Securing and Monitoring Resources with AWS

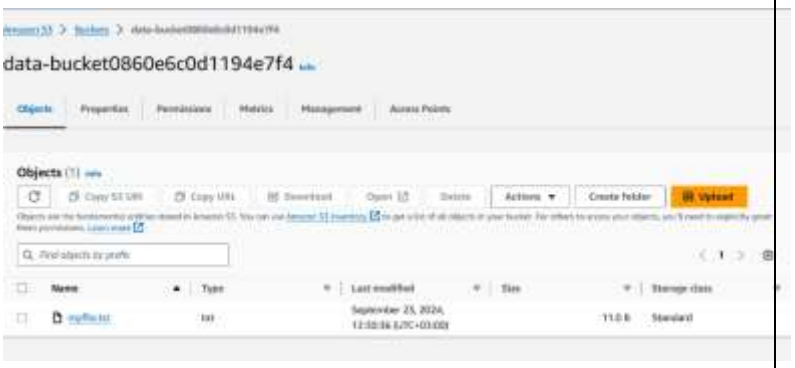
Salma Mohamed Mohamed Kassem

AWS Solution Architect and Admin Track

Week1 : **Securing data in Amazon S3**

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

- ✓ Create a new S3 bucket.
- ✓ Apply a bucket policy that restricts access.
- ✓ Upload myfile.txt



Test access

Paulo

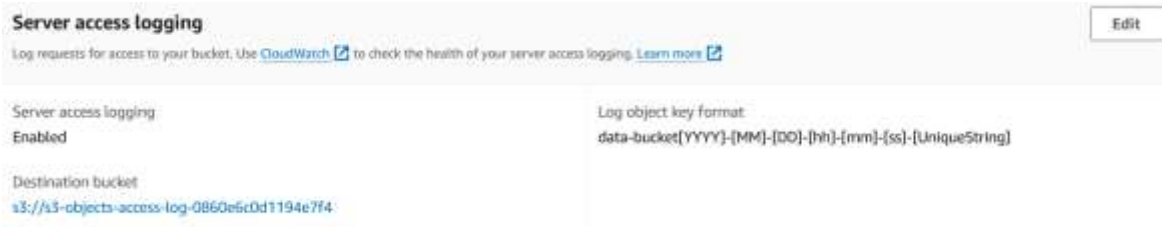
- Has access to data-bucket object and can download the file

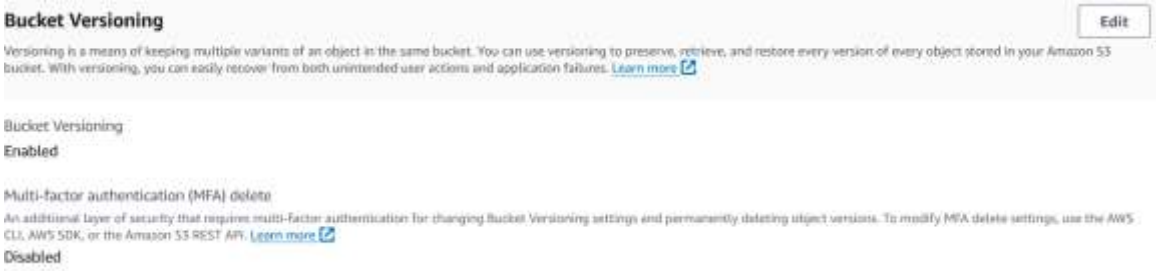
Mary

- Don’t have access to the data-bucket objects

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





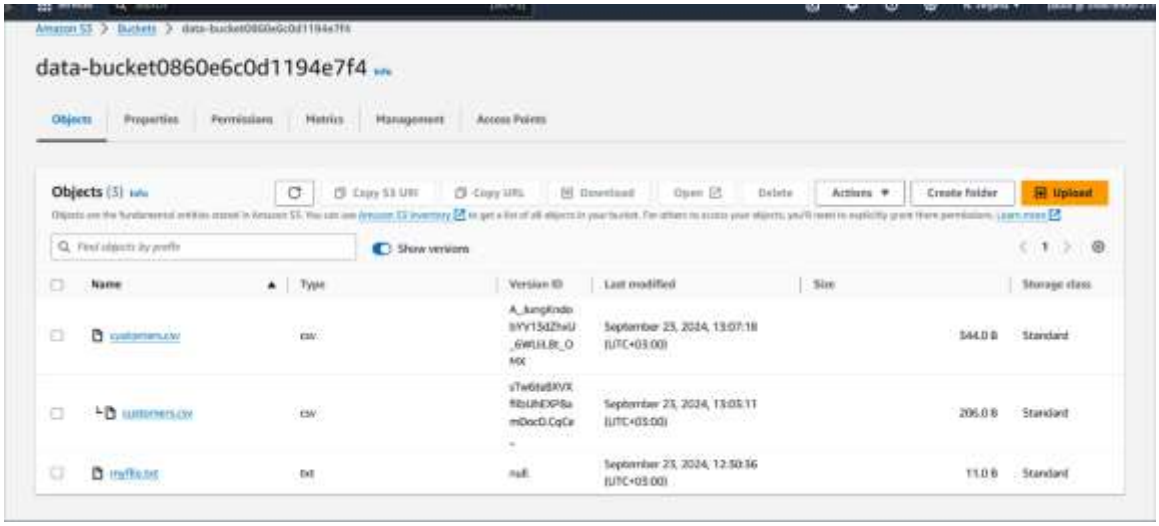
Task 1.3: Implement the S3 Inventory feature on a bucket

- ✓ Enable the S3 Inventory feature on the data-bucket

Task 1.4: Confirm that versioning works as intended

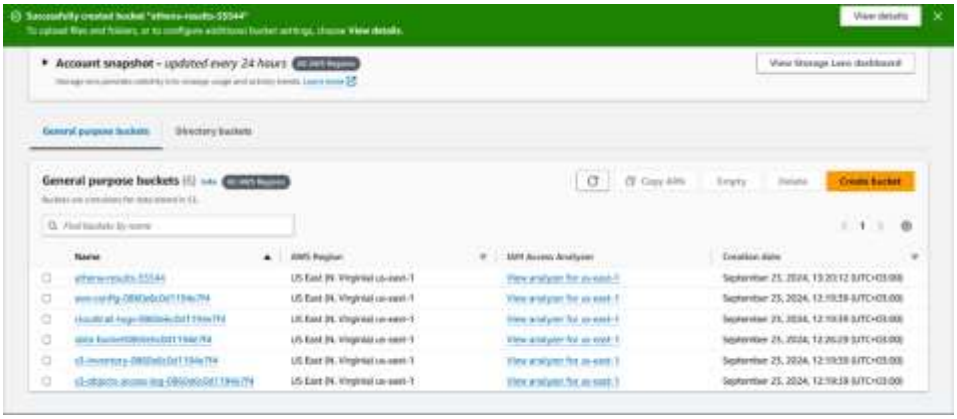
- ✓ On your computer, create a new file named customers.csv. Then, copy the following text to the file and save the changes
- ✓ Log in to the AWS account as the paulo user and upload the customers.csv file to the data-bucket
- ✓ Analyze how many versions of customer.csv exist by navigating to the customers.csv details page and choosing the Versions tab
- ✓ On your computer, edit the customers.csv file and add more data to it. For example, add the following two rows of data at the bottom of the file
- ✓ Login as Paulo : Paulo can access files

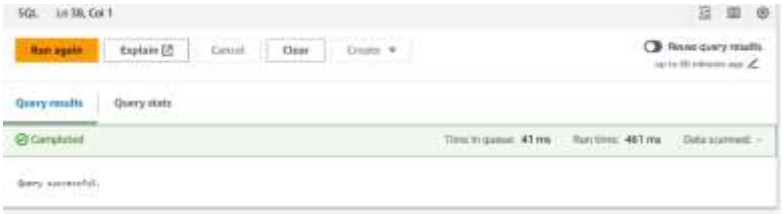
- Login as Mary : Mary cant access files



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

- ✓ Create an Athena table from the access logs
- ✓ In the Editor tab paste the following query into the query area
- ✓ Query the table to discover access details





Cost assessment to secure Amazon S3:-

Includes upfront cost

Upfront cost	Monthly cost	Total 12 months cost
0.01 USD	**21.42 USD**	**257.05 USD**

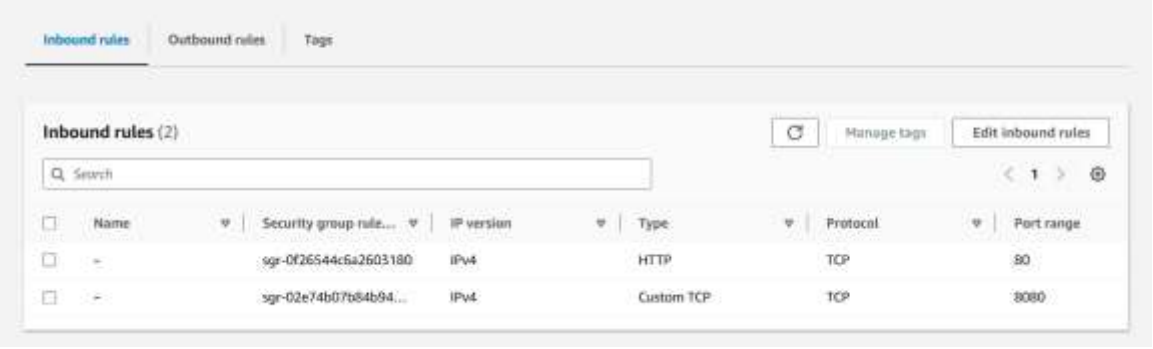
Week 2 : Securing VPCs

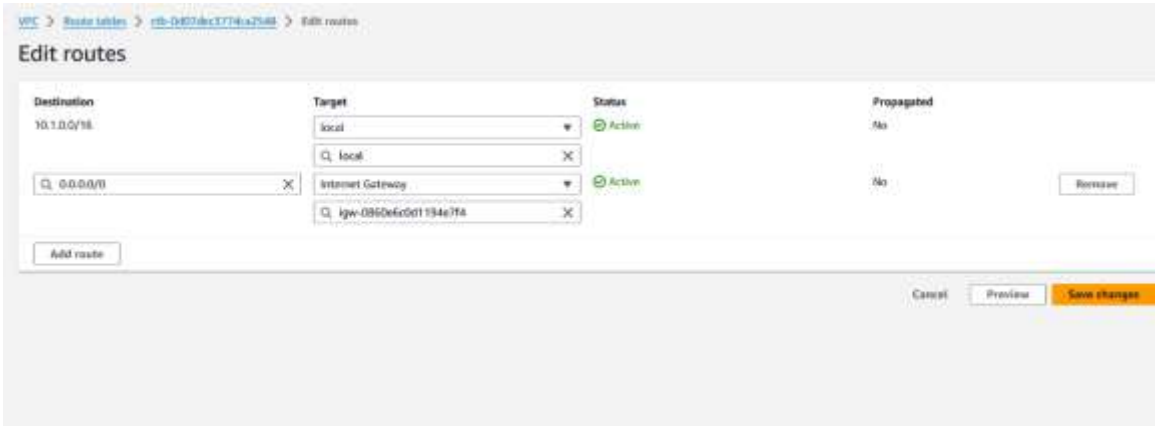
Task 2.1: Review LabVPC and its associated resources

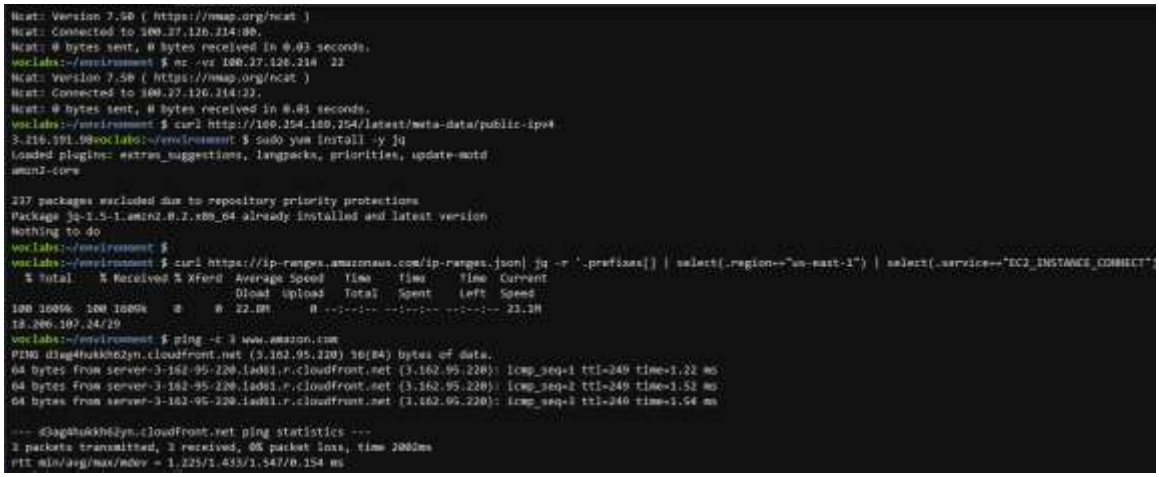
Task 2.2: Create a VPC flow log

Task 3.2: Access the WebServer instance from the internet and review VPC flow logs in CloudWatch

Task 2.4: Configure route table and security group settings







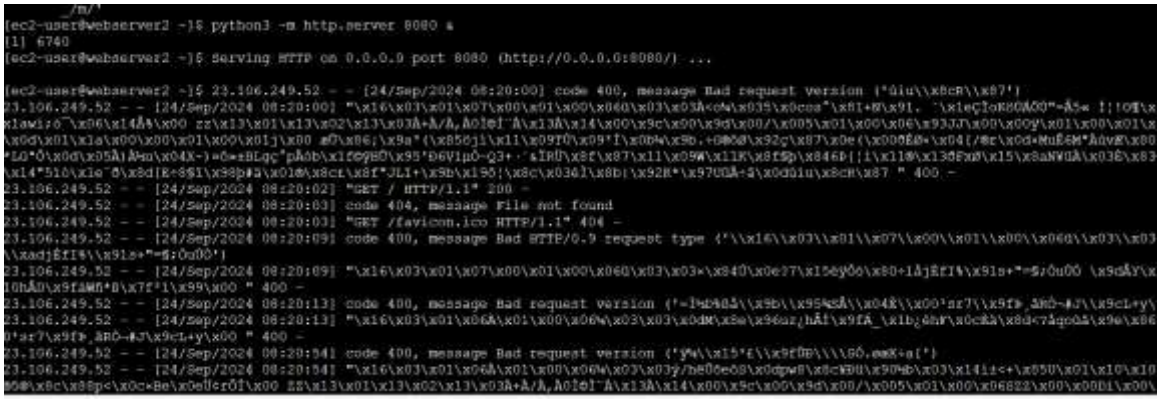
Hello world from WebServer!

Task 2.5: Secure the Webserver Subnet with a network ACL

Hello world from WebServer2 port 8080!

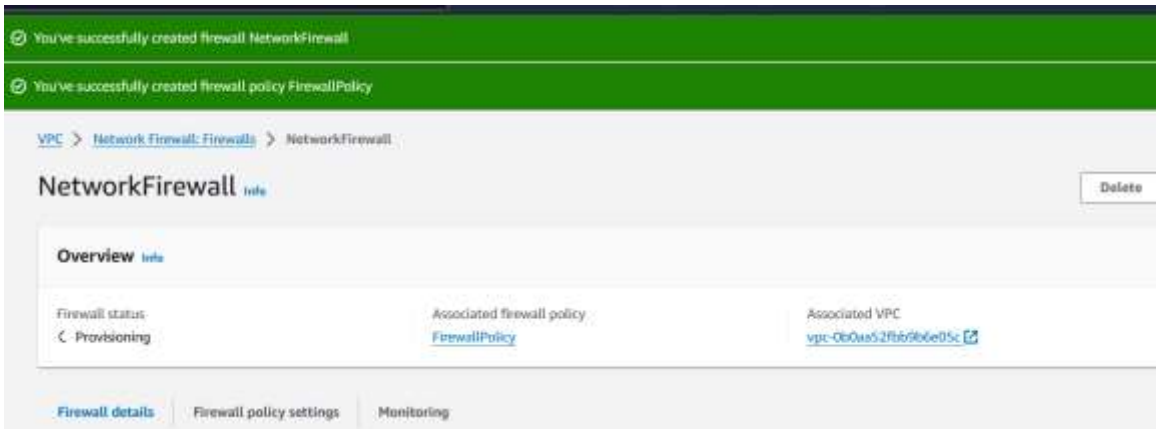
Task 2.6: Review NetworkFirewallVPC and its associated resources

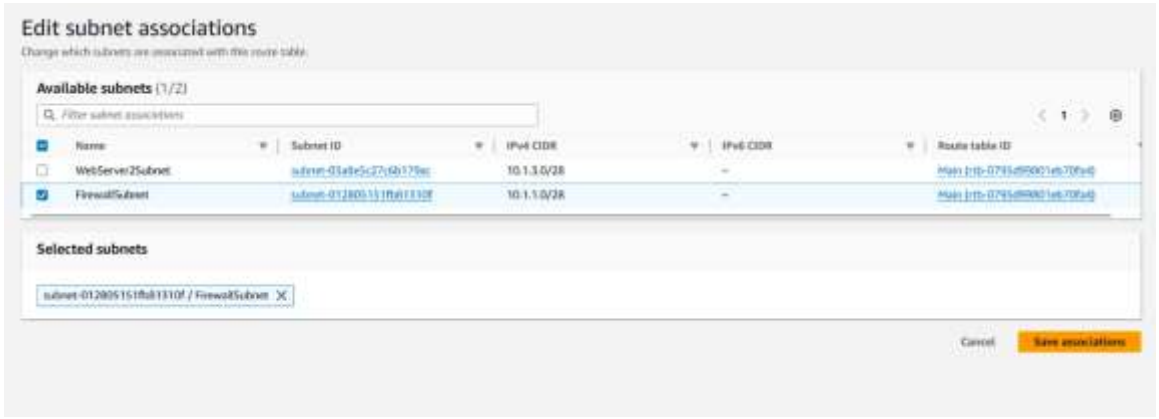
- ✓ Observe the existing NetworkFirewallVPC resources and configurations.
- ✓ Confirm access to the WebServer2 instance on ports 80 and 22
- ✓ Start an additional website that runs on WebServer2 port 8080 and test access.

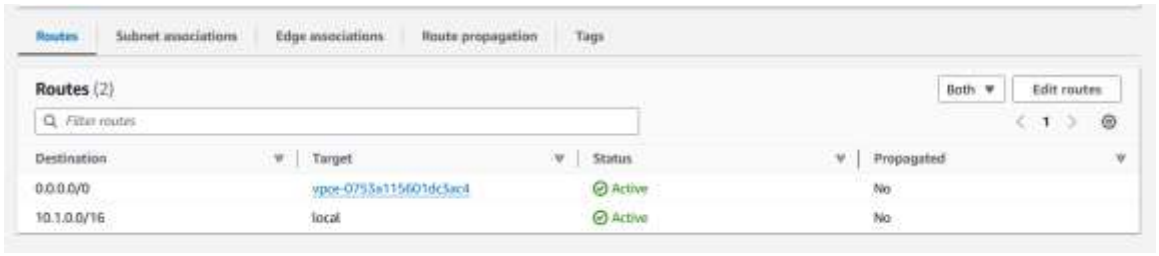


Task 2.7: Create a network firewall

- ✓ In the Amazon VPC console, create a firewall named NetworkFirewall
- ✓ Create route tables
- ✓ Add an edge association to the IGW-Ingress-Route-Table so that the NetworkFirewallIG internet gateway is associated with the route table.
- ✓ Create another route table in *NetworkFirewallVPC* for the *FirewallSubnet*



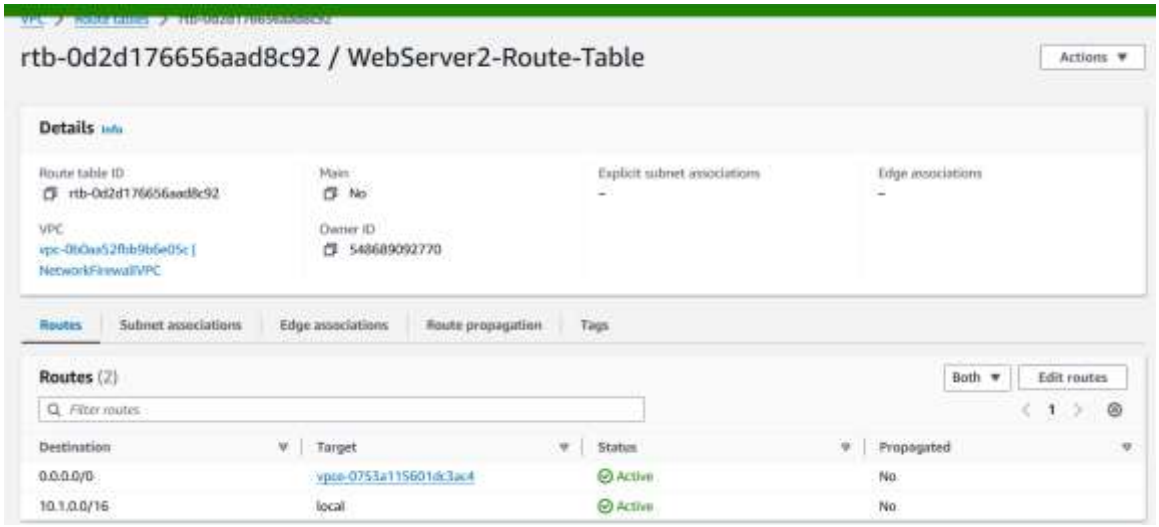


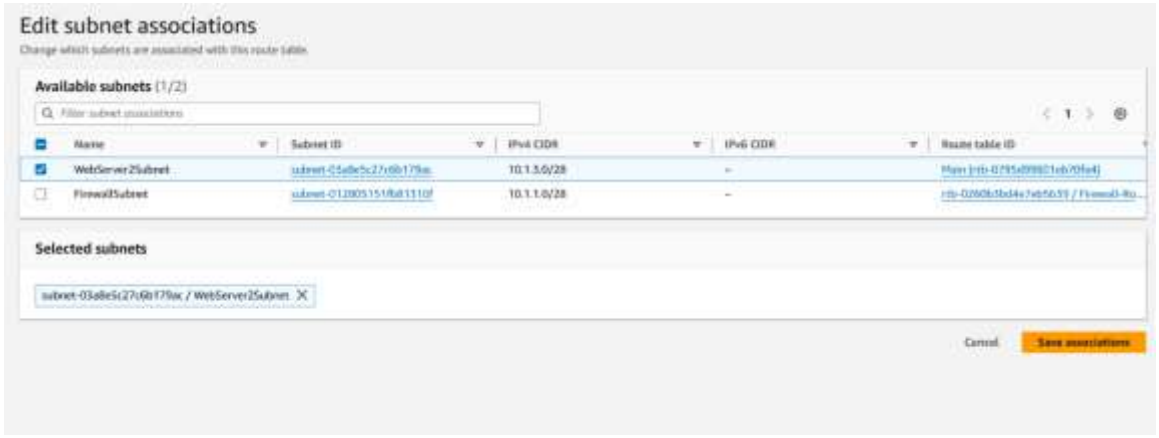


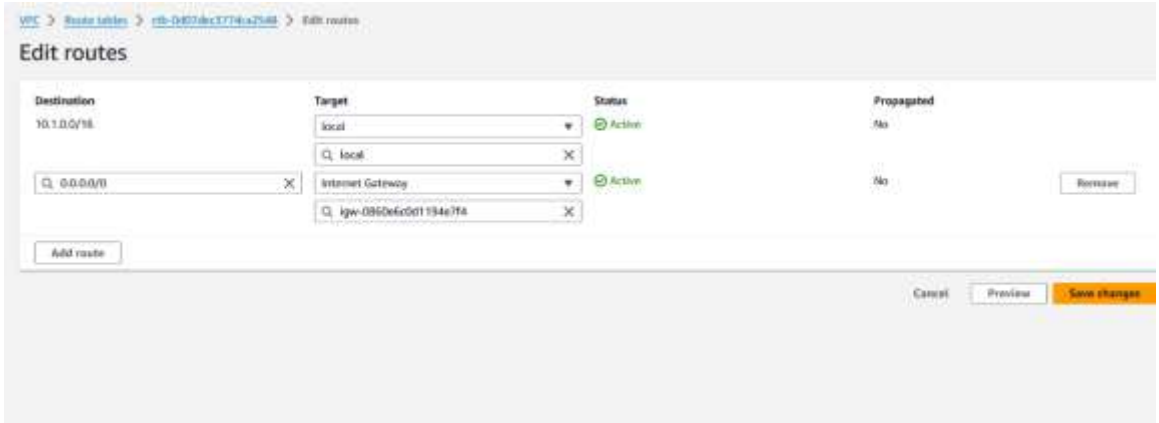
Task 2.8 Create all the route tables that are needed to route traffic to and from the internet through the firewall endpoint

- ✓ Created IGW-Ingress-Route-Table in the *NetworkFirewallVPC*
- ✓ Edit the route table to add a new route
- ✓ Add an edge association to the *IGW-Ingress-Route-Table* so that the *NetworkFirewallIG* internet gateway is associated with the route table
- ✓ Created a `Firewall-Route-Table` route table in *NetworkFirewallVPC* for the *FirewallSubnet*
- Created a WebServer2-Route-Table

- ✓ At the end of task we were asked to delete all resources related to task

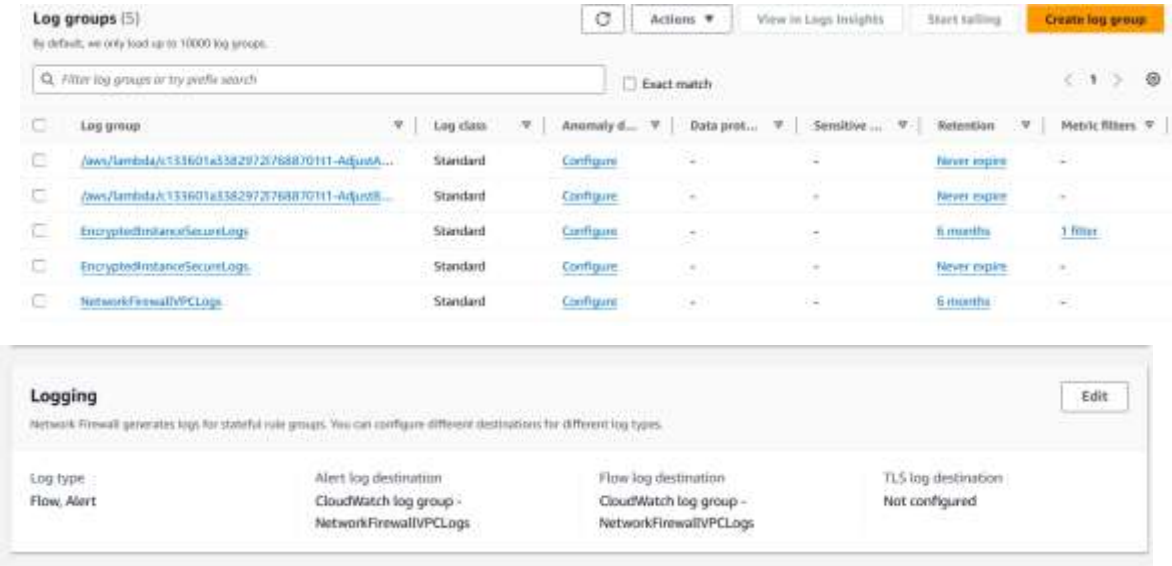






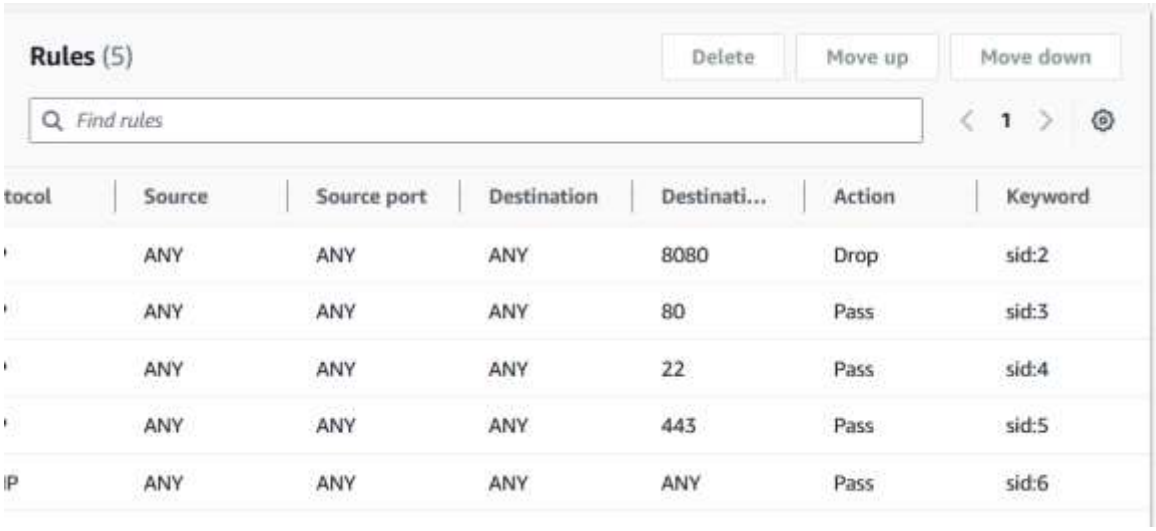
Task 2.9: Configure logging for the network firewall

- ✓ Create a CloudWatch log group named NetworkFirewallVPCLogs with a retention setting of 6 months
- ✓ In the settings for the NetworkFirewall that you created, browse to the Firewall details area, and configure both Alert and Flow type logging. Set the log destination for both types of logging to use the NetworkFirewallVPCLogs CloudWatch log group.



Task 2.10: Configure the firewall policy and test access

- ✓ Navigate to the details page for the NetworkFirewall and begin to create the rule group
- ✓ Configure the stateful rule group with the name NetworkFirewallVPCRuleGroup and a capacity of *100*. Use the other default settings
- ✓ Test the firewall rules
- ✓ In the CloudWatch console, observe the network firewall log entries that were created by your tests in the previous step



Protocol	Port	Action	
TCP	80	Pass	
TCP	22	Pass	
TCP	8080	Drop	
ICMP	Any	Pass	
TCP	443	Pass	

IGW-Ingress-Route-Table

0.0.0.0/0	**Gateway load balancer Endpoint**	All	All	Allow
10.0.1.0/24	**Local**	All	All	Allow

Firewall-Route-Table

0.0.0.0/0	**NetworkFirewallIG**	**All**	**All**	**Allow**
10.0.2.0/24	**Local**	All	All	Allow

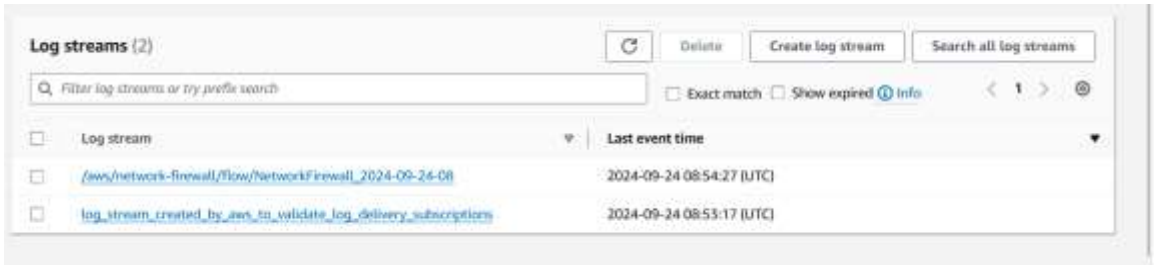
Webserver2-Route-Table

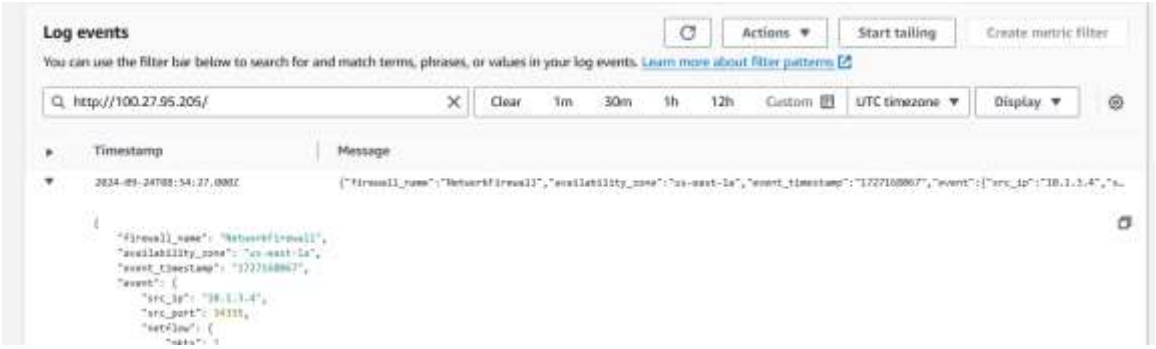
0.0.0.0/0	**Gateway load balancer Endpoint**	All	All	Allow
10.0.3.0/24	**Local**	All	All	Allow

```
Last login: Tue Sep 24 12:29:33 2024 from 3.216.191.98
[ec2-user@webserver2 ~]$ ping -c 3 www.amazon.com

sudo netstat -tulpn | grep -i listen
PING www-amazon-com.customer.fastly.net (162.219.225.118) 56(84) bytes of data.
64 bytes from 162.219.225.118 (162.219.225.118): icmp_seq=1 ttl=56 time=1.76 ms
64 bytes from 162.219.225.118 (162.219.225.118): icmp_seq=2 ttl=56 time=1.81 ms
64 bytes from 162.219.225.118 (162.219.225.118): icmp_seq=3 ttl=56 time=1.63 ms

--- www-amazon-com.customer.fastly.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.633/1.734/1.811/0.074 ms
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2344/sshd: /usr/sbi
tcp6       0      0 :::22                   :::*                    LISTEN      2344/sshd: /usr/sbi
tcp6       0      0 :::80                   :::*                    LISTEN      1998/httpd
```



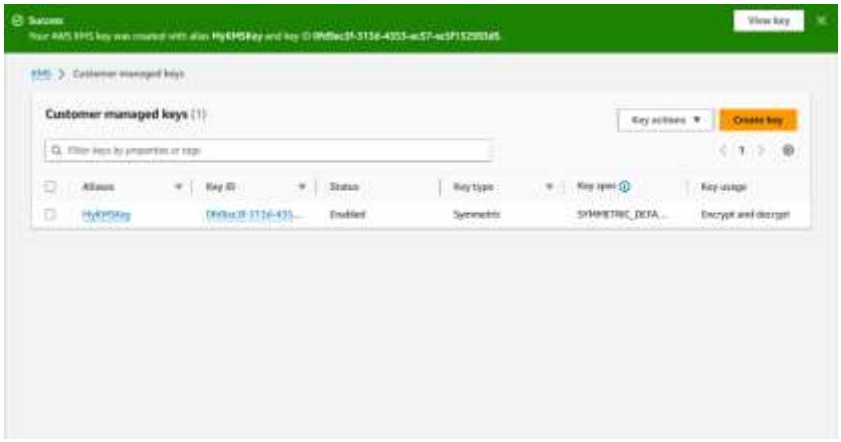


Cost estimate to secure a VPC with a network firewall

Upfront cost	Monthly cost	Total 12 months cost
0.00 USD	161.90 USD	1,942.80 USD Includes upfront cost

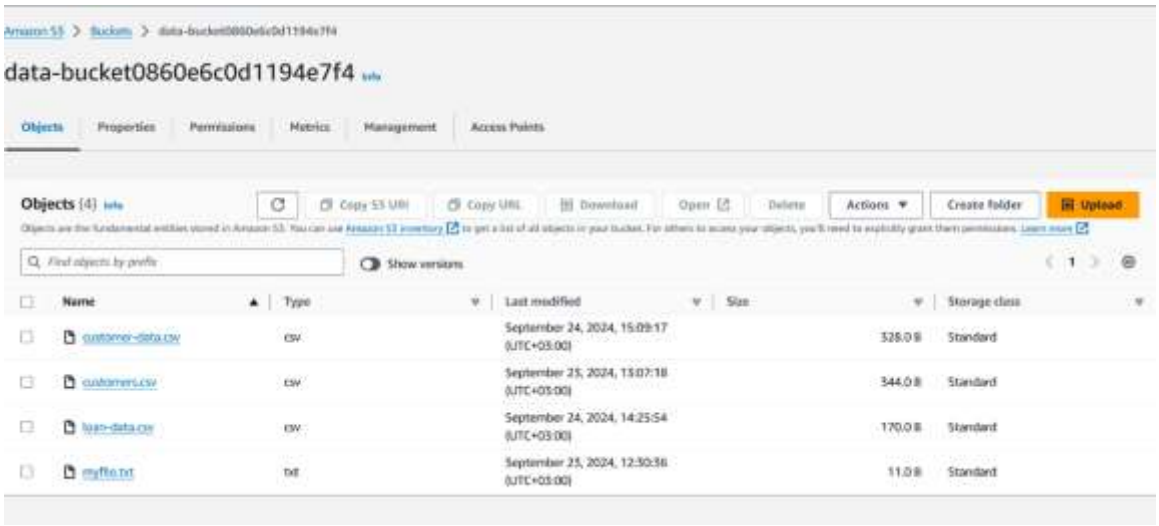
Week33 :Securing AWS resources by using AWS KMS

Task 3.1: Create a customer managed key and configure key rotation3



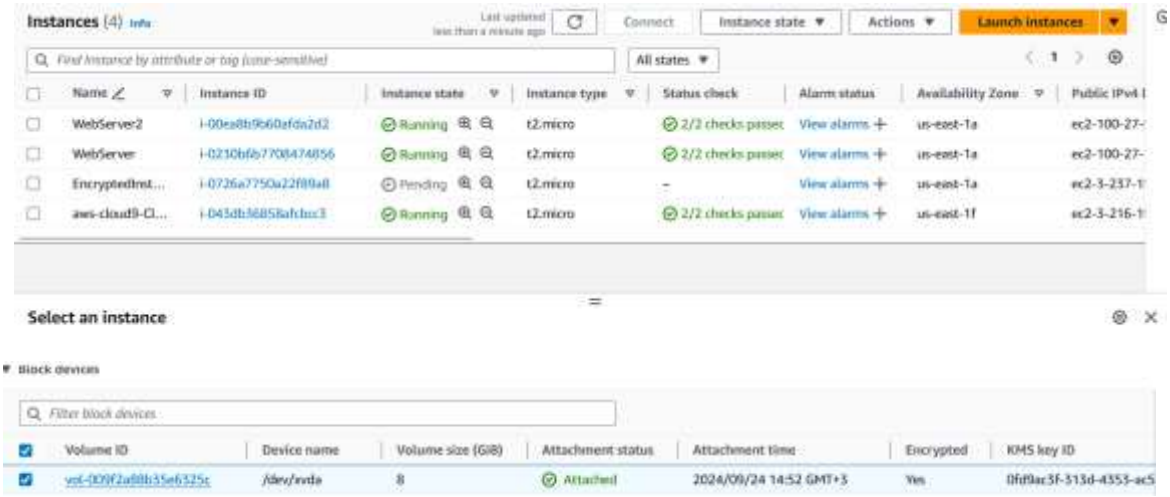
Task 3.2: Update the AWS KMS key policy and analyze an IAM policy

- ✓ Sofia can access bucket containing loan-data.csv
- ✓ Paulo can't access

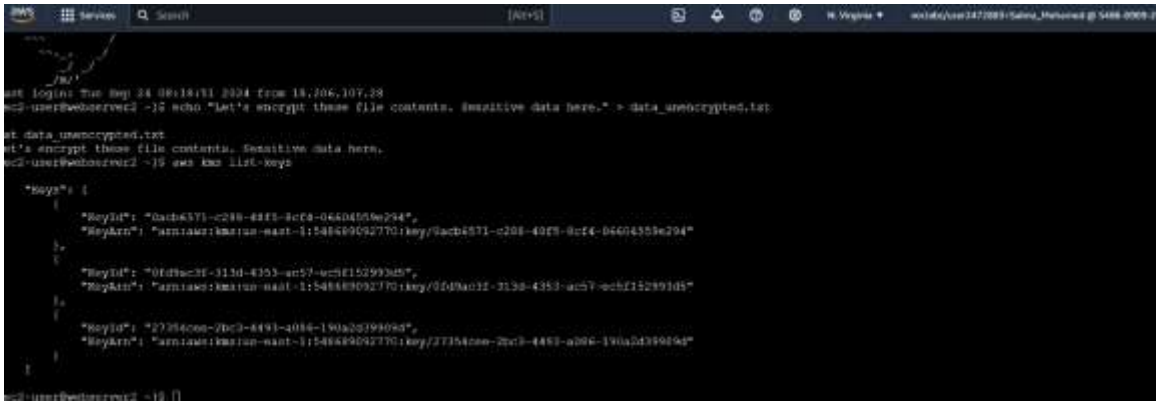


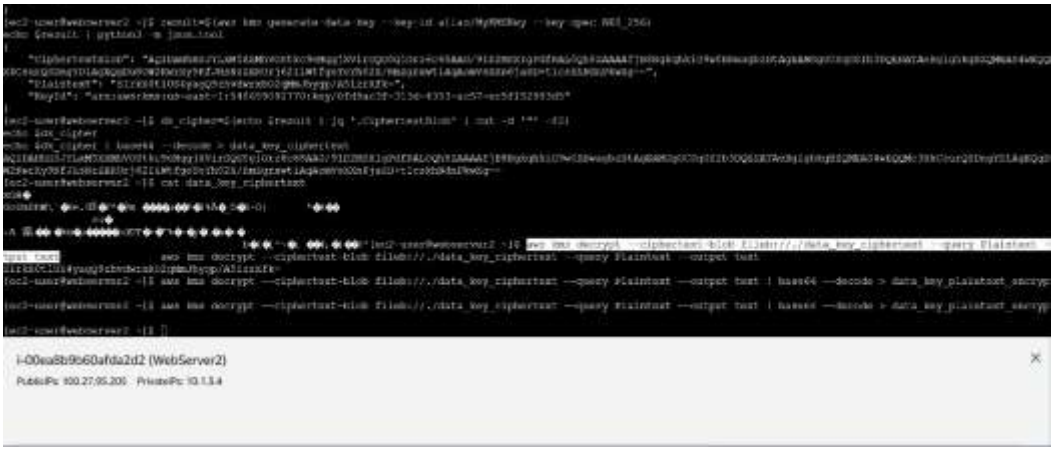
Task 3.4: Use AWS KMS to encrypt the root volume of an EC2 instance

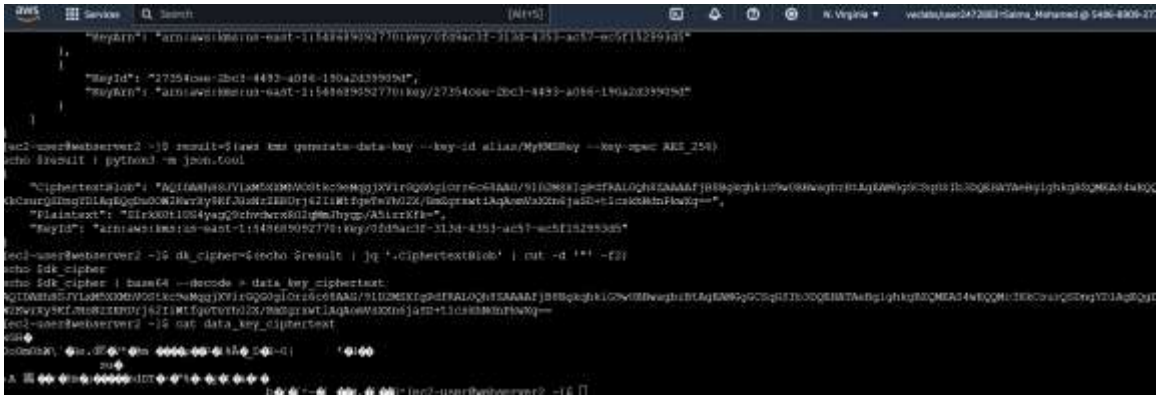
- ✓ While logged in with the *voclabs* role, create a new EC2 instance. Keep the default settings except for the following
- ✓ On the details page for *EncryptedInstance*, choose the **Storage** tab and verify that the instance root volume is encrypted.



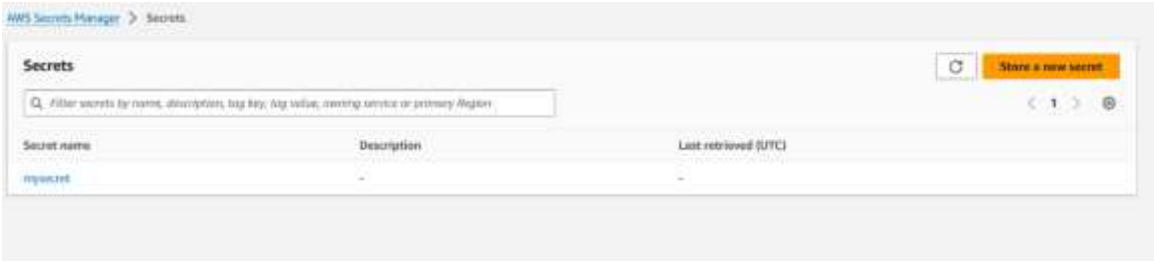
Task 3.5: Use AWS KMS envelope encryption to encrypt data in place

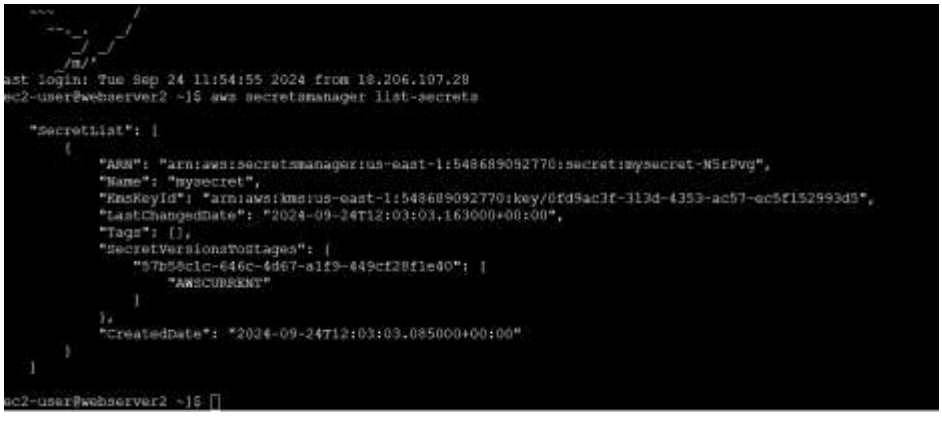






Task 3.6: Use AWS KMS to encrypt a Secrets Manager secret





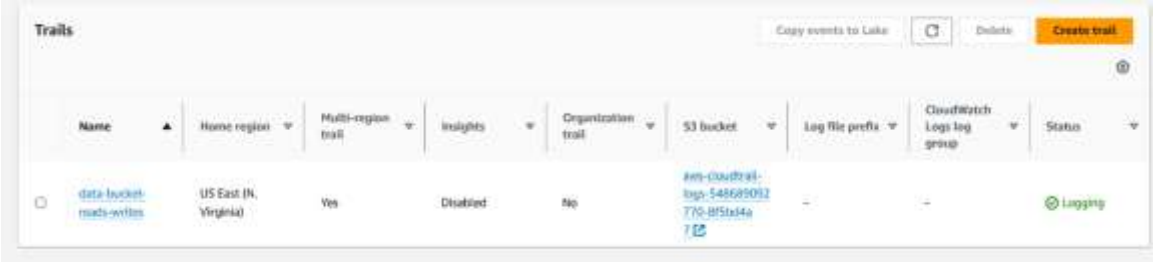
Cost estimate

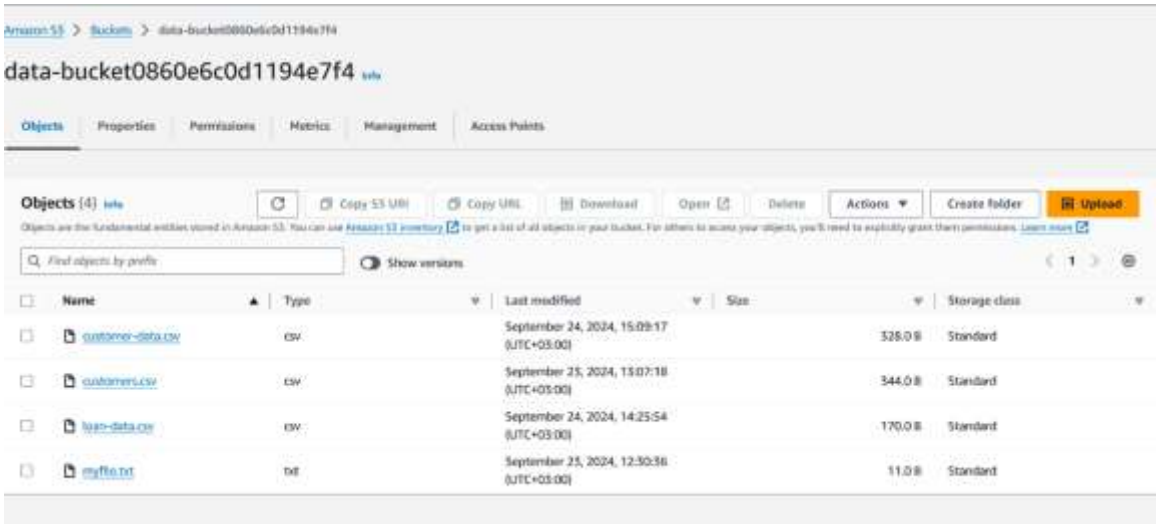
Upfront cost	Monthly cost	12 months cost
0.00 USD	7.00 USD	84.00 USD

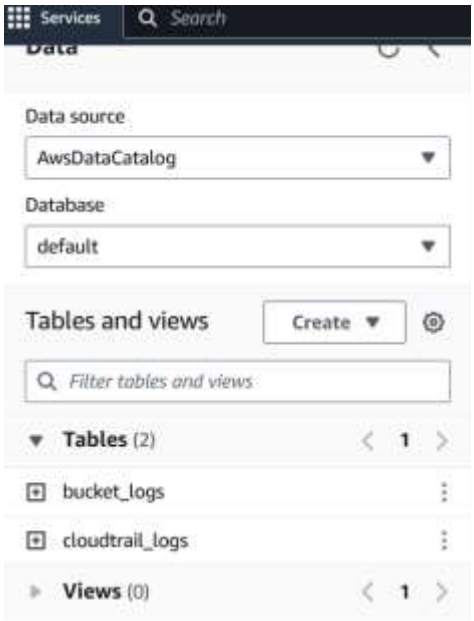
Phase 4: Monitoring and logging

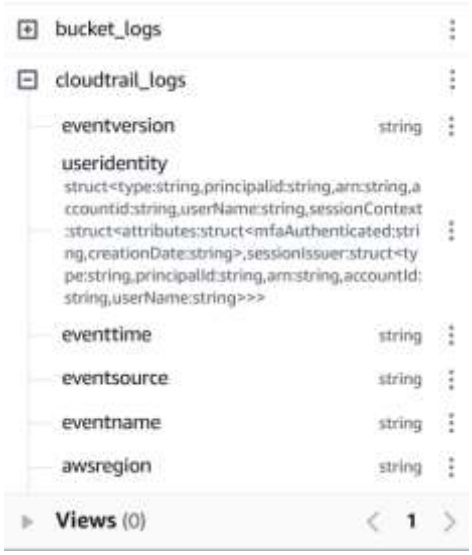
Task 4.1: Use CloudTrail to record Amazon S3 API calls

- ✓ Create a CloudTrail trail
- ✓ On your computer, create a file named `customer-data.csv`. Then, in a text editor, paste the following data into the file and save the changes.
- ✓ Use the CloudTrail console to create an Athena table that describes the format of the data in the cloudtrail-logs S3 bucket.

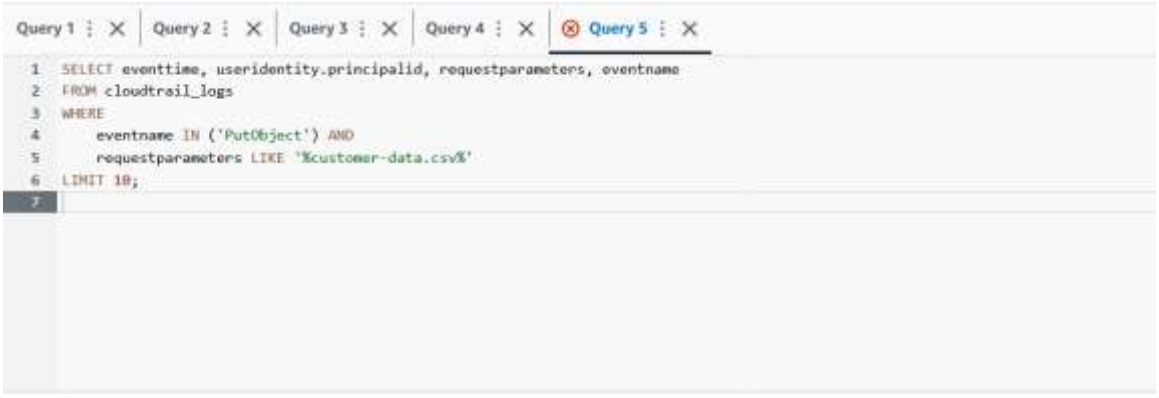




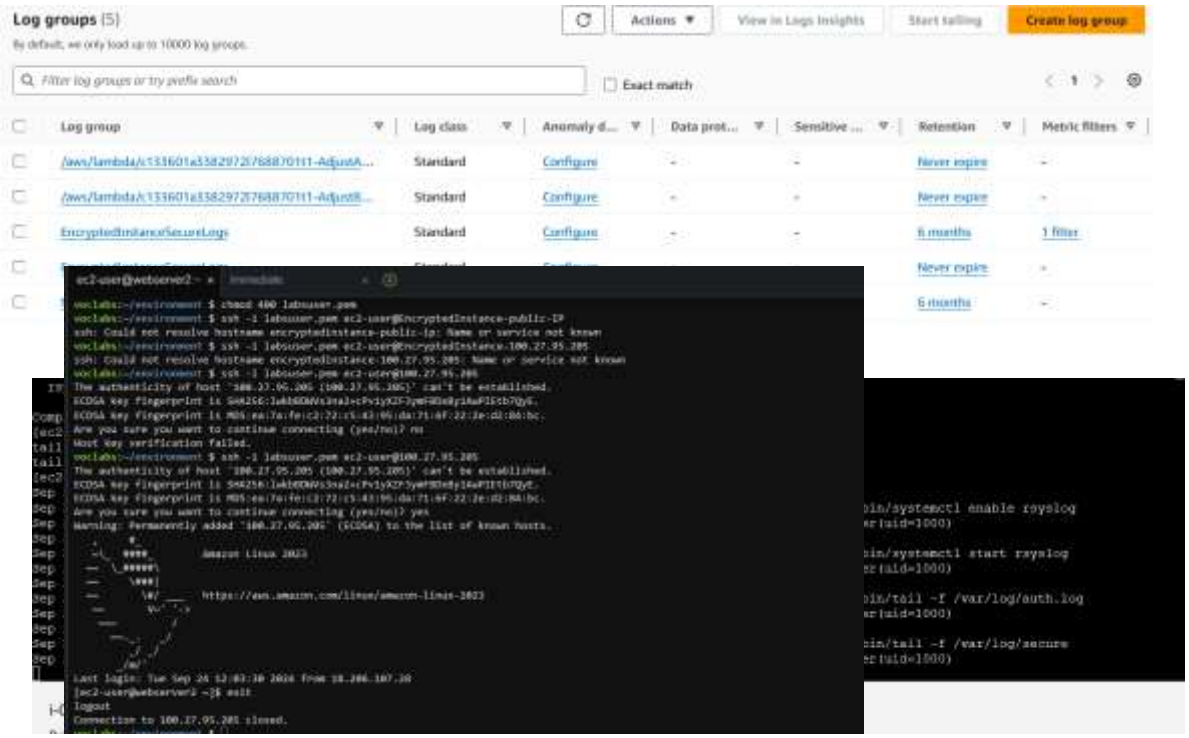


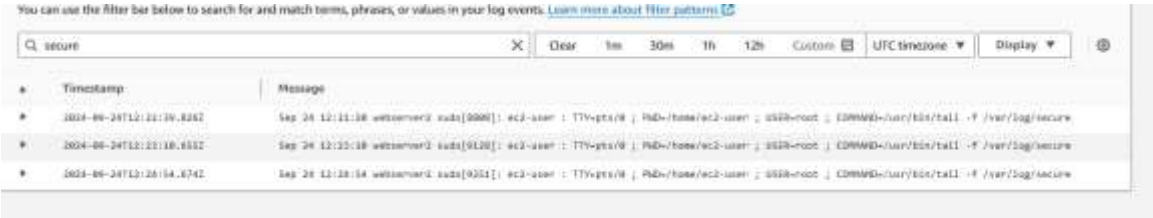



```
48  )
49  ROW FORMAT SERDE 'org.openx.data.jsonserde.JsonSerDe'
50  WITH SERDEPROPERTIES (
51      'ignore.malformed.json' = 'true'
52  )
53  LOCATION 's3://cloudtrail-logs/'
54  TBLPROPERTIES ('has_encrypted_data'='false');
55
```

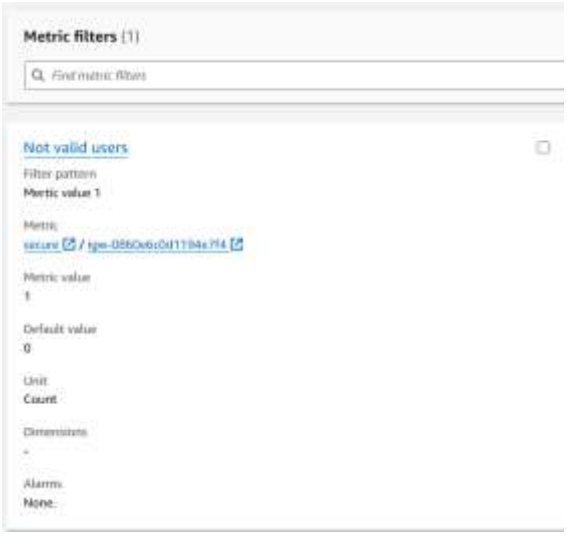


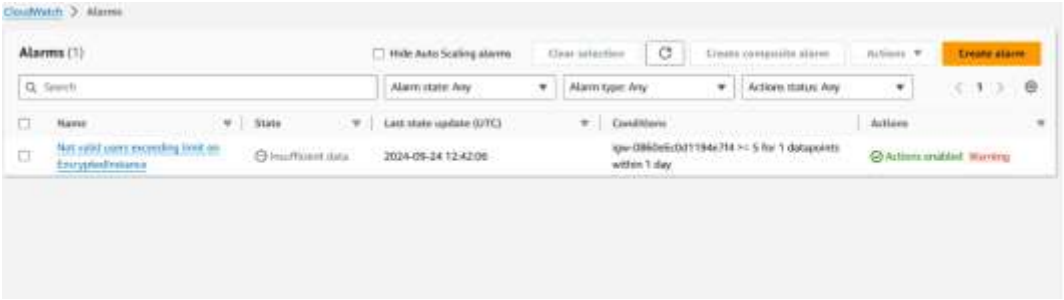
Task 4 . 2: Use CloudWatch Logs to monitor secure logs





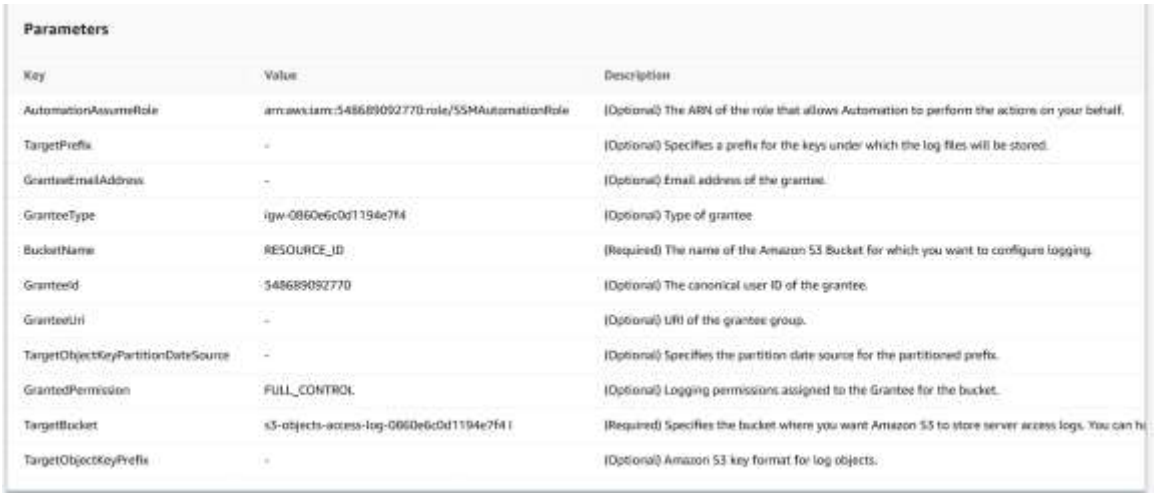
Task 4.3: Create a CloudWatch alarm to send notifications for security incidents





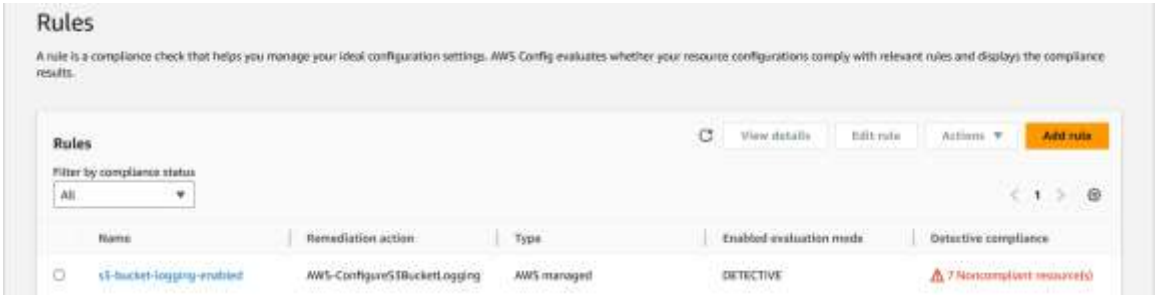
```
        _/m/'
Last login: Tue Sep 24 12:03:30 2024 from 18.206.107.28
[ec2-user@webserver2 ~]$ exit
logout
Connection to 100.27.95.205 closed.
voclabs:~/environment $ ssh -i labsuser.pem ubuntu@EncryptedInstance-100.27.95
ssh: Could not resolve hostname encryptedinstance-100.27.95.205: Name or servi
voclabs:~/environment $ ssh invalid-user@<EncryptedInstance-public-IP>
bash: syntax error near unexpected token `newline'
voclabs:~/environment $ ssh invalid-user@100.27.95.205
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $ ssh invalid-user@100.27.95.205
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $ ssh invalid-user@100.27.95.205
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $ ssh invalid-user@100.27.95.205
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $ ssh invalid-user@100.27.95.205
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $
```

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



Parameters

Key	Value	Description
AutomationAssumeRole	arn:aws:iam::548689092770:role/SSMAutomationRole	(Optional) The ARN of the role that allows Automation to perform the actions on your behalf.
TargetPrefix	-	(Optional) Specifies a prefix for the keys under which the log files will be stored.
GranteeEmailAddress	-	(Optional) Email address of the grantee.
GranteeType	igw-0860e6c0d1194e7f4	(Optional) Type of grantee
BucketName	RESOURCE_ID	(Required) The name of the Amazon S3 Bucket for which you want to configure logging.
GranteeId	548689092770	(Optional) The canonical user ID of the grantee.
GranteeUri	-	(Optional) URI of the grantee group.
TargetObjectKeyPartitionDateSource	-	(Optional) Specifies the partition date source for the partitioned prefix.
GrantedPermission	FULL_CONTROL	(Optional) Logging permissions assigned to the Grantee for the bucket.
TargetBucket	s3-objects-access-log-0860e6c0d1194e7f4	(Required) Specifies the bucket where you want Amazon S3 to store server access logs. You can h
TargetObjectKeyPrefix	-	(Optional) Amazon S3 key format for log objects.



Rules

A rule is a compliance check that helps you manage your ideal configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and displays the compliance results.

Rules

View details | Edit rule | Actions | Add rule

Filter by compliance status: All

Name	Remediation action	Type	Enabled evaluation mode	Detective compliance
s3-bucket-logging-enabled	AWS-ConfigureS3BucketLogging	AWS managed	DETECTIVE	7 Noncompliant resource(s)

Rule details

Edit

Description: Checks if logging is enabled for your S3 buckets. The rule is NON_COMPLIANT if logging is not enabled.

Config rule ARN: arn:aws:config:us-east-1:548689092770:config-rule/config-rule-le2bn4

Enabled evaluation mode: • DETECTIVE

Last successful detective evaluation: September 24, 2024 3:59 PM

Detective evaluation trigger type: • Oversized configuration changes • Configuration changes

Scope of changes: Resources

Resource types: S3 Bucket

Parameters

Key	Type	Value	Description
targetBucket	String	-	Target S3 bucket for storing server access logs.
targetPrefix	String	-	Prefix of the S3 bucket for storing server access logs.

Cost Estimate

Upfront cost	Monthly cost	12 Months cost
0.00 USD	13.71 USD	164.52 USD Includes upfront costs