud Security Builder
AWS Academy Graduate - AWS Academy Cloud Security Builder
Issued by Amazon Web Services Training and Certification
Earners of this badge have completed AWS Academy Lab Project - Cloud Security Builder.
Learn more
Learning
Skills
Amazon KMS
AWS Cloudwatch
AWS KMS
Data Security
Elastic Block Storage
Type here to search
25°C
ENG
9:43 PM
10/10/2024