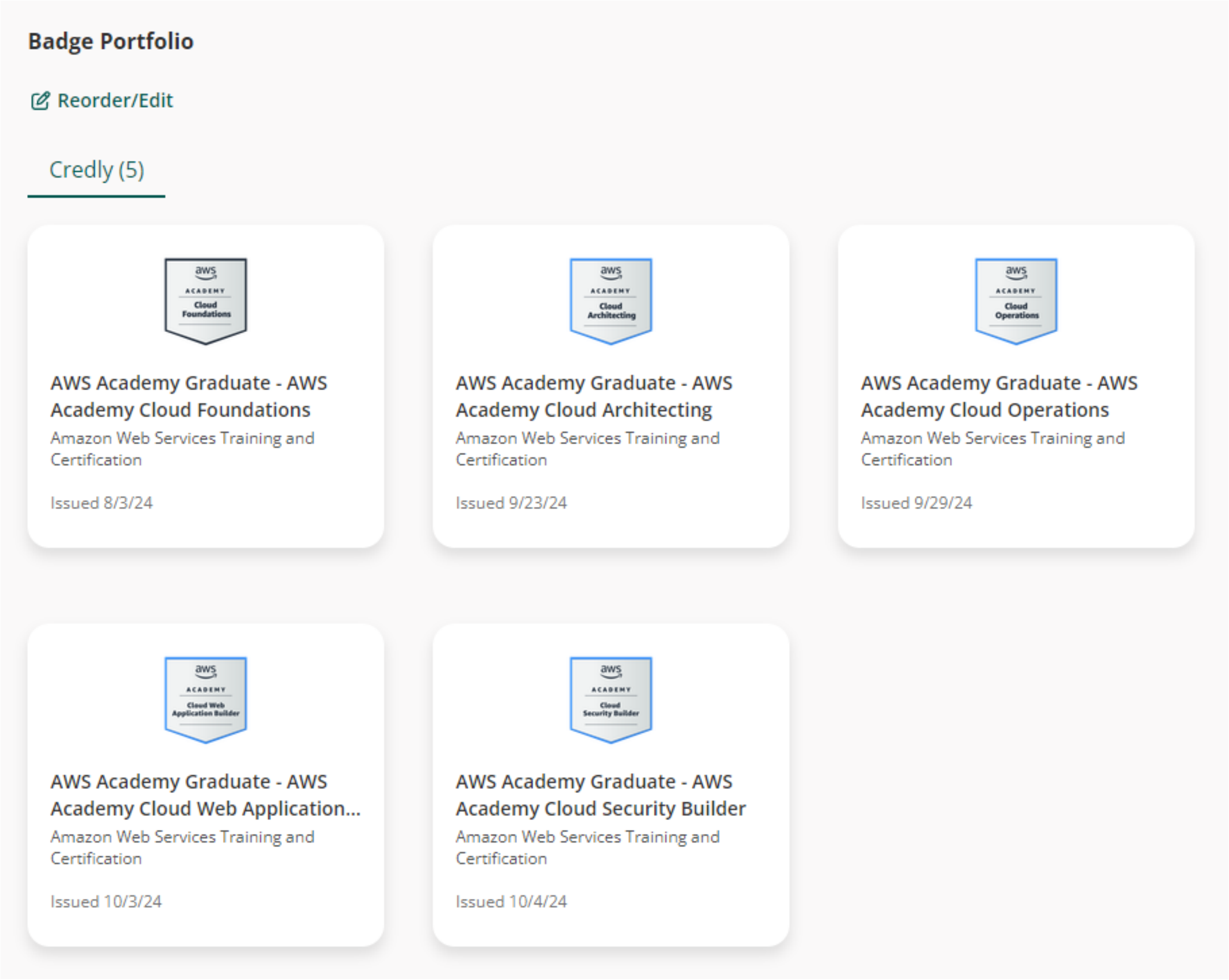
Securing and Monitoring Resources with AWS

Name	Badr Eldin Wael Mohamed Mohamed
Group	ALX1_ISS4_M1e
Student ID	21007401
Badges	https://www.credly.com/users/badr-eldin-wael



aws ACADEMY Cloud Foundations
aws ACADEMY Cloud Architecting
aws ACADEMY Cloud Operations
aws ACADEMY Cloud Web Application Builder
aws ACADEMY Cloud Security Builder

Badge Portfolio

Reorder/Edit

Credly (5)

AWS Academy Graduate - AWS Academy Cloud Foundations
Amazon Web Services Training and Certification
Issued 8/3/24

AWS Academy Graduate - AWS Academy Cloud Architecting
Amazon Web Services Training and Certification
Issued 9/23/24

AWS Academy Graduate - AWS Academy Cloud Operations
Amazon Web Services Training and Certification
Issued 9/29/24

AWS Academy Graduate - AWS Academy Cloud Web Application...
Amazon Web Services Training and Certification
Issued 10/3/24

AWS Academy Graduate - AWS Academy Cloud Security Builder
Amazon Web Services Training and Certification
Issued 10/4/24

Phase 1: Securing data in Amazon S3

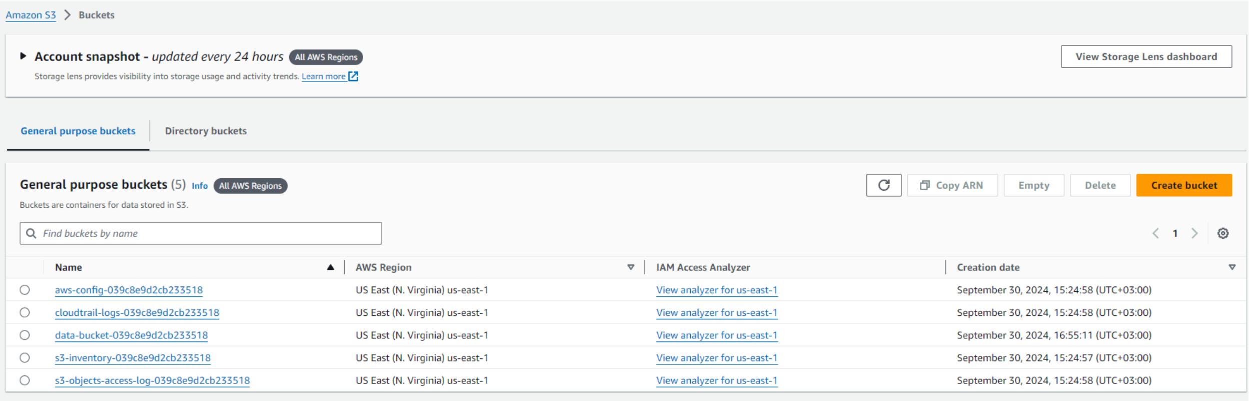
Task 1.1: Create a bucket, apply a bucket policy, and test access

-Create a s3 data bucket and give it a policies then uploud myfile.txt

-Allow all S3 actions for the voclabs IAM role, Paulo, and Sofia users

-Deny all S3 actions for any principal not matching those ARNs.

-paulo has access but mary doesn't have access to s3 objects



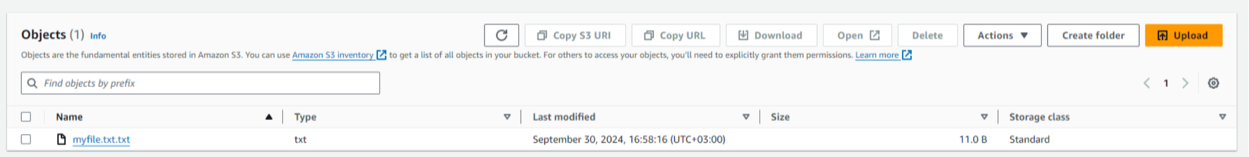
▸ Account snapshot - *updated every 24 hours* All AWS Regions

Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets (5)

Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
○	aws-config-039c8e9d2cb233518	US East (N. Virginia) us-east-1	View analyzer for us-east-1	September 30, 2024, 15:24:58 (UTC+03:00)
○	cloudtrail-logs-039c8e9d2cb233518	US East (N. Virginia) us-east-1	View analyzer for us-east-1	September 30, 2024, 15:24:58 (UTC+03:00)
○	data-bucket-039c8e9d2cb233518	US East (N. Virginia) us-east-1	View analyzer for us-east-1	September 30, 2024, 16:55:11 (UTC+03:00)
○	s3-inventory-039c8e9d2cb233518	US East (N. Virginia) us-east-1	View analyzer for us-east-1	September 30, 2024, 15:24:57 (UTC+03:00)
○	s3-objects-access-log-039c8e9d2cb233518	US East (N. Virginia) us-east-1	View analyzer for us-east-1	September 30, 2024, 15:24:58 (UTC+03:00)

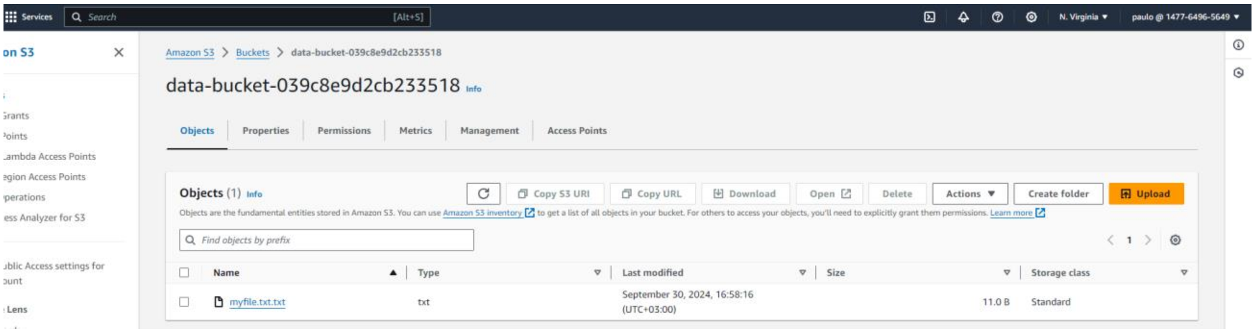


Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name	Type	Last modified	Size	Storage class
□	myfile.txt.txt	txt	September 30, 2024, 16:58:16 (UTC+03:00)	11.0 B	Standard

Paulo:



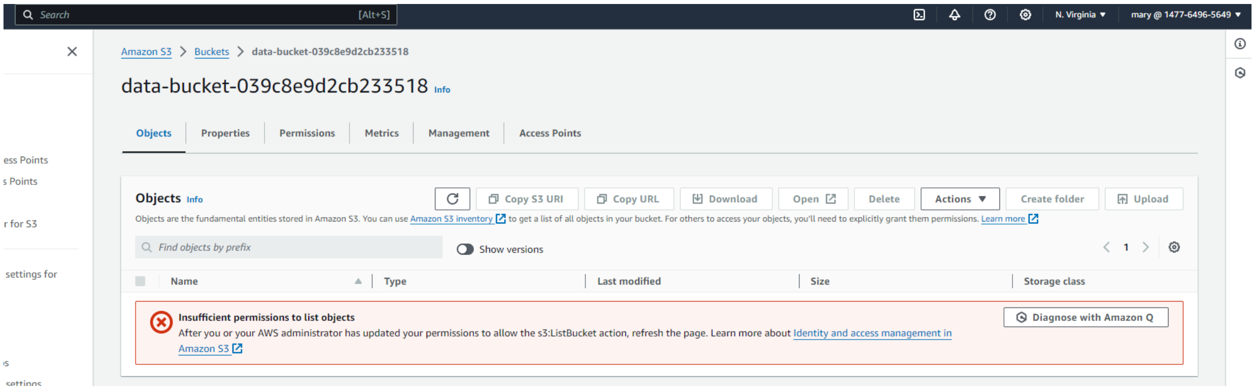
data-bucket-039c8e9d2cb233518

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name	Type	Last modified	Size	Storage class
□	myfile.txt.txt	txt	September 30, 2024, 16:58:16 (UTC+03:00)	11.0 B	Standard

Mary:



data-bucket-039c8e9d2cb233518

Objects

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

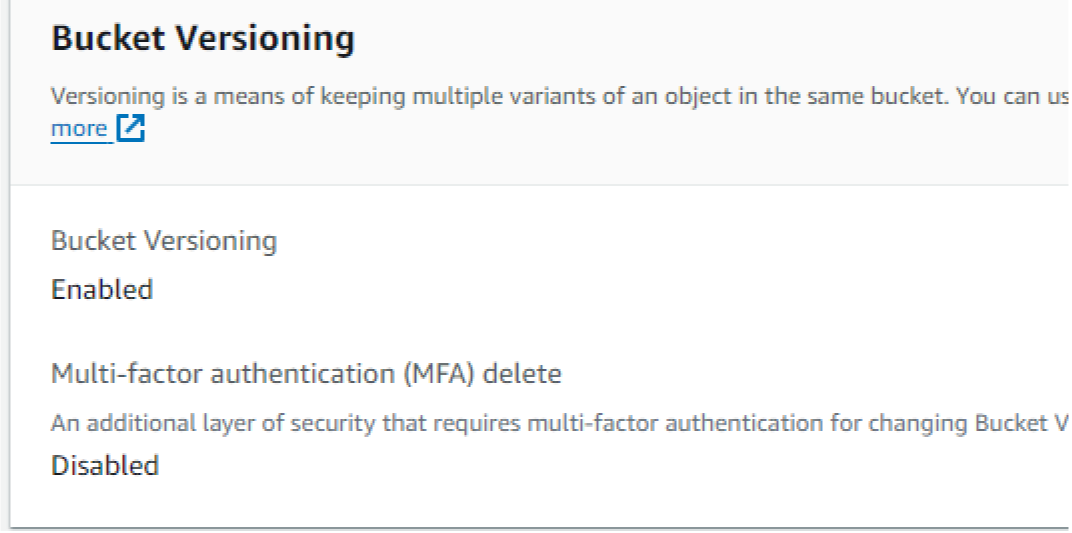
Insufficient permissions to list objects

After you or your AWS administrator has updated your permissions to allow the s3:ListBucket action, refresh the page. Learn more about Identity and access management in Amazon S3

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

-Enable versioning and object-level logging on the data-bucket. Versioning will allow me to track changes to objects and revert to previous versions if needed, while object-level logging creates an audit trail for the objects in the bucket, helping detect security issues.

-Enable server access logging for the bucket, directing the logs to the s3-objects-access-log bucket and using /data-bucket

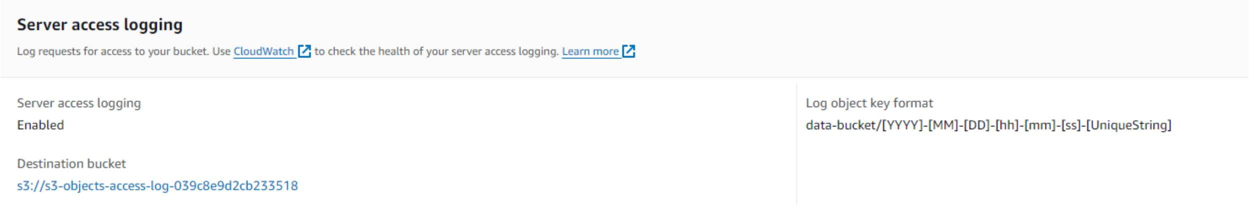


Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can us
more

Bucket Versioning
Enabled

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket V
Disabled



Server access logging

Log requests for access to your bucket. Use CloudWatch to check the health of your server access logging. Learn more

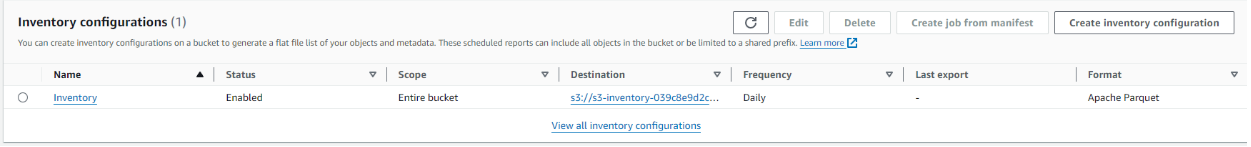
Server access logging
Enabled

Destination bucket
s3://s3-objects-access-log-039c8e9d2cb233518

Log object key format
data-bucket/[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]

Task 1.3: Implement the S3 Inventory feature on a bucket

-Enable the S3 Inventory feature on the data-bucket to monitor object changes and generate reports. S3 Inventory provides scheduled reports on metadata and object-level changes



Inventory configurations (1)

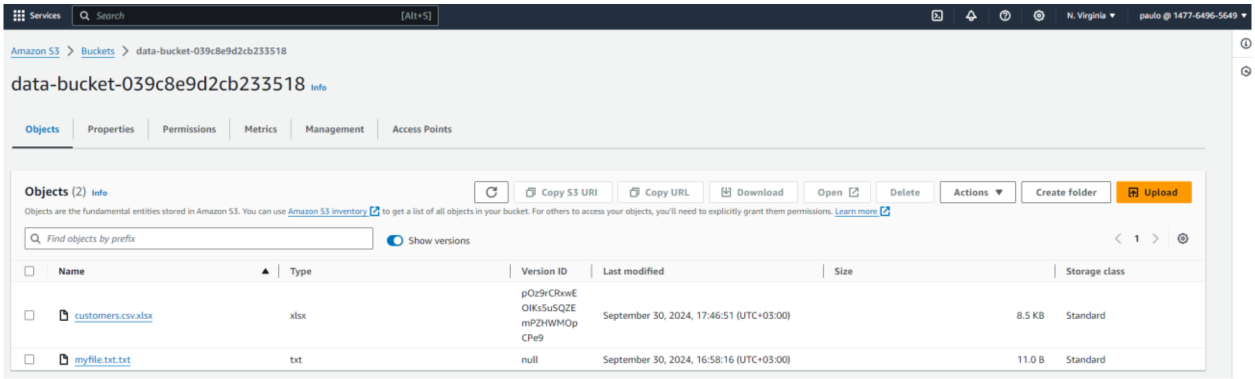
You can create inventory configurations on a bucket to generate a flat file list of your objects and metadata. These scheduled reports can include all objects in the bucket or be limited to a shared prefix. Learn more

	Name	Status	Scope	Destination	Frequency	Last export	Format
○	Inventory	Enabled	Entire bucket	s3://s3-inventory-039c8e9d2c...	Daily	-	Apache Parquet

View all inventory configurations

Task 1.4: Confirm that versioning works as intended

-Paulo uses versioning



data-bucket-039c8e9d2cb233518

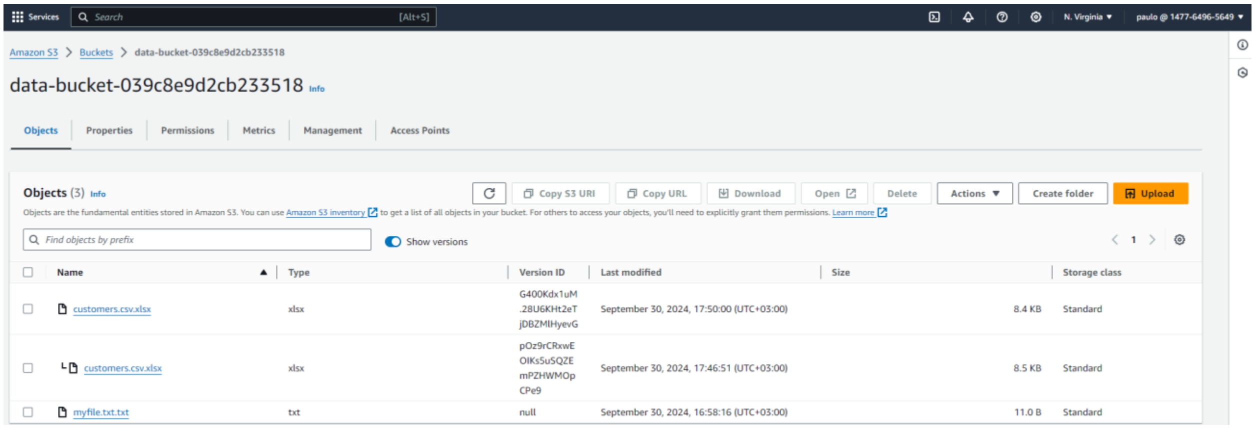
Objects (2) Info

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Find objects by prefix

Show versions

□	Name	Type	Version ID	Last modified	Size	Storage class
□	customers.csv.xlsx	xlsx	pOz9rCRxwEOIKs5uSQZEmPZHWMOpCPe9	September 30, 2024, 17:46:51 (UTC+03:00)	8.5 KB	Standard
□	myfile.txt.txt	txt	null	September 30, 2024, 16:58:16 (UTC+03:00)	11.0 B	Standard



data-bucket-039c8e9d2cb233518

Objects (3) Info

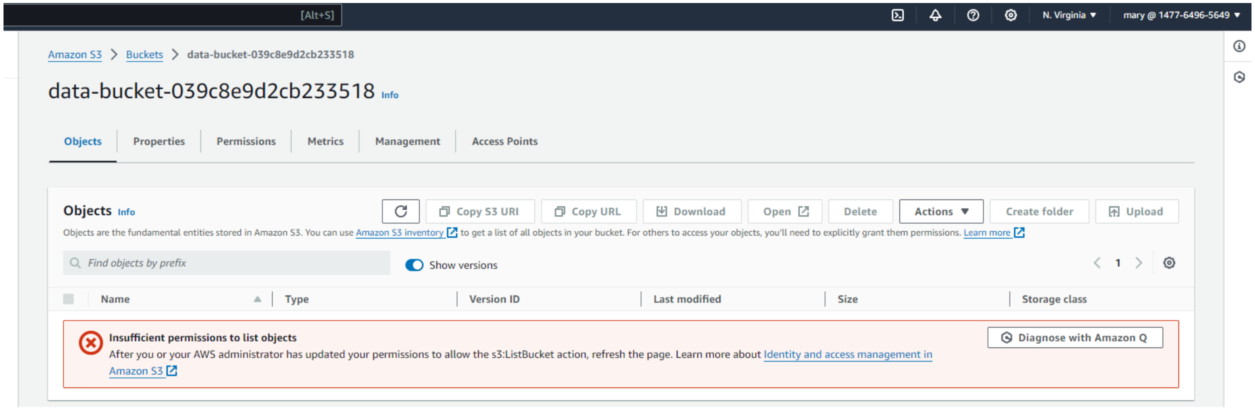
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Find objects by prefix

Show versions

□	Name	Type	Version ID	Last modified	Size	Storage class
□	customers.csv.xlsx	xlsx	G400Kdx1uM.28U6KHt2eTjDBZMlHyevG	September 30, 2024, 17:50:00 (UTC+03:00)	8.4 KB	Standard
□	└ customers.csv.xlsx	xlsx	pOz9rCRxwEOIKs5uSQZEmPZHWMOpCPe9	September 30, 2024, 17:46:51 (UTC+03:00)	8.5 KB	Standard
□	myfile.txt.txt	txt	null	September 30, 2024, 16:58:16 (UTC+03:00)	11.0 B	Standard

-Mary uses logs:



data-bucket-039c8e9d2cb233518 Info

Objects Info

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Insufficient permissions to list objects
After you or your AWS administrator has updated your permissions to allow the s3:ListBucket action, refresh the page. Learn more about Identity and access management in Amazon S3

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

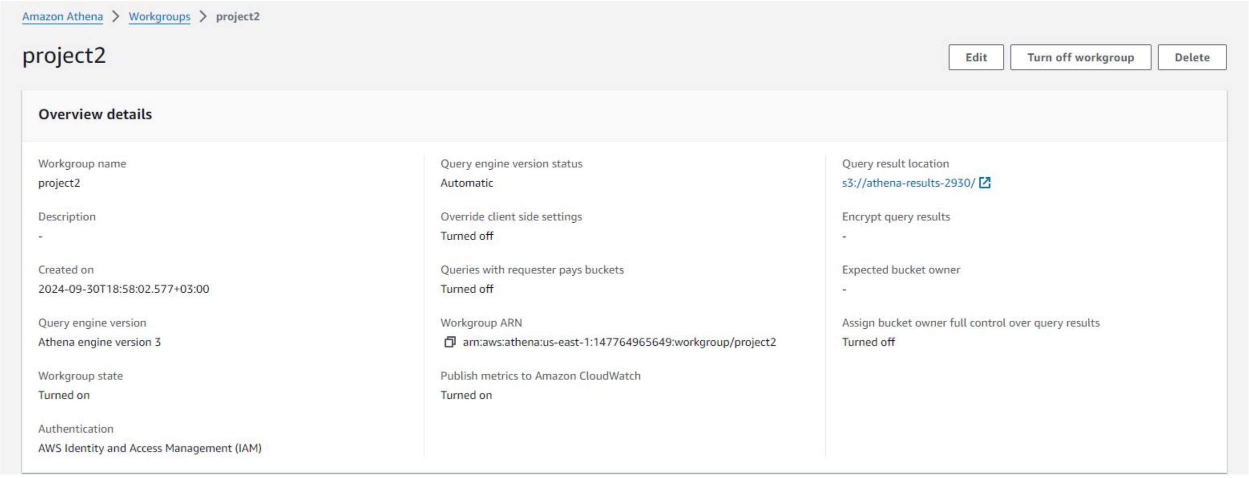
-Confirm that S3 object-level logging is successfully writing logs to the s3-objects-access-log bucket. Then, I'll query these logs using Athena.

-Create an S3 bucket named athena-results for query results.

-Use the Athena query editor to set the athena-results bucket as the destination for results.

-Run a query to create the bucket_logs table from the access logs.

-The query filters out actions taken by the voclabs role and shows actions taken by users like Paulo and Mary. For Paulo, the requests should have a status of 200 (successful), while Mary's requests will have a status of 403 (forbidden)



project2

Overview details

Workgroup name
project2

Description
-

Created on
2024-09-30T18:58:02.577+03:00

Query engine version
Athena engine version 3

Workgroup state
Turned on

Authentication
AWS Identity and Access Management (IAM)

Query engine version status
Automatic

Override client side settings
Turned off

Queries with requester pays buckets
Turned off

Workgroup ARN
arn:aws:athena:us-east-1:147764965649:workgroup/project2

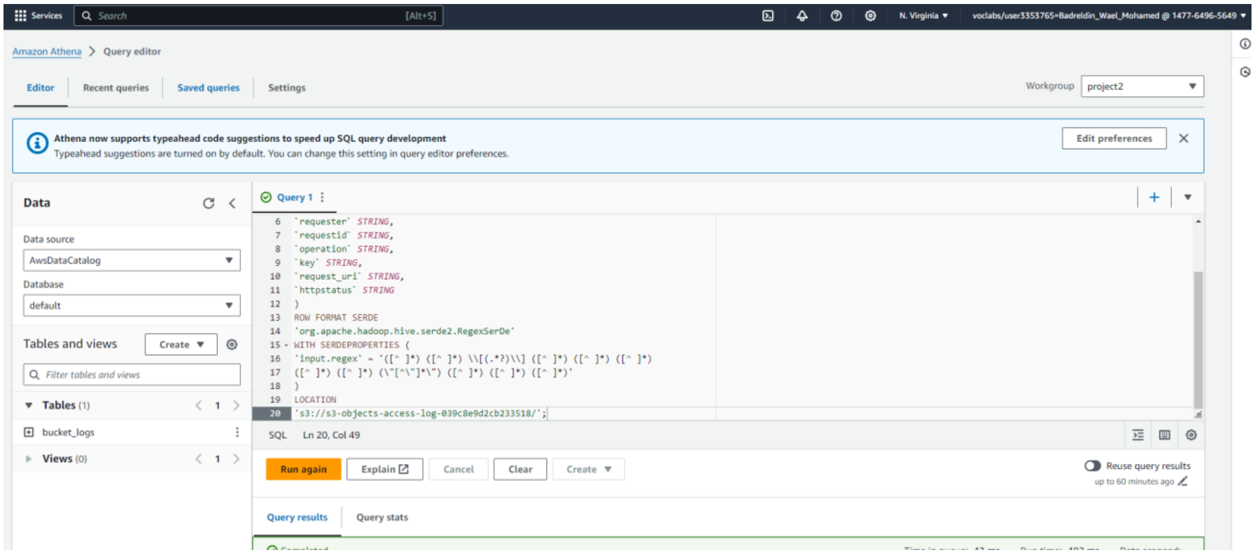
Publish metrics to Amazon CloudWatch
Turned on

Query result location
s3://athena-results-2930/

Encrypt query results
-

Expected bucket owner
-

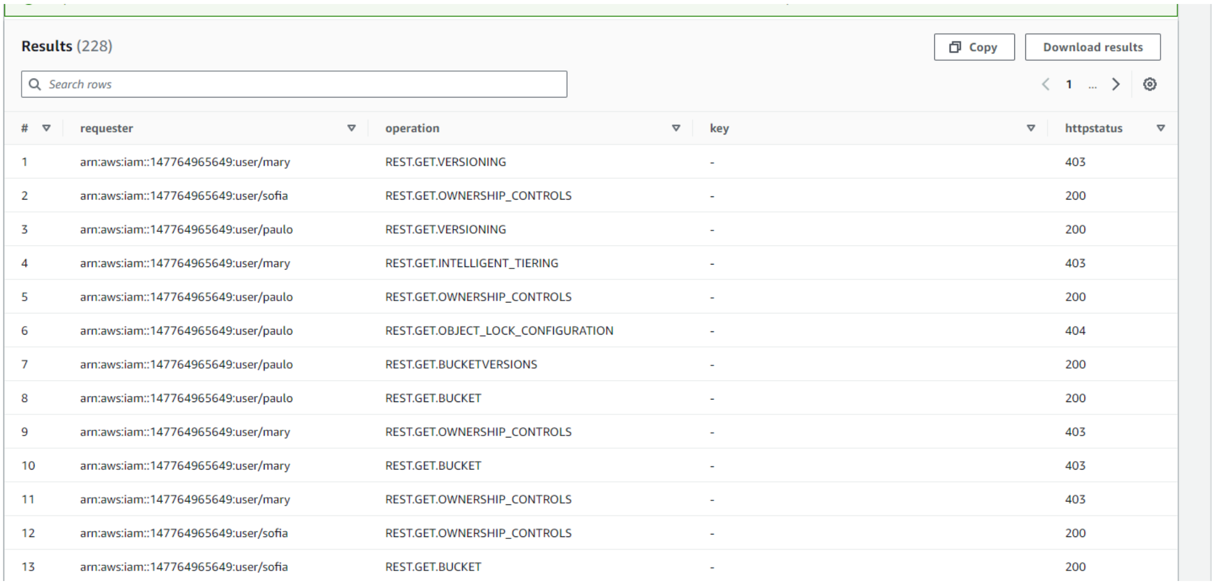
Assign bucket owner full control over query results
Turned off



Athena now supports typeahead code suggestions to speed up SQL query development
Typeahead suggestions are turned on by default. You can change this setting in query editor preferences.

```
`requester` STRING,
`requestid` STRING,
`operation` STRING,
`key` STRING,
`request_uri` STRING,
`httpstatus` STRING
)
ROW FORMAT SERDE
'org.apache.hadoop.hive.serde2.RegexSerDe'
WITH SERDEPROPERTIES (
'input.regex' = '([^ ]*) ([^ ]*) \\[(.*?)\\] ([^ ]*) ([^ ]*) ([^ ]*)
([^ ]*) ([^ ]*) (\"[^\"]*\") ([^ ]*) ([^ ]*) ([^ ]*)'
)
LOCATION
's3://s3-objects-access-log-039c8e9d2cb233518/';
```

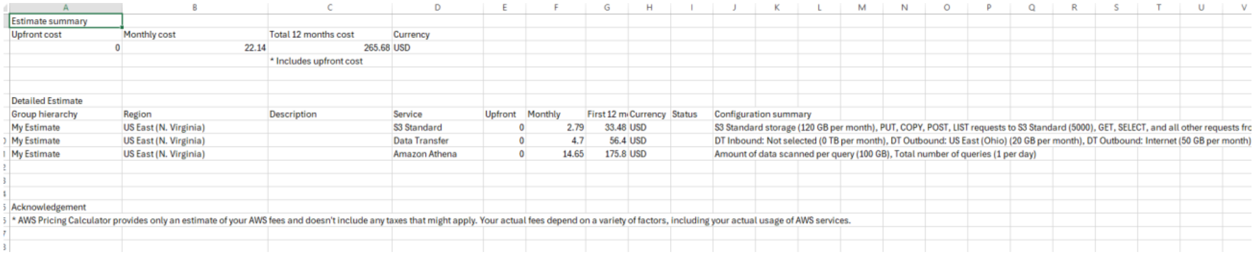
SQL Ln 20, Col 49



Results (228)

#	requester	operation	key	httpstatus
1	arn:aws:iam::147764965649:user/mary	REST.GET.VERSIONING	-	403
2	arn:aws:iam::147764965649:user/sofia	REST.GET.OWNERSHIP_CONTROLS	-	200
3	arn:aws:iam::147764965649:user/paulo	REST.GET.VERSIONING	-	200
4	arn:aws:iam::147764965649:user/mary	REST.GET.INTELLIGENT_TIERING	-	403
5	arn:aws:iam::147764965649:user/paulo	REST.GET.OWNERSHIP_CONTROLS	-	200
6	arn:aws:iam::147764965649:user/paulo	REST.GET.OBJECT_LOCK_CONFIGURATION	-	404
7	arn:aws:iam::147764965649:user/paulo	REST.GET.BUCKETVERSIONS	-	200
8	arn:aws:iam::147764965649:user/paulo	REST.GET.BUCKET	-	200
9	arn:aws:iam::147764965649:user/mary	REST.GET.OWNERSHIP_CONTROLS	-	403
10	arn:aws:iam::147764965649:user/mary	REST.GET.BUCKET	-	403
11	arn:aws:iam::147764965649:user/mary	REST.GET.OWNERSHIP_CONTROLS	-	403
12	arn:aws:iam::147764965649:user/sofia	REST.GET.OWNERSHIP_CONTROLS	-	200
13	arn:aws:iam::147764965649:user/sofia	REST.GET.BUCKET	-	200

Cost estimate



Estimate summary

Upfront cost	Monthly cost	Total 12 months cost	Currency
0	22.14	265.68	USD
		* Includes upfront cost	

Detailed Estimate

Group hierarchy	Region	Description	Service	Upfront	Monthly	First 12 m	Currency	Status	Configuration summary
My Estimate	US East (N. Virginia)		S3 Standard	0	2.79	33.48	USD		S3 Standard storage (120 GB per month), PUT, COPY, POST, LIST requests to S3 Standard (5000), GET, SELECT, and all other requests fro
My Estimate	US East (N. Virginia)		Data Transfer	0	4.7	56.4	USD		DT Inbound: Not selected (0 TB per month), DT Outbound: US East (Ohio) (20 GB per month), DT Outbound: Internet (50 GB per month)
My Estimate	US East (N. Virginia)		Amazon Athena	0	14.65	175.8	USD		Amount of data scanned per query (100 GB), Total number of queries (1 per day)

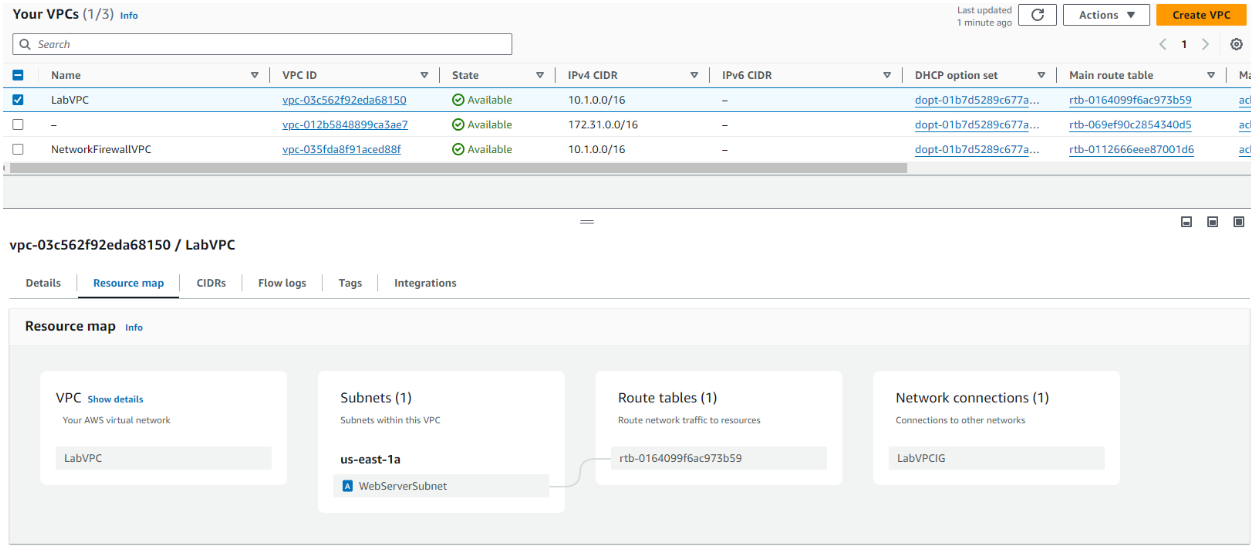
Acknowledgement

* 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.

Phase 2: Securing VPCs

Task 2.1: Review LabVPC and its associated resources

-Reviewing the resources



☐	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table	Ma
☑	LabVPC	vpc-03c562f92eda68150	✓ Available	10.1.0.0/16	–	dopt-01b7d5289c677a...	rtb-0164099f6ac973b59	acl
☐	–	vpc-012b5848899ca3ae7	✓ Available	172.31.0.0/16	–	dopt-01b7d5289c677a...	rtb-069ef90c2854340d5	acl
☐	NetworkFirewallVPC	vpc-035fda8f91aced88f	✓ Available	10.1.0.0/16	–	dopt-01b7d5289c677a...	rtb-0112666eee87001d6	acl

vpc-03c562f92eda68150 / LabVPC

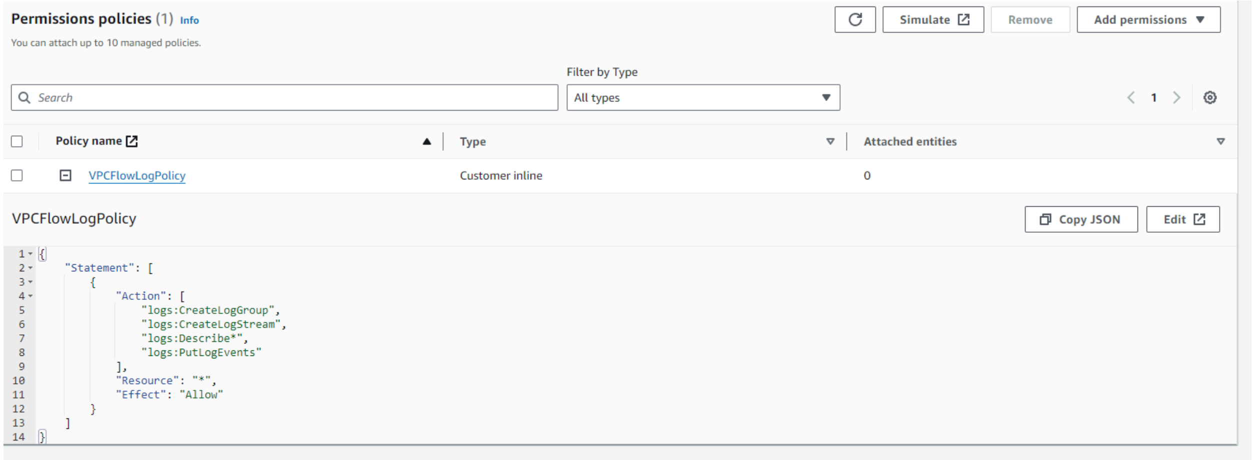
Resource map Info

VPC Show details
Your AWS virtual network
LabVPC

Subnets (1)
Subnets within this VPC
us-east-1a
A WebServerSubnet

Route tables (1)
Route network traffic to resources
rtb-0164099f6ac973b59

Network connections (1)
Connections to other networks
LabVPCIG



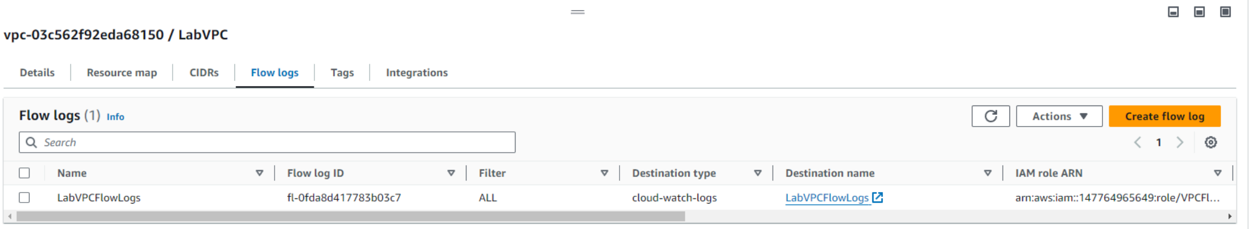
☐	Policy name	Type	Attached entities
☐	VPCFlowLogPolicy	Customer inline	0

VPCFlowLogPolicy

```
{
    "Statement": [
        {
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:Describe*",
                "logs:PutLogEvents"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Task 2.2: Create a VPC flow log

-create a VPC flow log for LabVPC to monitor inbound and outbound traffic

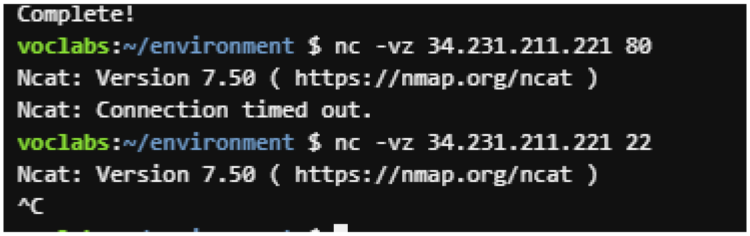


vpc-03c562f92eda68150 / LabVPC

☐	Name	Flow log ID	Filter	Destination type	Destination name	IAM role ARN
☐	LabVPCFlowLogs	fl-0fda8d417783b03c7	ALL	cloud-watch-logs	LabVPCFlowLogs	arn:aws:iam::147764965649:role/VPCFl...

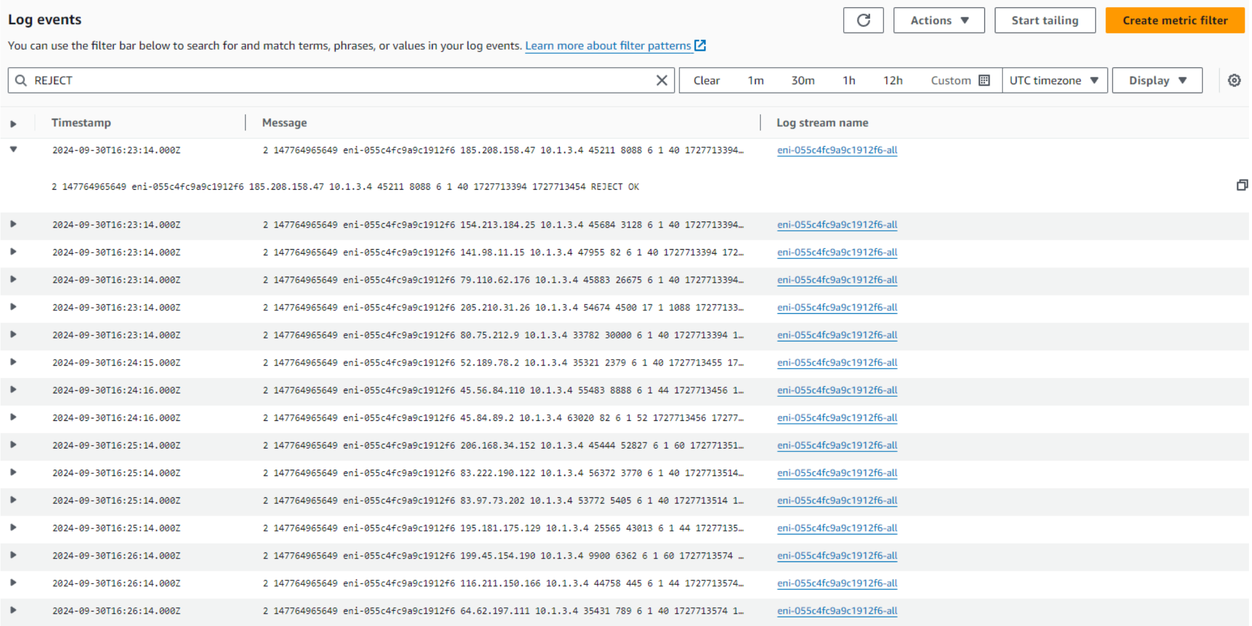
Task 2.3: Access the WebServer instance from the internet and review VPC flow logs in CloudWatch

-This connection will also fail or timeout.



```
Complete!
voclabs:~/environment $ nc -vz 34.231.211.221 80
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connection timed out.
voclabs:~/environment $ nc -vz 34.231.211.221 22
Ncat: Version 7.50 ( https://nmap.org/ncat )
^C
```

Reject:

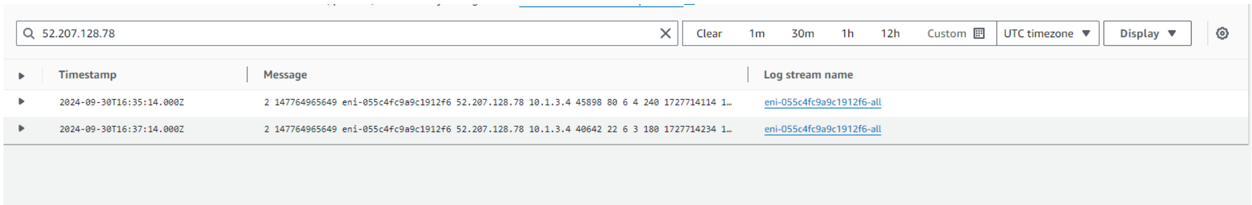


You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns

REJECT

Timestamp	Message	Log stream name
2024-09-30T16:23:14.000Z	2 147764965649 eni-055c4fc9a9c1912f6 185.208.158.47 10.1.3.4 45211 8088 6 1 40 1727713394…	eni-055c4fc9a9c1912f6-all
2 147764965649 eni-055c4fc9a9c1912f6 185.208.158.47 10.1.3.4 45211 8088 6 1 40 1727713394 1727713454 REJECT OK		
2024-09-30T16:23:14.000Z	2 147764965649 eni-055c4fc9a9c1912f6 154.213.184.25 10.1.3.4 45684 3128 6 1 40 1727713394…	eni-055c4fc9a9c1912f6-all
2024-09-30T16:23:14.000Z	2 147764965649 eni-055c4fc9a9c1912f6 141.98.11.15 10.1.3.4 47955 82 6 1 40 1727713394 172…	eni-055c4fc9a9c1912f6-all
2024-09-30T16:23:14.000Z	2 147764965649 eni-055c4fc9a9c1912f6 79.110.62.176 10.1.3.4 45883 26675 6 1 40 1727713394…	eni-055c4fc9a9c1912f6-all
2024-09-30T16:23:14.000Z	2 147764965649 eni-055c4fc9a9c1912f6 205.210.31.26 10.1.3.4 54674 4500 17 1 1088 17277133…	eni-055c4fc9a9c1912f6-all
2024-09-30T16:23:14.000Z	2 147764965649 eni-055c4fc9a9c1912f6 80.75.212.9 10.1.3.4 33782 30000 6 1 40 1727713394 1…	eni-055c4fc9a9c1912f6-all
2024-09-30T16:24:15.000Z	2 147764965649 eni-055c4fc9a9c1912f6 52.189.78.2 10.1.3.4 35321 2379 6 1 40 1727713455 17…	eni-055c4fc9a9c1912f6-all
2024-09-30T16:24:16.000Z	2 147764965649 eni-055c4fc9a9c1912f6 45.56.84.110 10.1.3.4 55483 8888 6 1 44 1727713456 1…	eni-055c4fc9a9c1912f6-all
2024-09-30T16:24:16.000Z	2 147764965649 eni-055c4fc9a9c1912f6 45.84.89.2 10.1.3.4 63020 82 6 1 52 1727713456 17277…	eni-055c4fc9a9c1912f6-all
2024-09-30T16:25:14.000Z	2 147764965649 eni-055c4fc9a9c1912f6 206.168.34.152 10.1.3.4 45444 52827 6 1 60 172771351…	eni-055c4fc9a9c1912f6-all
2024-09-30T16:25:14.000Z	2 147764965649 eni-055c4fc9a9c1912f6 83.222.190.122 10.1.3.4 56372 3770 6 1 40 1727713514…	eni-055c4fc9a9c1912f6-all
2024-09-30T16:25:14.000Z	2 147764965649 eni-055c4fc9a9c1912f6 83.97.73.202 10.1.3.4 53772 5405 6 1 40 1727713514 1…	eni-055c4fc9a9c1912f6-all
2024-09-30T16:25:14.000Z	2 147764965649 eni-055c4fc9a9c1912f6 195.181.175.129 10.1.3.4 25565 43013 6 1 44 17277135…	eni-055c4fc9a9c1912f6-all
2024-09-30T16:26:14.000Z	2 147764965649 eni-055c4fc9a9c1912f6 199.45.154.190 10.1.3.4 9900 6362 6 1 60 1727713574 …	eni-055c4fc9a9c1912f6-all
2024-09-30T16:26:14.000Z	2 147764965649 eni-055c4fc9a9c1912f6 116.211.150.166 10.1.3.4 44758 445 6 1 44 1727713574…	eni-055c4fc9a9c1912f6-all
2024-09-30T16:26:14.000Z	2 147764965649 eni-055c4fc9a9c1912f6 64.62.197.111 10.1.3.4 35431 789 6 1 40 1727713574 1…	eni-055c4fc9a9c1912f6-all

Cloud9:



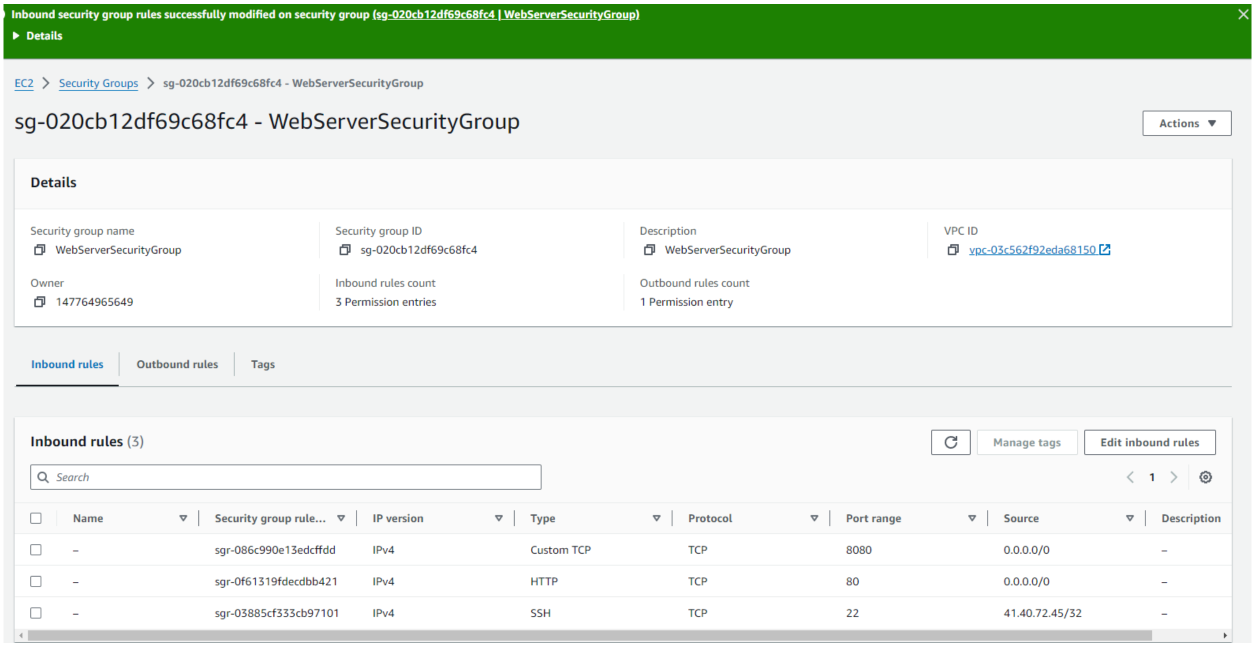
52.207.128.78

Timestamp	Message	Log stream name
2024-09-30T16:35:14.000Z	2 147764965649 eni-055c4fc9a9c1912f6 52.207.128.78 10.1.3.4 45898 80 6 4 240 1727714114 1…	eni-055c4fc9a9c1912f6-all
2024-09-30T16:37:14.000Z	2 147764965649 eni-055c4fc9a9c1912f6 52.207.128.78 10.1.3.4 40642 22 6 3 180 1727714234 1…	eni-055c4fc9a9c1912f6-all

Task 2.4: Configure route table and security group settings

-Change webserver security group,allow http and ssh

-Added a route in the route table associated with the WebServerSubnet to direct traffic to and from the internet (0.0.0.0/0) through the existing internet gateway (LabVPCIG).



Inbound security group rules successfully modified on security group (sg-020cb12df69c68fc4 | WebServerSecurityGroup)

▶ Details

EC2 > Security Groups > sg-020cb12df69c68fc4 - WebServerSecurityGroup

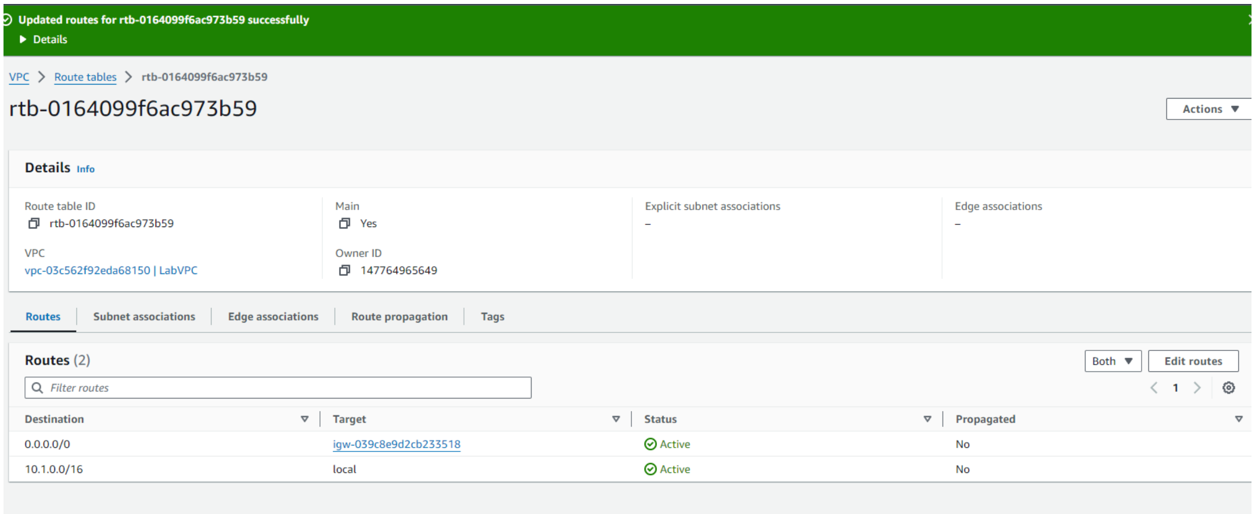
sg-020cb12df69c68fc4 - WebServerSecurityGroup

Details

Security group name WebServerSecurityGroup	Security group ID sg-020cb12df69c68fc4	Description WebServerSecurityGroup	VPC ID vpc-03c562f92eda68150
Owner 147764965649	Inbound rules count 3 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules (3)

□	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
□	–	sgr-086c990e13edcffdd	IPv4	Custom TCP	TCP	8080	0.0.0.0/0	–
□	–	sgr-0f61319fdecdbb421	IPv4	HTTP	TCP	80	0.0.0.0/0	–
□	–	sgr-03885cf333cb97101	IPv4	SSH	TCP	22	41.40.72.45/32	–



Updated routes for rtb-0164099f6ac973b59 successfully

▶ Details

VPC > Route tables > rtb-0164099f6ac973b59

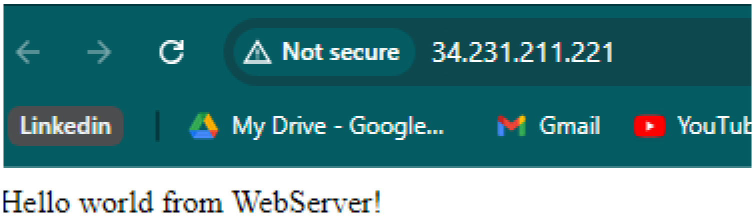
rtb-0164099f6ac973b59

Details Info

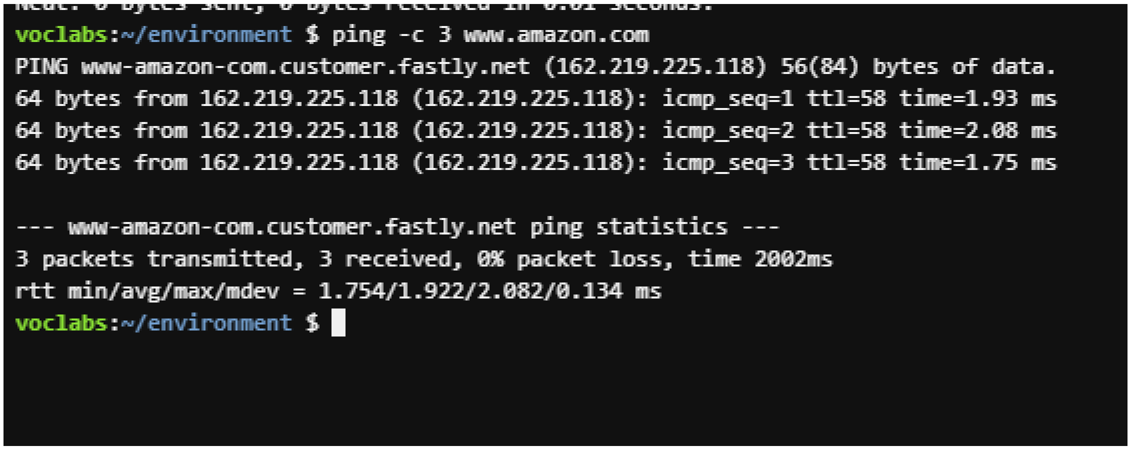
Route table ID rtb-0164099f6ac973b59	Main Yes	Explicit subnet associations –	Edge associations –
VPC vpc-03c562f92eda68150 | LabVPC	Owner ID 147764965649		

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-039c8e9d2cb233518	✓ Active	No
10.1.0.0/16	local	✓ Active	No



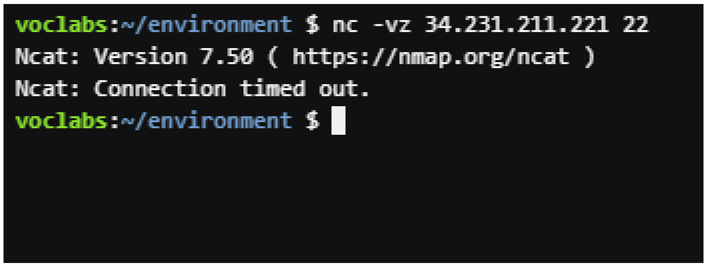
Hello world from WebServer!



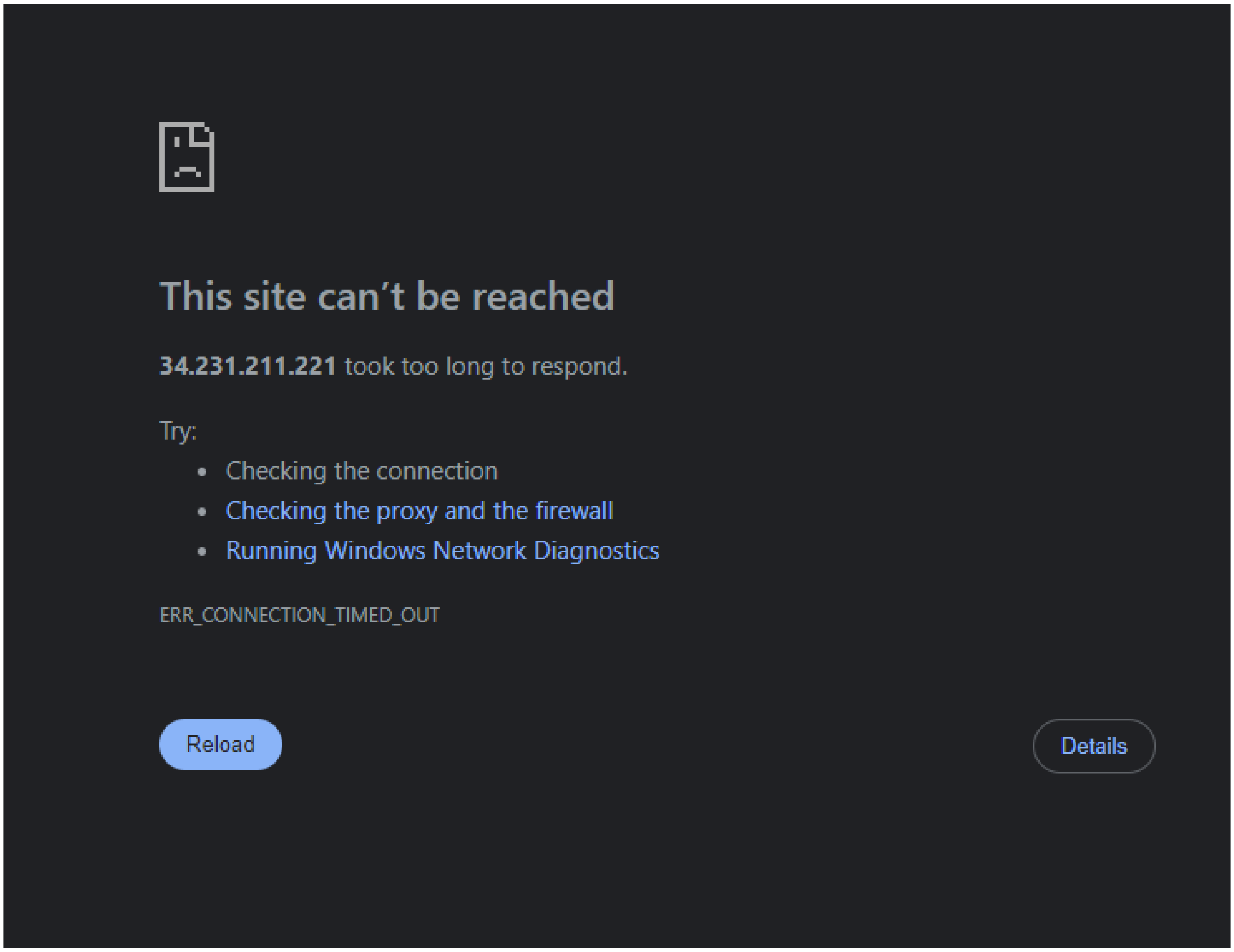
```
Ncat: 0 bytes sent, 0 bytes received in 0.01 seconds.
voclabs:~/environment $ ping -c 3 www.amazon.com
PING www-amazon-com.customer.fastly.net (162.219.225.118) 56(84) bytes of data.
64 bytes from 162.219.225.118 (162.219.225.118): icmp_seq=1 ttl=58 time=1.93 ms
64 bytes from 162.219.225.118 (162.219.225.118): icmp_seq=2 ttl=58 time=2.08 ms
64 bytes from 162.219.225.118 (162.219.225.118): icmp_seq=3 ttl=58 time=1.75 ms

--- www-amazon-com.customer.fastly.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 1.754/1.922/2.082/0.134 ms
voclabs:~/environment $ 
```

Task 2.5: Secure the WebServerSubnet with a network ACL

-After changing ACl ssh and web failed as we changed the rule from allow to deny



```
voclabs:~/environment $ nc -vz 34.231.211.221 22
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connection timed out.
voclabs:~/environment $ 
```



This site can’t be reached

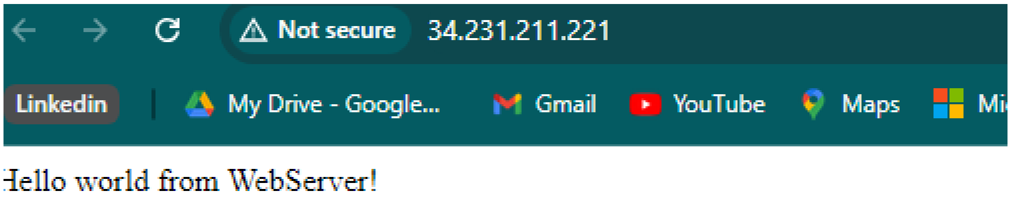
34.231.211.221 took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

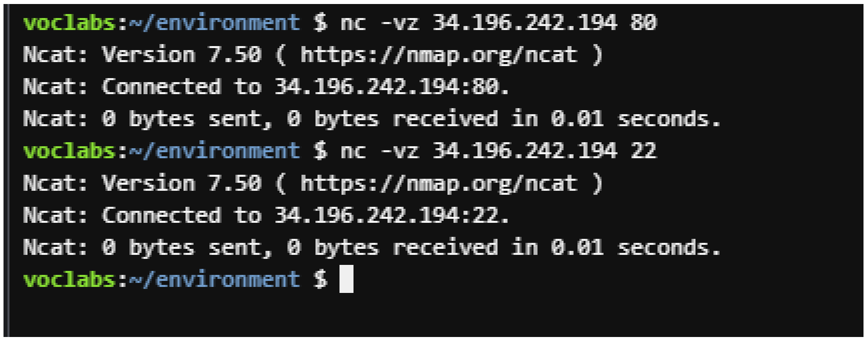
ERR_CONNECTION_TIMED_OUT

-After changing ACl again it worked fine , as we allowed http in rule 90

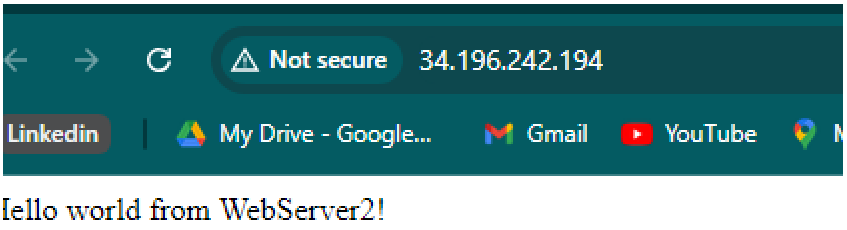


Hello world from WebServer!

Task 2.6: Review NetworkFirewallVPC and its associated resources

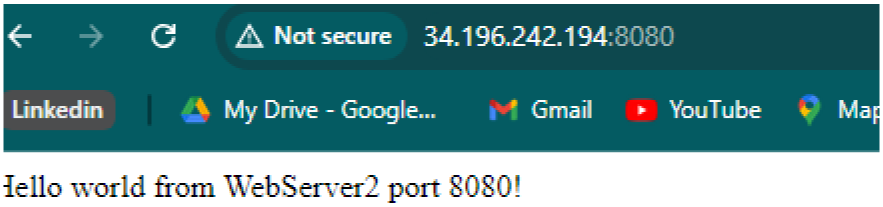


```
voclabs:~/environment $ nc -vz 34.196.242.194 80
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connected to 34.196.242.194:80.
Ncat: 0 bytes sent, 0 bytes received in 0.01 seconds.
voclabs:~/environment $ nc -vz 34.196.242.194 22
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connected to 34.196.242.194:22.
Ncat: 0 bytes sent, 0 bytes received in 0.01 seconds.
voclabs:~/environment $
```



Iello world from WebServer2!

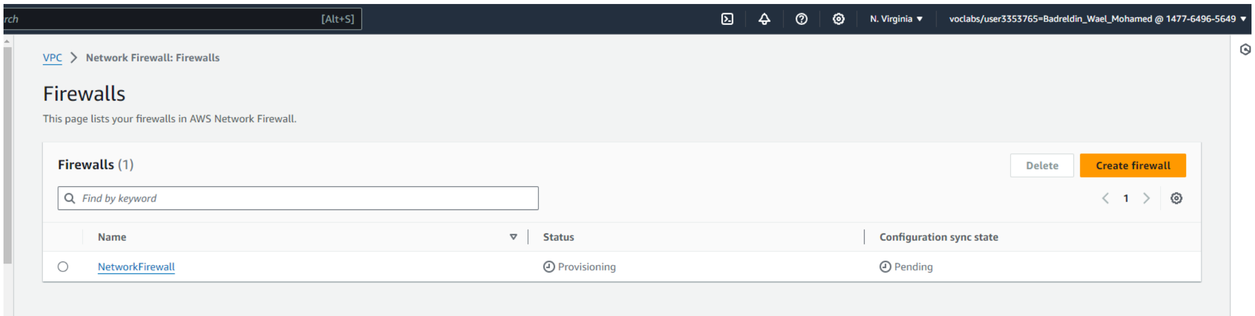
-USING PORT8080



Iello world from WebServer2 port 8080!

Task 2.7: Create a network firewall

-creating firewall



rch [Alt+S]
N. Virginia ▼
voclabs/user3353765=Badreldin_Wael_Mohamed @ 1477-6496-5649 ▼

VPC > Network Firewall: Firewalls

Firewalls

This page lists your firewalls in AWS Network Firewall.

Firewalls (1)

Delete
Create firewall
Find by keyword
1

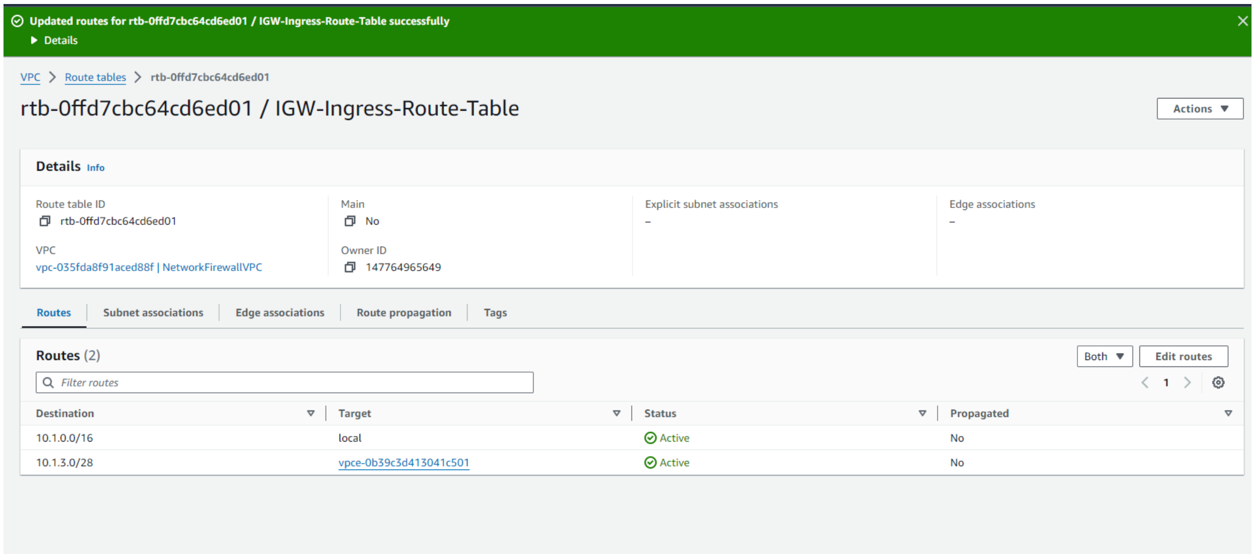
	Name	Status	Configuration sync state
○	NetworkFirewall	Provisioning	Pending

Task 2.8: Create route tables

-Create IGW-Ingress-Route-Table

-Create Firewall-Route-Table

-Create WebServer2-Route-Table



Updated routes for rtb-0ffd7cbc64cd6ed01 / IGW-Ingress-Route-Table successfully

VPC > Route tables > rtb-0ffd7cbc64cd6ed01

rtb-0ffd7cbc64cd6ed01 / IGW-Ingress-Route-Table

Details Info

Route table ID: rtb-0ffd7cbc64cd6ed01

Main: No

Explicit subnet associations: –

Edge associations: –

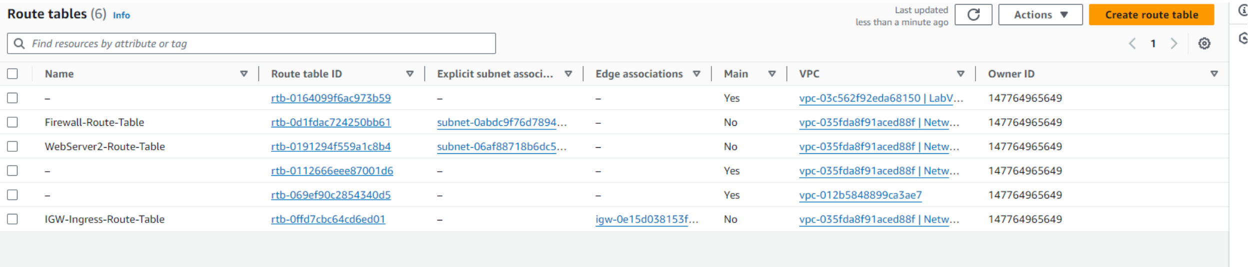
VPC: vpc-035fda8f91aced88f | NetworkFirewallVPC

Owner ID: 147764965649

Routes (2)

Destination	Target	Status	Propagated
10.1.0.0/16	local	Active	No
10.1.3.0/28	vpce-0b39c3d413041c501	Active	No

Route tables



Route tables (6) Info

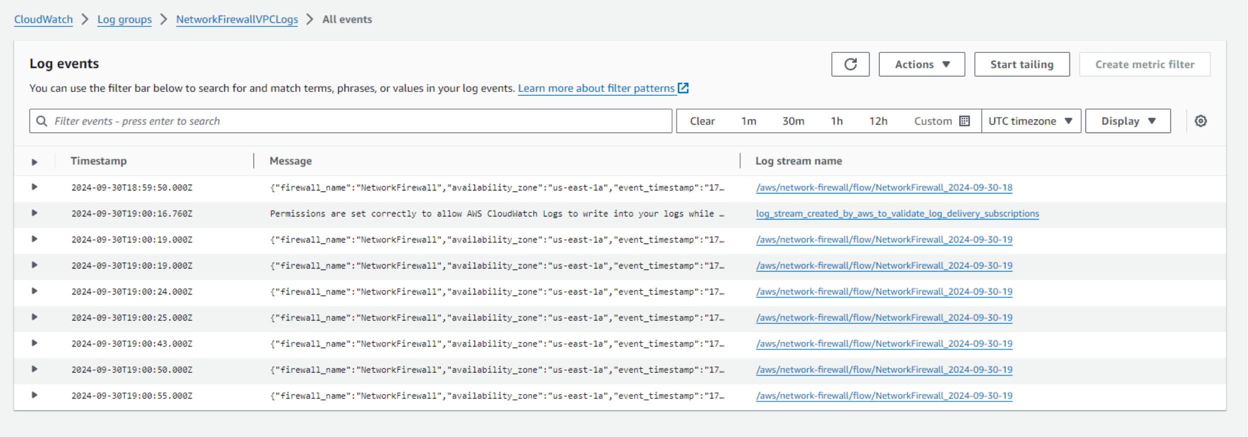
□	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC	Owner ID
□	–	rtb-0164099f6ac973b59	–	–	Yes	vpc-03c562f92eda68150 | LabV...	147764965649
□	Firewall-Route-Table	rtb-0d1fdac724250bb61	subnet-0abdc9f76d7894...	–	No	vpc-035fda8f91aced88f | Netw...	147764965649
□	WebServer2-Route-Table	rtb-0191294f559a1c8b4	subnet-06af88718b6dc5...	–	No	vpc-035fda8f91aced88f | Netw...	147764965649
□	–	rtb-0112666eee87001d6	–	–	Yes	vpc-035fda8f91aced88f | Netw...	147764965649
□	–	rtb-069ef90c2854340d5	–	–	Yes	vpc-012b5848899ca3ae7	147764965649
□	IGW-Ingress-Route-Table	rtb-0ffd7cbc64cd6ed01	–	igw-0e15d038153f...	No	vpc-035fda8f91aced88f | Netw...	147764965649

Task 2.9: Configure logging for the network firewall

-Create a CloudWatch Log Group

-Configure Firewall Logging

-Test Logging Configuration


CloudWatch > Log groups > NetworkFirewallVPCLogs > All events
Actions
Start tailing
Create metric filter
Filter events - press enter to search
Clear
1m
30m
1h
12h
Custom
UTC timezone
Display

Log events

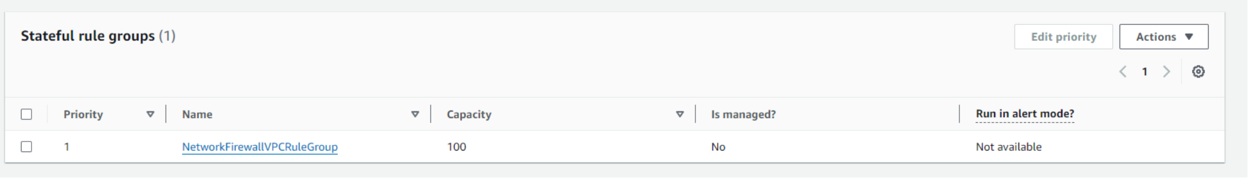
You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns

Timestamp	Message	Log stream name
2024-09-30T18:59:50.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"17…	/aws/network-firewall/flow/NetworkFirewall_2024-09-30-18
2024-09-30T19:00:16.760Z	Permissions are set correctly to allow AWS CloudWatch Logs to write into your logs while …	log_stream_created_by_aws_to_validate_log_delivery_subscriptions
2024-09-30T19:00:19.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"17…	/aws/network-firewall/flow/NetworkFirewall_2024-09-30-19
2024-09-30T19:00:19.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"17…	/aws/network-firewall/flow/NetworkFirewall_2024-09-30-19
2024-09-30T19:00:24.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"17…	/aws/network-firewall/flow/NetworkFirewall_2024-09-30-19
2024-09-30T19:00:25.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"17…	/aws/network-firewall/flow/NetworkFirewall_2024-09-30-19
2024-09-30T19:00:43.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"17…	/aws/network-firewall/flow/NetworkFirewall_2024-09-30-19
2024-09-30T19:00:50.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"17…	/aws/network-firewall/flow/NetworkFirewall_2024-09-30-19
2024-09-30T19:00:55.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"17…	/aws/network-firewall/flow/NetworkFirewall_2024-09-30-19

Task 2.10: Configure the firewall policy and test access

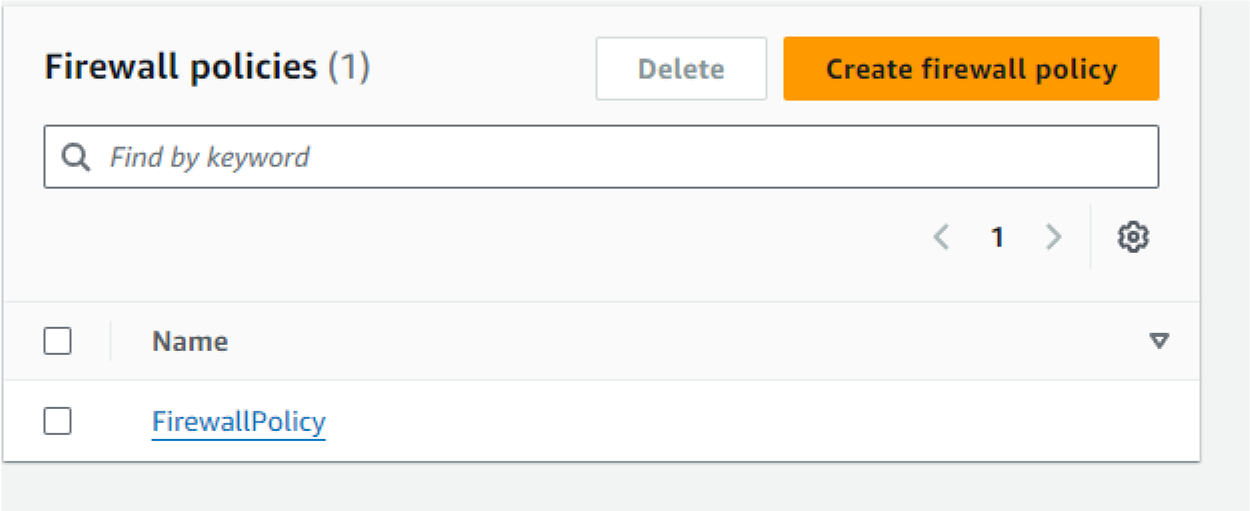
-Create a Rule Group(pass:80,22,443.Drop:8080)

-Create firewall policy



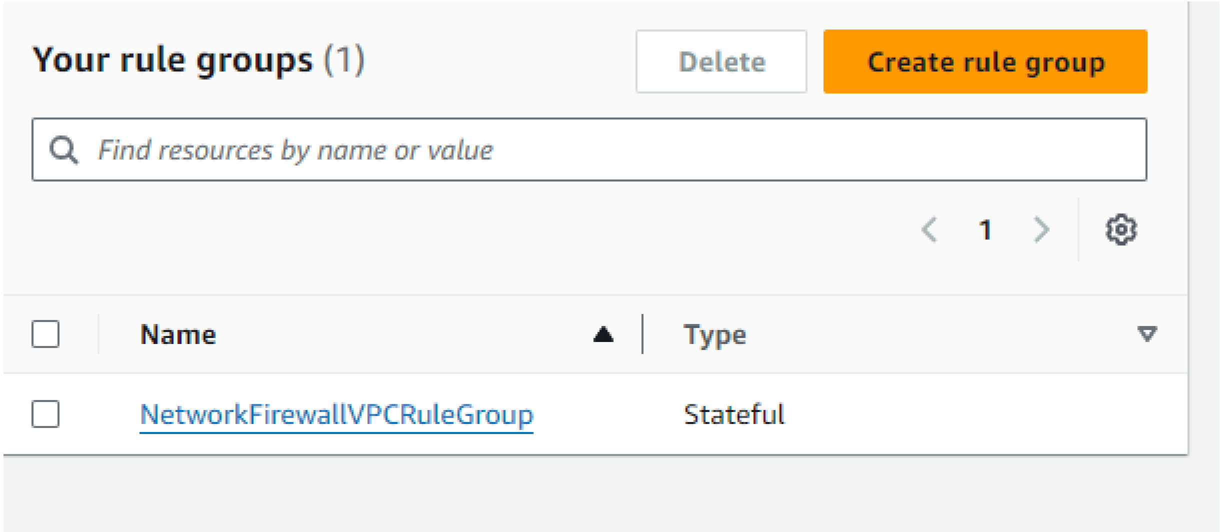
Stateful rule groups (1)

☐	Priority	Name	Capacity	Is managed?	Run in alert mode?
☐	1	NetworkFirewallVPCRuleGroup	100	No	Not available



Firewall policies (1)

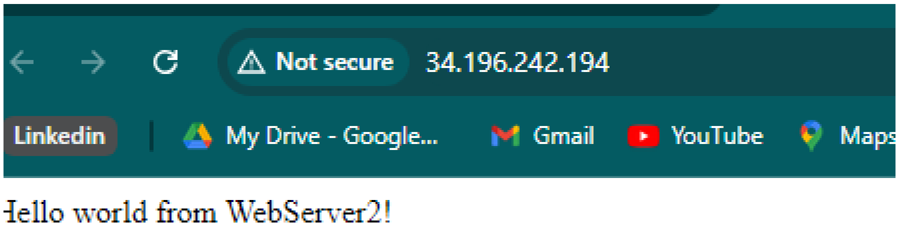
□	Name
□	FirewallPolicy



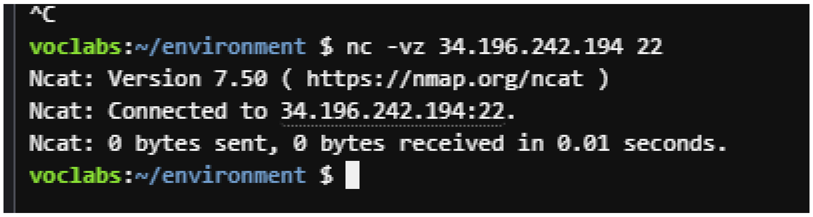
Your rule groups (1)

□	Name	Type
□	NetworkFirewallVPCRuleGroup	Stateful

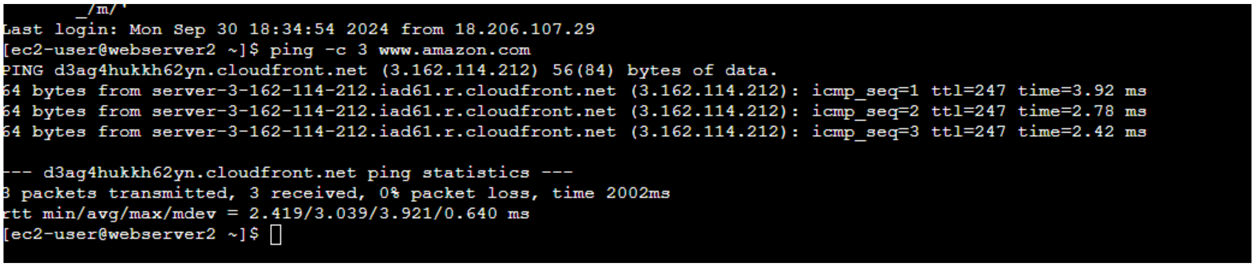
Testing:



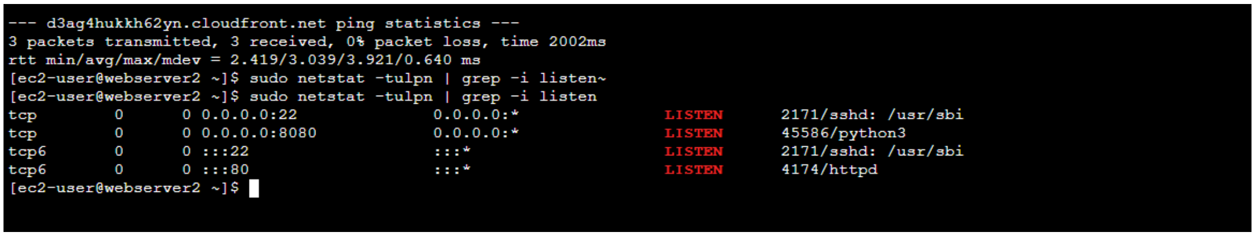
Hello world from WebServer2!



```
^C
voclabs:~/environment $ nc -vz 34.196.242.194 22
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connected to 34.196.242.194:22.
Ncat: 0 bytes sent, 0 bytes received in 0.01 seconds.
voclabs:~/environment $
```

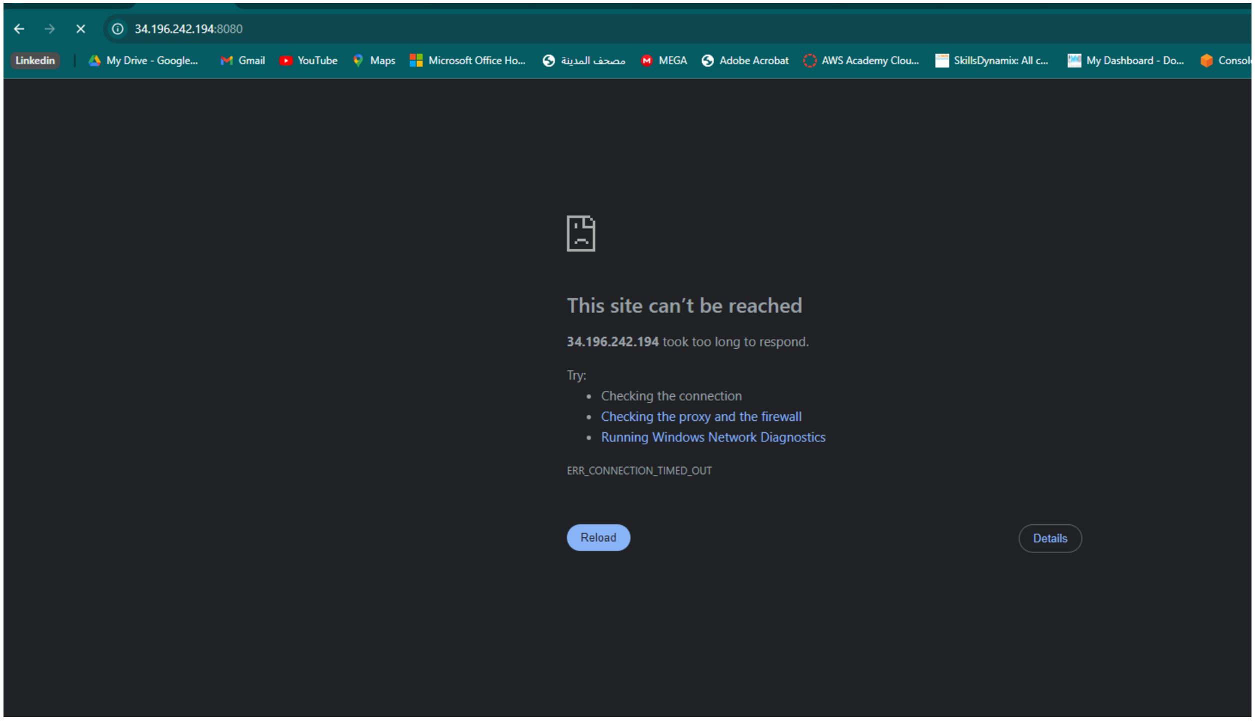


```
       _/m/'
Last login: Mon Sep 30 18:34:54 2024 from 18.206.107.29
[ec2-user@webserver2 ~]$ ping -c 3 www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (3.162.114.212) 56(84) bytes of data.
64 bytes from server-3-162-114-212.iad61.r.cloudfront.net (3.162.114.212): icmp_seq=1 ttl=247 time=3.92 ms
64 bytes from server-3-162-114-212.iad61.r.cloudfront.net (3.162.114.212): icmp_seq=2 ttl=247 time=2.78 ms
64 bytes from server-3-162-114-212.iad61.r.cloudfront.net (3.162.114.212): icmp_seq=3 ttl=247 time=2.42 ms

--- d3ag4hukkh62yn.cloudfront.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 2.419/3.039/3.921/0.640 ms
[ec2-user@webserver2 ~]$
```



```
--- d3ag4hukkh62yn.cloudfront.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 2.419/3.039/3.921/0.640 ms
[ec2-user@webserver2 ~]$ sudo netstat -tulpn | grep -i listen~
[ec2-user@webserver2 ~]$ sudo netstat -tulpn | grep -i listen
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2171/sshd: /usr/sbi
tcp        0      0 0.0.0.0:8080            0.0.0.0:*               LISTEN      45586/python3
tcp6       0      0 :::22                   :::*                    LISTEN      2171/sshd: /usr/sbi
tcp6       0      0 :::80                   :::*                    LISTEN      4174/httpd
[ec2-user@webserver2 ~]$
```

-Using 8080 that was dropped



This site can’t be reached

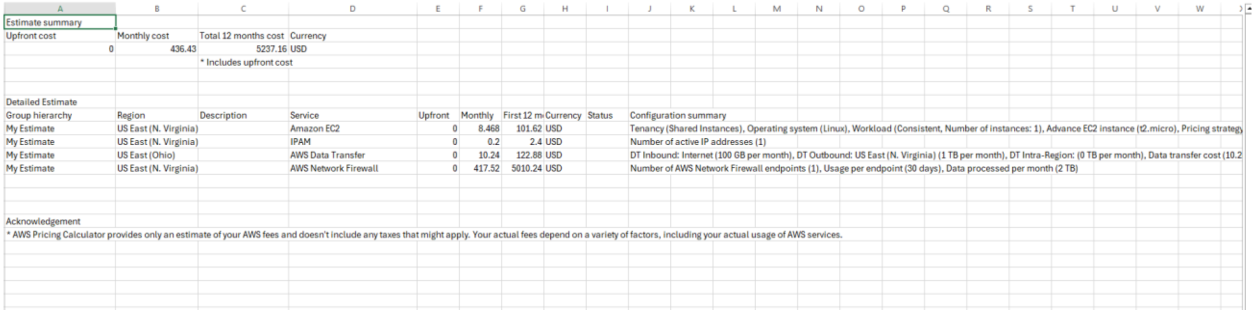
34.196.242.194 took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

Cost estimation



Estimate summary

Upfront cost	Monthly cost	Total 12 months cost	Currency
0	436.43	5237.16	USD
		* Includes upfront cost	

Detailed Estimate

Group hierarchy	Region	Description	Service	Upfront	Monthly	First 12 m	Currency	Status	Configuration summary
My Estimate	US East (N. Virginia)		Amazon EC2	0	8.468	101.62	USD		Tenancy (Shared Instances), Operating system (Linux), Workload (Consistent, Number of instances: 1), Advance EC2 instance (t2.micro), Pricing strategy
My Estimate	US East (N. Virginia)		IPAM	0	0.2	2.4	USD		Number of active IP addresses (1)
My Estimate	US East (Ohio)		AWS Data Transfer	0	10.24	122.88	USD		DT Inbound: Internet (100 GB per month), DT Outbound: US East (N. Virginia) (1 TB per month), DT Intra-Region: (0 TB per month), Data transfer cost (10.2
My Estimate	US East (N. Virginia)		AWS Network Firewall	0	417.52	5010.24	USD		Number of AWS Network Firewall endpoints (1), Usage per endpoint (30 days), Data processed per month (2 TB)

Acknowledgement

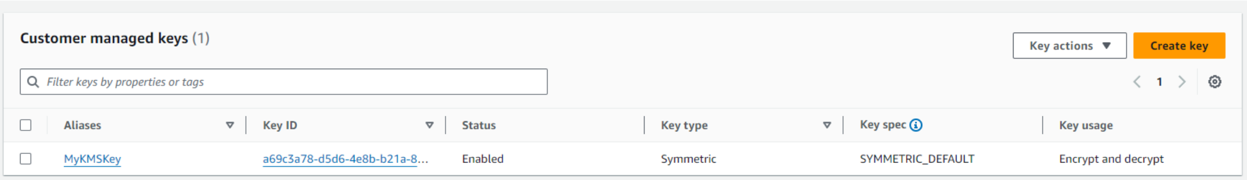
* AWS Pricing Calculator provides only an estimate of your AWS fees and doesn't include any taxes that might apply. Your actual fees depend on a variety of factors, including your actual usage of AWS services.

Phase 3: Securing AWS resources by using AWS KMS

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

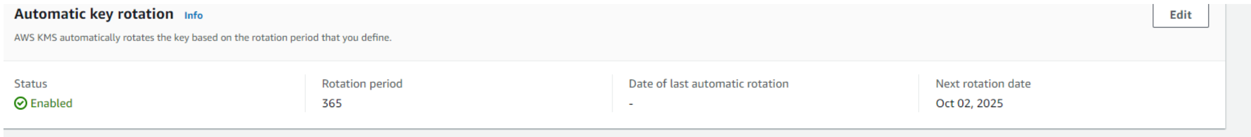
-Create a Customer Managed Key

-Configure Automatic Key Rotation



Customer managed keys (1)

☐	Aliases	Key ID	Status	Key type	Key spec	Key usage
☐	MyKMSKey	a69c3a78-d5d6-4e8b-b21a-8...	Enabled	Symmetric	SYMMETRIC_DEFAULT	Encrypt and decrypt



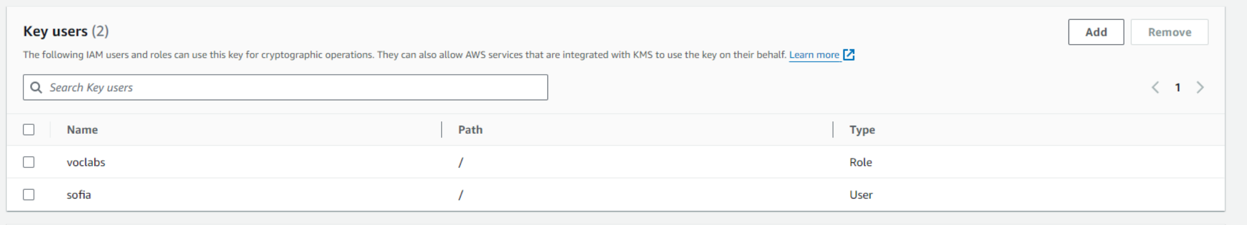
Automatic key rotation Info

AWS KMS automatically rotates the key based on the rotation period that you define.

Status	Rotation period	Date of last automatic rotation	Next rotation date
✓ Enabled	365	-	Oct 02, 2025

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

-Modify the AWS KMS key policy to authorize the sofia user to use the key



Key users (2)

The following IAM users and roles can use this key for cryptographic operations. They can also allow AWS services that are integrated with KMS to use the key on their behalf. Learn more

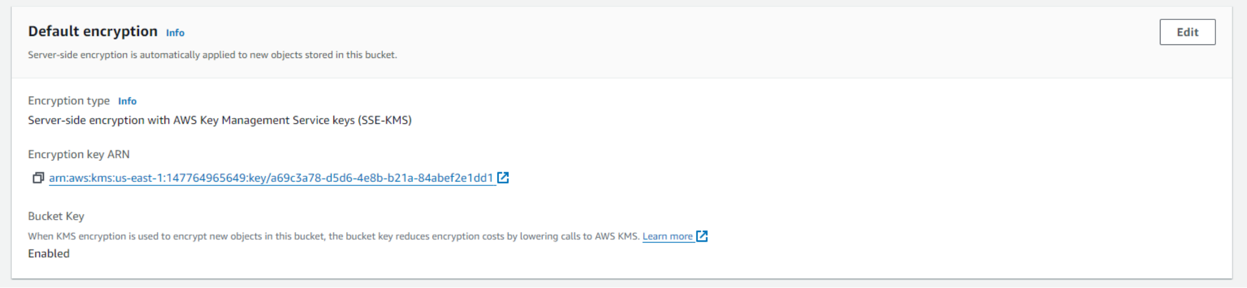
☐	Name	Path	Type
☐	voclabs	/	Role
☐	sofia	/	User

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

-Change the encryption settings on the data-bucket S3 bucket to use SSE-KMS encryption.

-Create a CSV File

-Analyze Encryption Settings



Default encryption Info

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

Encryption type Info

Server-side encryption with AWS Key Management Service keys (SSE-KMS)

Encryption key ARN

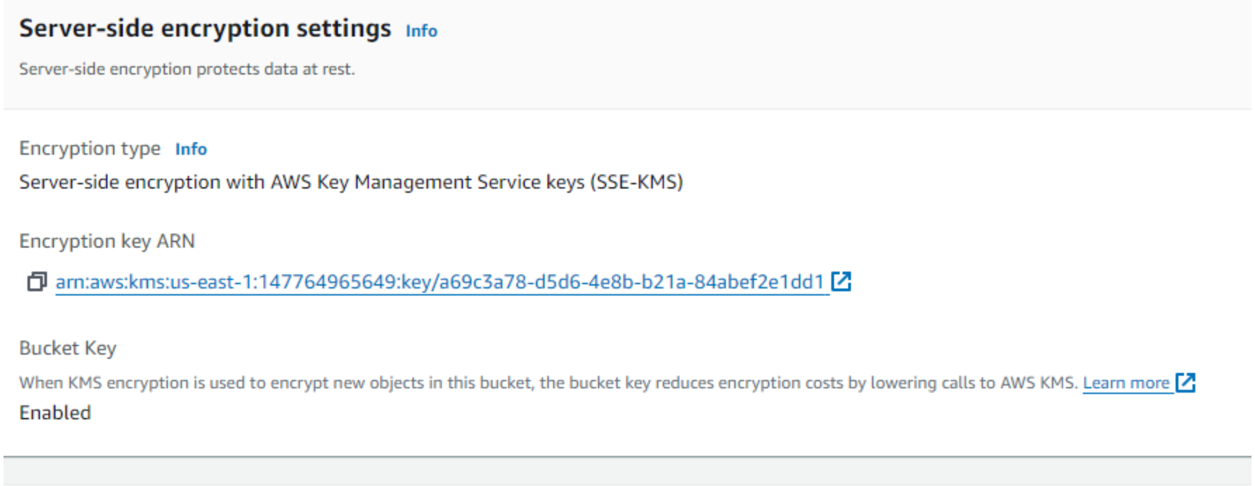
arn:aws:kms:us-east-1:147764965649:key/a69c3a78-d5d6-4e8b-b21a-84abef2e1dd1

Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. Learn more

Enabled

Encrypt loan data



Server-side encryption settings Info

Server-side encryption protects data at rest.

Encryption type Info

Server-side encryption with AWS Key Management Service keys (SSE-KMS)

Encryption key ARN

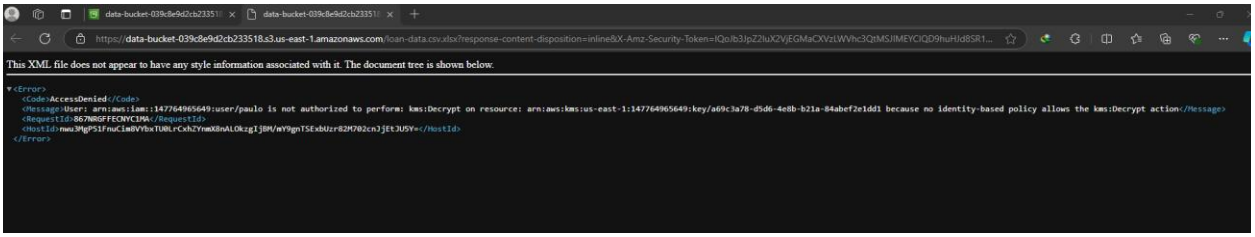
arn:aws:kms:us-east-1:147764965649:key/a69c3a78-d5d6-4e8b-b21a-84abef2e1dd1

Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. Learn more

Enabled

-Paolo messages unable to access the encrypted file due to lacking permissions in the KMS key policy



https://data-bucket-039c8e9d2cb233518.s3.us-east-1.amazonaws.com/loan-data.csv.xlsx?response-content-disposition=inline&X-Amz-Security-Token=IQoJb3JpZ2luX2VjEGMaCXVzLWVhc3QtMSJIMEYCIQD9huHJd8SR1...

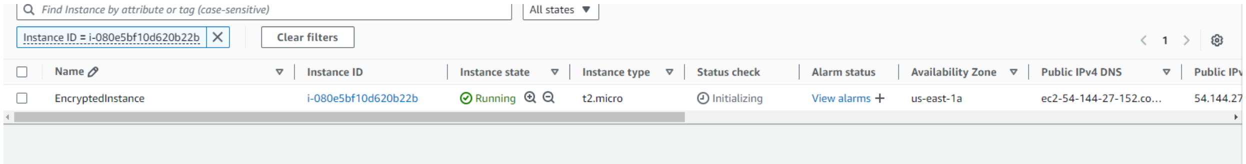
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<Error>
   <Code>AccessDenied</Code>
   <Message>User: arn:aws:iam::147764965649:user/paulo is not authorized to perform: kms:Decrypt on resource: arn:aws:kms:us-east-1:147764965649:key/a69c3a78-d5d6-4e8b-b21a-84abef2e1dd1 because no identity-based policy allows the kms:Decrypt action</Message>
   <RequestId>867NRGFFECNYC1MA</RequestId>
   <HostId>nwu3MgP51FnuCim8VYbxTU0LrCxhZYnmX8nALOkzgIjBM/mY9gnTSExbUzr82M702cnJjEtJU5Y=</HostId>
 </Error>
```

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

-Create EC2 Instance

-Select to encrypt the AMI root volume using MyKMSKey.

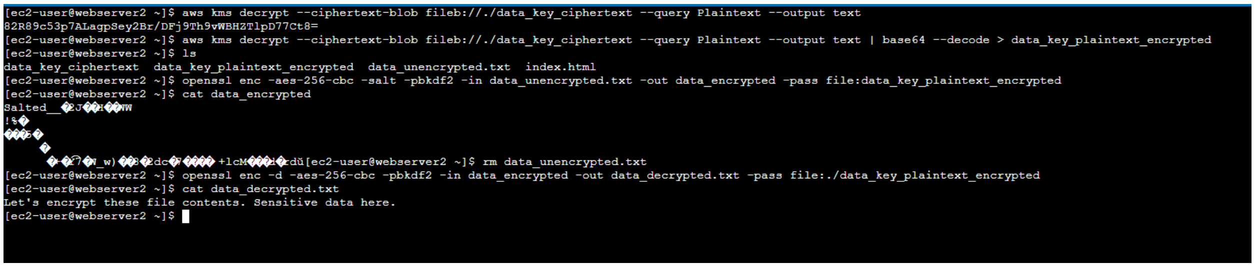


Find Instance by attribute or tag (case-sensitive)
All states
Instance ID = i-080e5bf10d620b22b
Clear filters
1

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv
□	EncryptedInstance	i-080e5bf10d620b22b	Running	t2.micro	Initializing	View alarms +	us-east-1a	ec2-54-144-27-152.co...	54.144.27

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

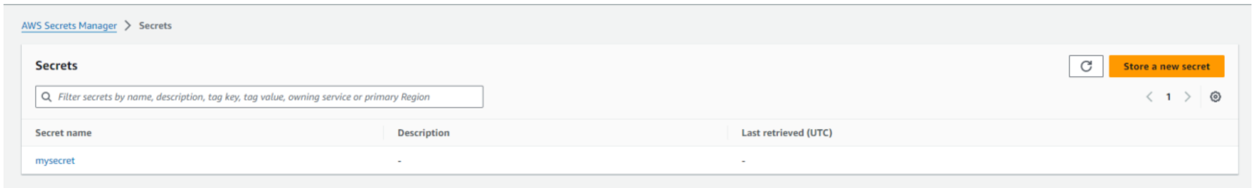
-Encrypt sensitive data at rest



```
[ec2-user@webserver2 ~]$ aws kms decrypt --ciphertext-blob fileb://./data_key_ciphertext --query Plaintext --output text
82R89c53p7ALagpSey2Br/DFj9Th9vWBHZTlpD77Ct8=
[ec2-user@webserver2 ~]$ aws kms decrypt --ciphertext-blob fileb://./data_key_ciphertext --query Plaintext --output text | base64 --decode > data_key_plaintext_encrypted
[ec2-user@webserver2 ~]$ ls
data_key_ciphertext  data_key_plaintext_encrypted  data_unencrypted.txt  index.html
[ec2-user@webserver2 ~]$ openssl enc -aes-256-cbc -salt -pbkdf2 -in data_unencrypted.txt -out data_encrypted -pass file:data_key_plaintext_encrypted
[ec2-user@webserver2 ~]$ cat data_encrypted
Salted__�2J��H��NW
!%�
���5�
     �
      ��7�W_w)��8�2dc�7���� +lcM���d�rdũ[ec2-user@webserver2 ~]$ rm data_unencrypted.txt
[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 ~]$ 
```

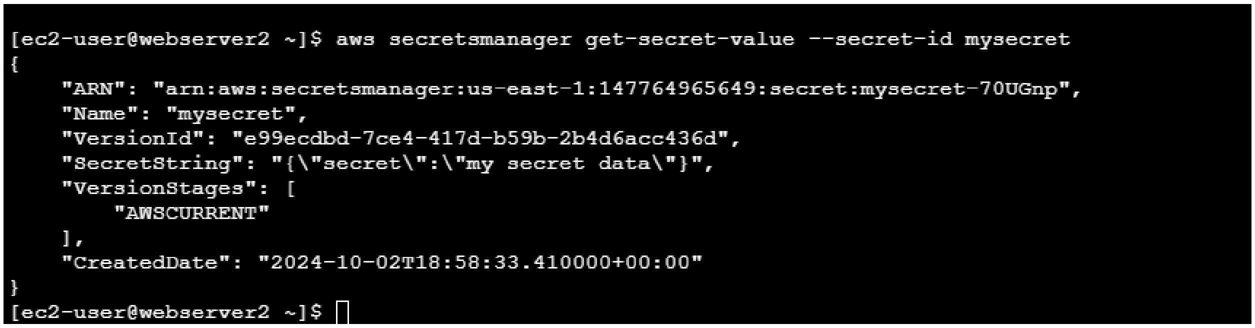
Task 3.6: Use AWS KMS to encrypt a Secrets Manager secret

-Created a secret in AWS Secrets Manager, encrypting it with your KMS key, which adds an additional layer of security



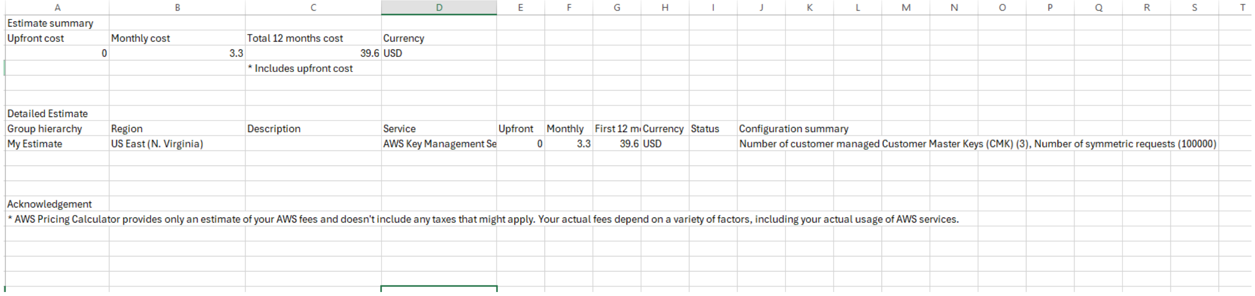
AWS Secrets Manager > Secrets
Secrets
Store a new secret
Filter secrets by name, description, tag key, tag value, owning service or primary Region
1

Secret name	Description	Last retrieved (UTC)
mysecret	-	-



```
[ec2-user@webserver2 ~]$ aws secretsmanager get-secret-value --secret-id mysecret
{
    "ARN": "arn:aws:secretsmanager:us-east-1:147764965649:secret:mysecret-70UGnp",
    "Name": "mysecret",
    "VersionId": "e99ecdbd-7ce4-417d-b59b-2b4d6acc436d",
    "SecretString": "{\"secret\":\"my secret data\"}",
    "VersionStages": [
        "AWSCURRENT"
    ],
    "CreatedDate": "2024-10-02T18:58:33.410000+00:00"
}
[ec2-user@webserver2 ~]$ 
```

Cost Estimation



A	B	C	D	E	F	G	H	I	J
Estimate summary									
Upfront cost	Monthly cost	Total 12 months cost	Currency						
0	3.3	39.6	USD						
		* Includes upfront cost							
Detailed Estimate									
Group hierarchy	Region	Description	Service	Upfront	Monthly	First 12 m	Currency	Status	Configuration summary
My Estimate	US East (N. Virginia)		AWS Key Management Se	0	3.3	39.6	USD		Number of customer managed Customer Master Keys (CMK) (3), Number of symmetric requests (100000)
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.									

Phase 4: Monitoring and logging

Task 4.1: Use CloudTrail to record Amazon S3 API calls

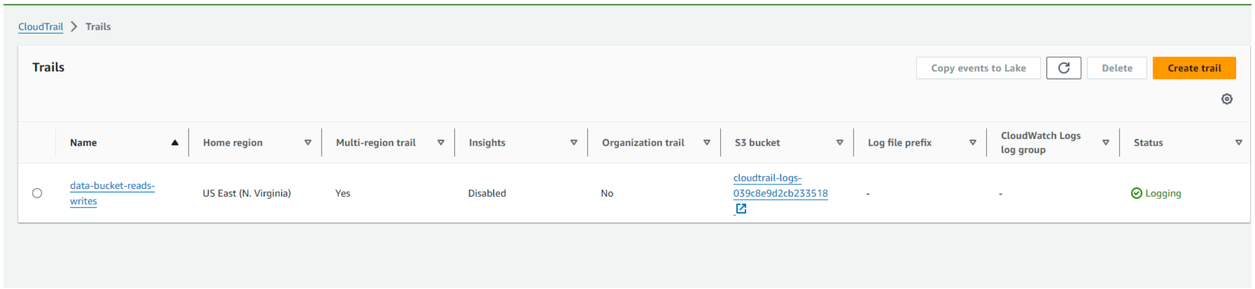
-Create a CloudTrail Trail

-Create the customer-data.csv File

-Upload the File to the S3 Bucket

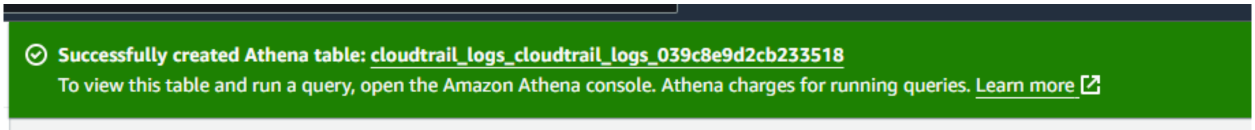
-Create an Athena Table for CloudTrail Logs

-Run the Athena Query

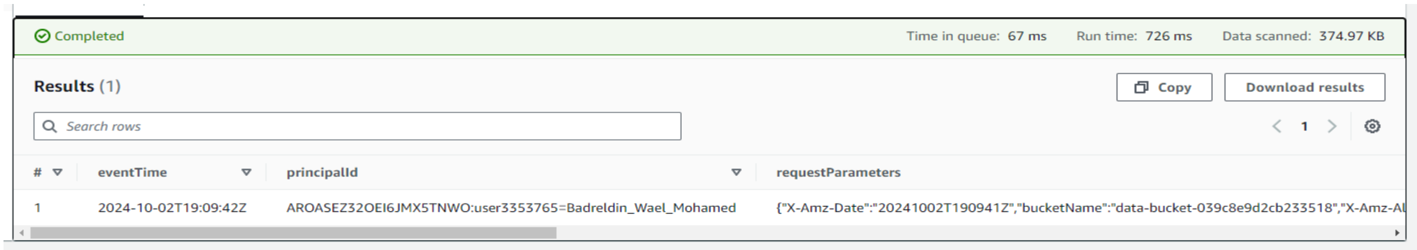


Trails

	Name	Home region	Multi-region trail	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
○	data-bucket-reads-writes	US East (N. Virginia)	Yes	Disabled	No	cloudtrail-logs-039c8e9d2cb233518	-	-	✓ Logging



Successfully created Athena table: cloudtrail_logs_cloudtrail_logs_039c8e9d2cb233518
To view this table and run a query, open the Amazon Athena console. Athena charges for running queries. Learn more



✓ Completed Time in queue: 67 ms Run time: 726 ms Data scanned: 374.97 KB

Results (1)

#	eventTime	principalId	requestParameters
1	2024-10-02T19:09:42Z	AROASEZ32OEI6JMX5TNWO:user3353765=Badreldin_Wael_Mohamed	{"X-Amz-Date":"20241002T190941Z","bucketName":"data-bucket-039c8e9d2cb233518","X-Amz-Al

Task 4.2: Use CloudWatch Logs to monitor secure logs

-Create a CloudWatch Log Group

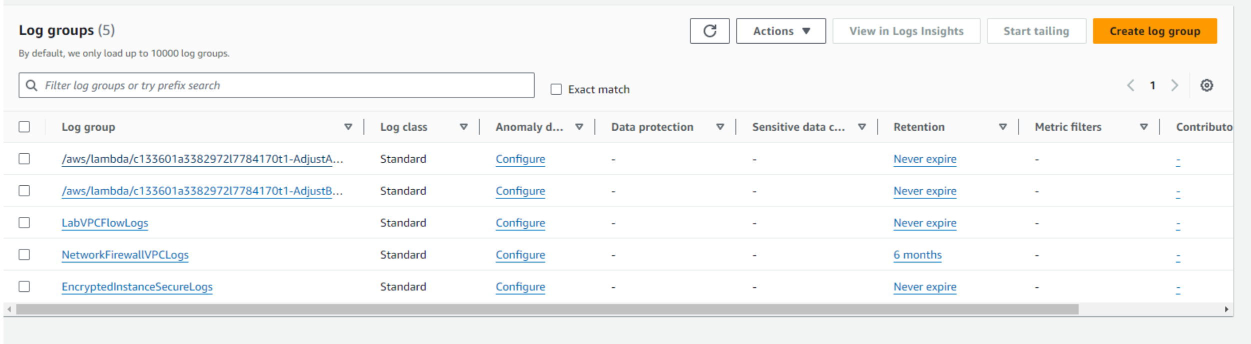
-Connect to EncryptedInstance

-Install the CloudWatch Agent and Collectd

-Download and Configure the CloudWatch Agent Configuration File

-Start the CloudWatch Agent

-Generate Security Logs by Connecting and Disconnecting, one time with correct username and another with ubuntu



Log groups (5)

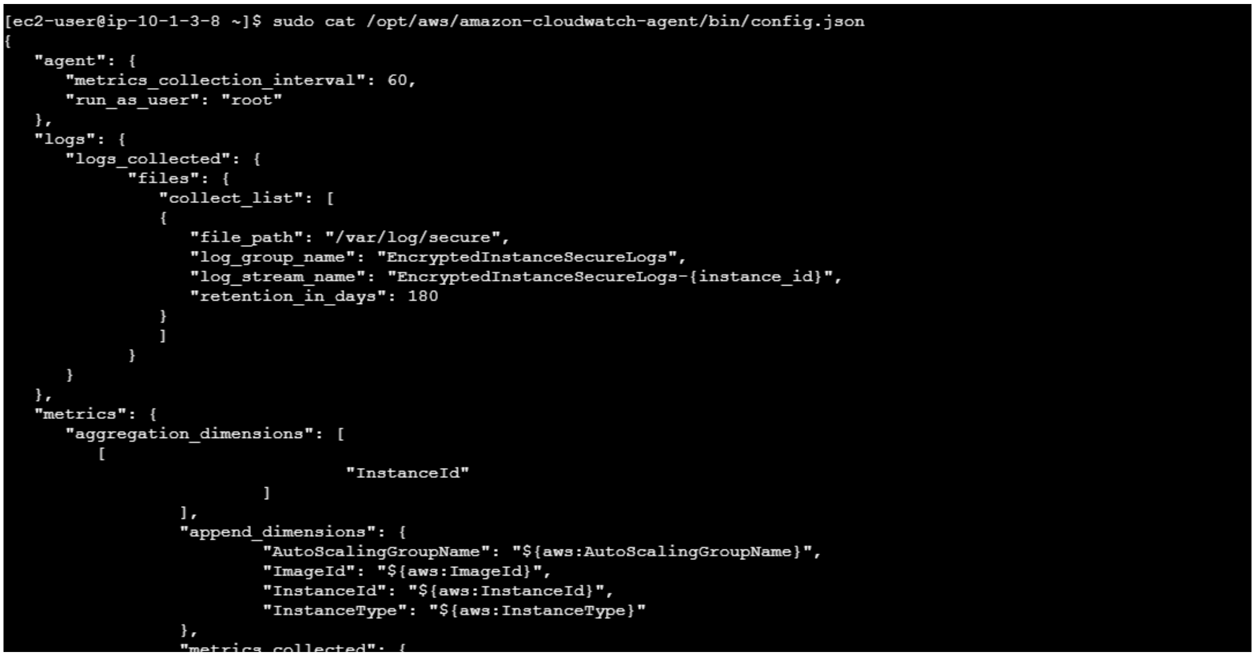
By default, we only load up to 10000 log groups.

Filter log groups or try prefix search

□ Exact match

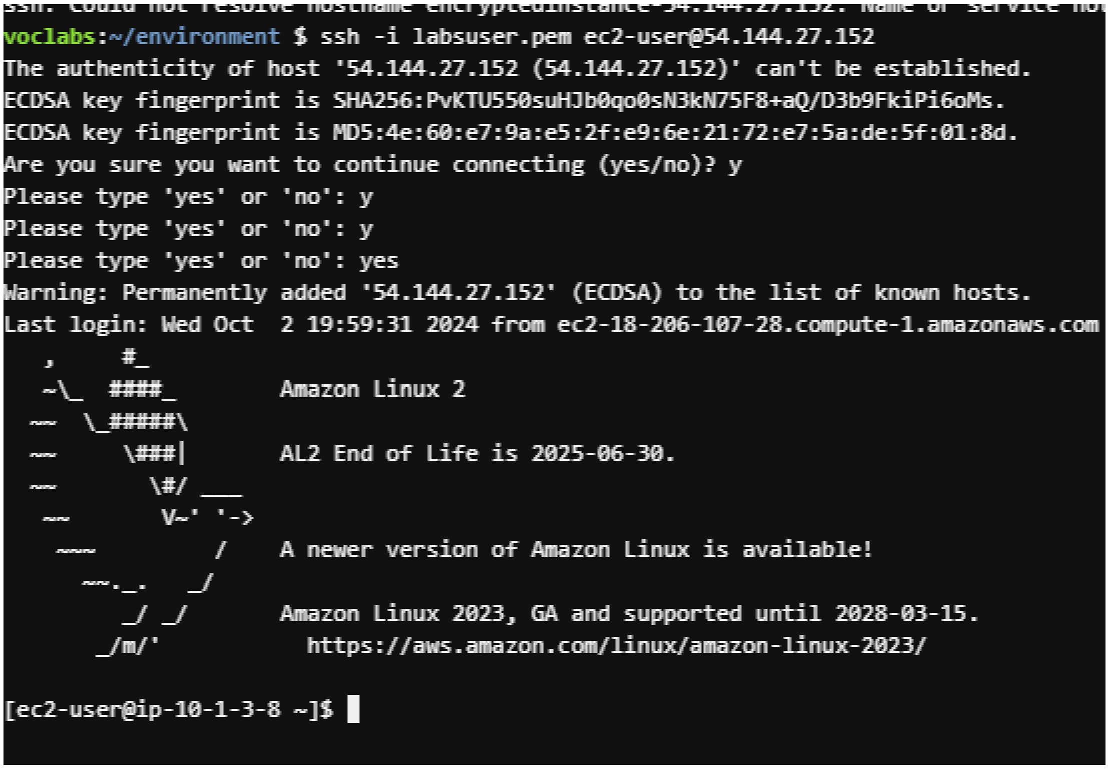
< 1 >

□	Log group	Log class	Anomaly d...	Data protection	Sensitive data c...	Retention	Metric filters	Contributo
□	/aws/lambda/c133601a3382972l7784170t1-AdjustA...	Standard	Configure	-	-	Never expire	-	-
□	/aws/lambda/c133601a3382972l7784170t1-AdjustB...	Standard	Configure	-	-	Never expire	-	-
□	LabVPCFlowLogs	Standard	Configure	-	-	Never expire	-	-
□	NetworkFirewallVPCLogs	Standard	Configure	-	-	6 months	-	-
□	EncryptedInstanceSecureLogs	Standard	Configure	-	-	Never expire	-	-

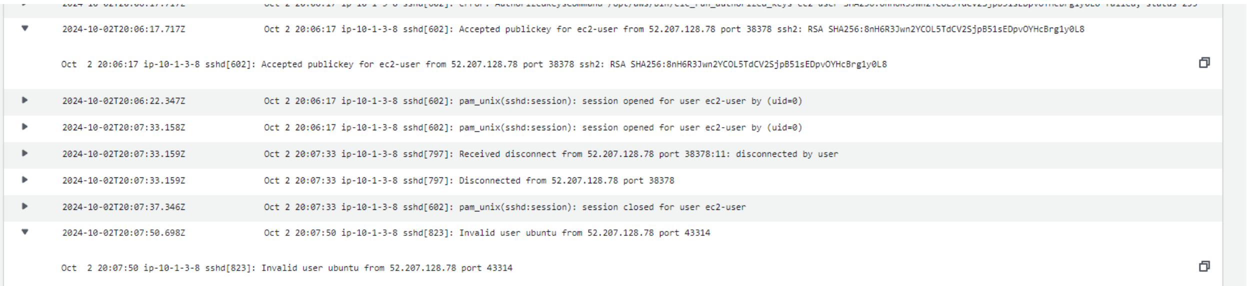


```
[ec2-user@ip-10-1-3-8 ~]$ sudo cat /opt/aws/amazon-cloudwatch-agent/bin/config.json
{
   "agent": {
      "metrics_collection_interval": 60,
      "run_as_user": "root"
   },
   "logs": {
      "logs_collected": {
            "files": {
               "collect_list": [
               {
                  "file_path": "/var/log/secure",
                  "log_group_name": "EncryptedInstanceSecureLogs",
                  "log_stream_name": "EncryptedInstanceSecureLogs-{instance_id}",
                  "retention_in_days": 180
               }
               ]
            }
      }
   },
   "metrics": {
      "aggregation_dimensions": [
         [
                                 "InstanceId"
                     ]
                ],
                "append_dimensions": {
                        "AutoScalingGroupName": "${aws:AutoScalingGroupName}",
                        "ImageId": "${aws:ImageId}",
                        "InstanceId": "${aws:InstanceId}",
                        "InstanceType": "${aws:InstanceType}"
                },
                "metrics_collected": {
```

-Connected ssh to encrypted instance



```
ssh: Could not resolve hostname encryptedinstance-54.144.27.152: Name or service not
voclabs:~/environment $ ssh -i labsuser.pem ec2-user@54.144.27.152
The authenticity of host '54.144.27.152 (54.144.27.152)' can't be established.
ECDSA key fingerprint is SHA256:PvKTU550suHJb0qo0sN3kN75F8+aQ/D3b9FkiPi6oMs.
ECDSA key fingerprint is MD5:4e:60:e7:9a:e5:2f:e9:6e:21:72:e7:5a:de:5f:01:8d.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': y
Please type 'yes' or 'no': y
Please type 'yes' or 'no': yes
Warning: Permanently added '54.144.27.152' (ECDSA) to the list of known hosts.
Last login: Wed Oct  2 19:59:31 2024 from ec2-18-206-107-28.compute-1.amazonaws.com
   ,     #_
   ~\_  ####_        Amazon Linux 2
  ~~  \_#####\
  ~~     \###|       AL2 End of Life is 2025-06-30.
  ~~       \#/ ___
   ~~       V~' '->
    ~~~         /    A newer version of Amazon Linux is available!
      ~~._.   _/
         _/ _/       Amazon Linux 2023, GA and supported until 2028-03-15.
       _/m/'           https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-10-1-3-8 ~]$ 
```



```
▸  2024-10-02T20:06:17.717Z    Oct 2 20:06:17 ip-10-1-3-8 sshd[602]: error: AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys ec2-user SHA256:8nH6R3Jwn2YCOL5TdCV2SjpB51sEDpvOYHcBrg1y0L8 failed, status 255
▾  2024-10-02T20:06:17.717Z    Oct 2 20:06:17 ip-10-1-3-8 sshd[602]: Accepted publickey for ec2-user from 52.207.128.78 port 38378 ssh2: RSA SHA256:8nH6R3Jwn2YCOL5TdCV2SjpB51sEDpvOYHcBrg1y0L8

   Oct  2 20:06:17 ip-10-1-3-8 sshd[602]: Accepted publickey for ec2-user from 52.207.128.78 port 38378 ssh2: RSA SHA256:8nH6R3Jwn2YCOL5TdCV2SjpB51sEDpvOYHcBrg1y0L8

▸  2024-10-02T20:06:22.347Z    Oct 2 20:06:17 ip-10-1-3-8 sshd[602]: pam_unix(sshd:session): session opened for user ec2-user by (uid=0)
▸  2024-10-02T20:07:33.158Z    Oct 2 20:06:17 ip-10-1-3-8 sshd[602]: pam_unix(sshd:session): session opened for user ec2-user by (uid=0)
▸  2024-10-02T20:07:33.159Z    Oct 2 20:07:33 ip-10-1-3-8 sshd[797]: Received disconnect from 52.207.128.78 port 38378:11: disconnected by user
▸  2024-10-02T20:07:33.159Z    Oct 2 20:07:33 ip-10-1-3-8 sshd[797]: Disconnected from 52.207.128.78 port 38378
▸  2024-10-02T20:07:37.346Z    Oct 2 20:07:33 ip-10-1-3-8 sshd[602]: pam_unix(sshd:session): session closed for user ec2-user
▾  2024-10-02T20:07:50.698Z    Oct 2 20:07:50 ip-10-1-3-8 sshd[823]: Invalid user ubuntu from 52.207.128.78 port 43314

   Oct  2 20:07:50 ip-10-1-3-8 sshd[823]: Invalid user ubuntu from 52.207.128.78 port 43314
```

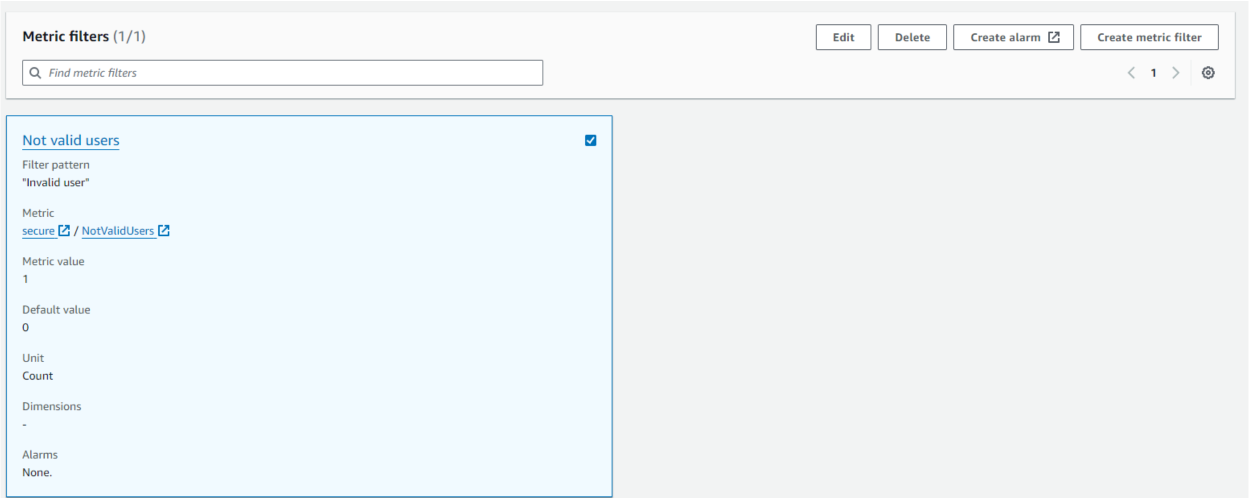
Task 4.3: Create a CloudWatch alarm to send notifications for security incidents

-Create a Metric Filter

-Create a CloudWatch Alarm

-Use SNS subscription

-Test the Alarm using invalid username at least 5 times



Metric filters (1/1)

☑ Not valid users

Filter pattern
"Invalid user"

Metric
secure / NotValidUsers

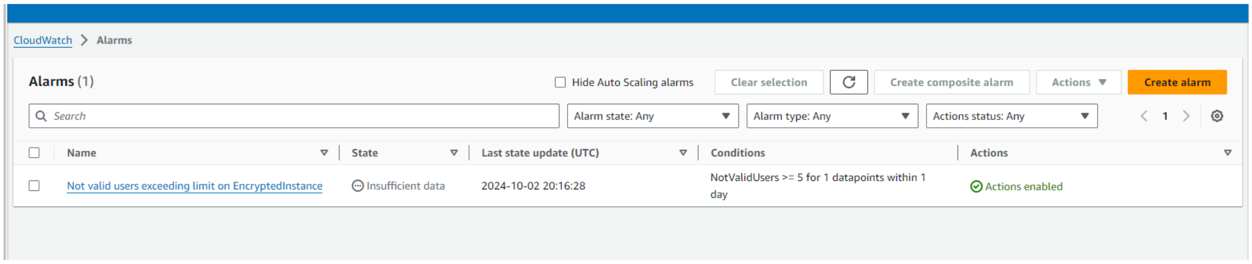
Metric value
1

Default value
0

Unit
Count

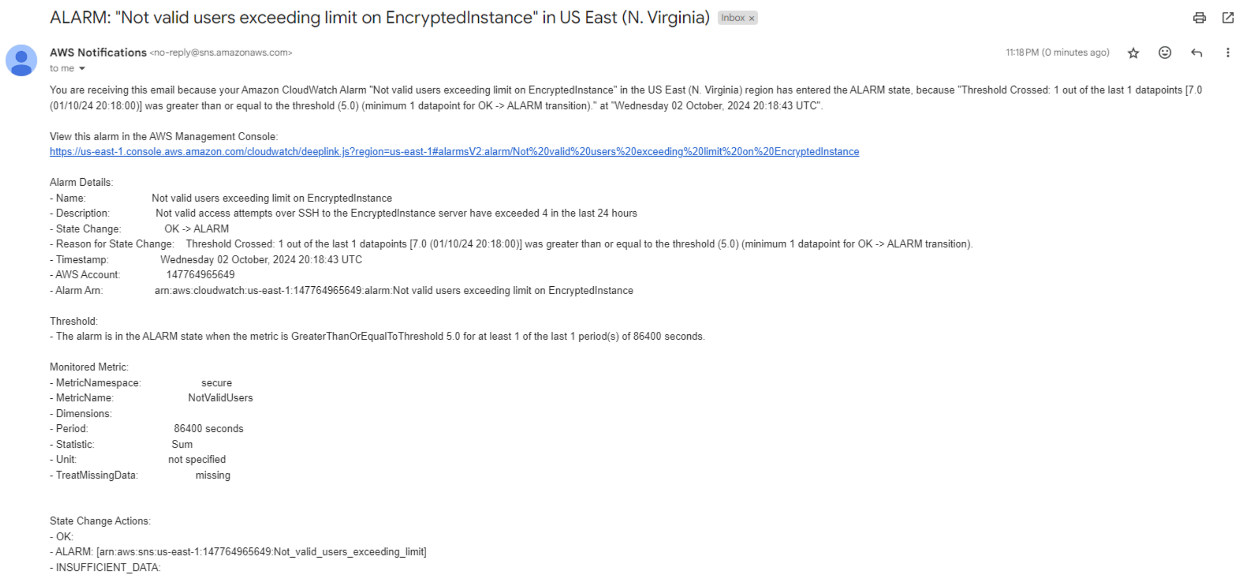
Dimensions
-

Alarms
None.



Alarms (1)

□	Name	State	Last state update (UTC)	Conditions	Actions
□	Not valid users exceeding limit on EncryptedInstance	Insufficient data	2024-10-02 20:16:28	NotValidUsers >= 5 for 1 datapoints within 1 day	✓ Actions enabled



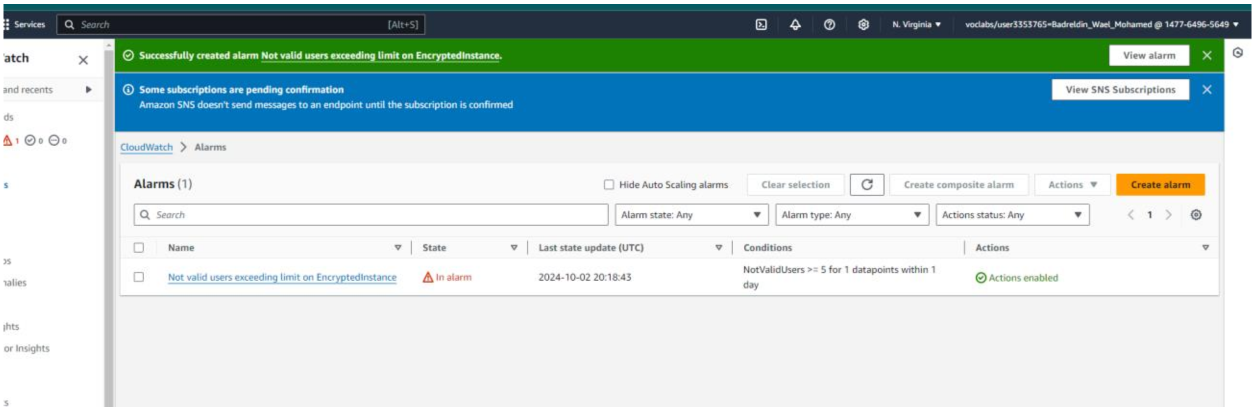
ALARM: "Not valid users exceeding limit on EncryptedInstance" in US East (N. Virginia)

AWS Notifications <no-reply@sns.amazonaws.com>
to me
11:18 PM (0 minutes ago)

You are receiving this email because your Amazon CloudWatch Alarm "Not valid users exceeding limit on EncryptedInstance" in the US East (N. Virginia) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [7.0 (01/10/24 20:18:00)] was greater than or equal to the threshold (5.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Wednesday 02 October, 2024 20:18:43 UTC".

View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-1#alarmsV2:alarm/Not%20valid%20users%20exceeding%20limit%20on%20EncryptedInstance

```
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 [7.0 (01/10/24 20:18:00)] was greater than or equal to the threshold (5.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp:              Wednesday 02 October, 2024 20:18:43 UTC
- AWS Account:            147764965649
- Alarm Arn:              arn:aws:cloudwatch:us-east-1:147764965649: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 86400 seconds.

Monitored Metric:
- MetricNamespace:                  secure
- MetricName:                       NotValidUsers
- Dimensions:
- Period:                           86400 seconds
- Statistic:                        Sum
- Unit:                             not specified
- TreatMissingData:                 missing


State Change Actions:
- OK:
- ALARM: [arn:aws:sns:us-east-1:147764965649:Not_valid_users_exceeding_limit]
- INSUFFICIENT_DATA:
```



Successfully created alarm Not valid users exceeding limit on EncryptedInstance.

Some subscriptions are pending confirmation
Amazon SNS doesn't send messages to an endpoint until the subscription is confirmed

Alarms (1)

Alarm state: Any | Alarm type: Any | Actions status: Any

Name	State	Last state update (UTC)	Conditions	Actions
Not valid users exceeding limit on EncryptedInstance	In alarm	2024-10-02 20:18:43	NotValidUsers >= 5 for 1 datapoints within 1 day	Actions enabled

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

-Create a New S3 compliance-bucket

-Enable Object Ownership on the Logging Bucket

-Set Up AWS Config

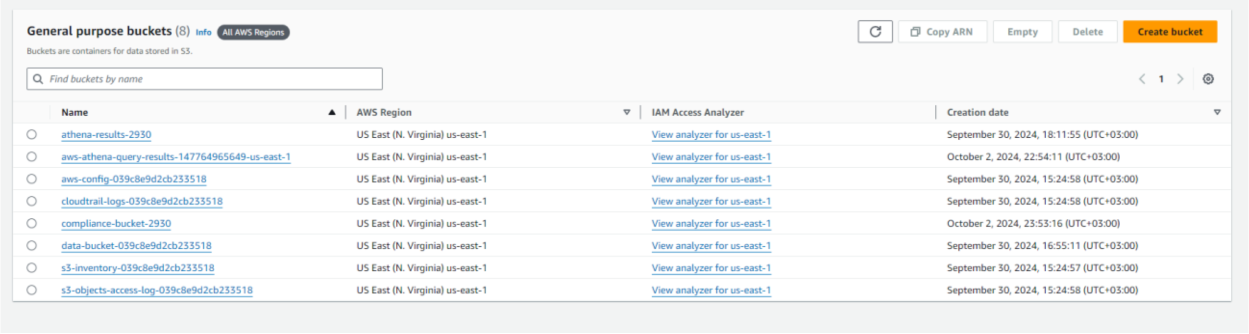
-Add AWS Managed Rule

-Verify Compliance Status

-Configure Manual Remediation

-Invoke the Remediation Action

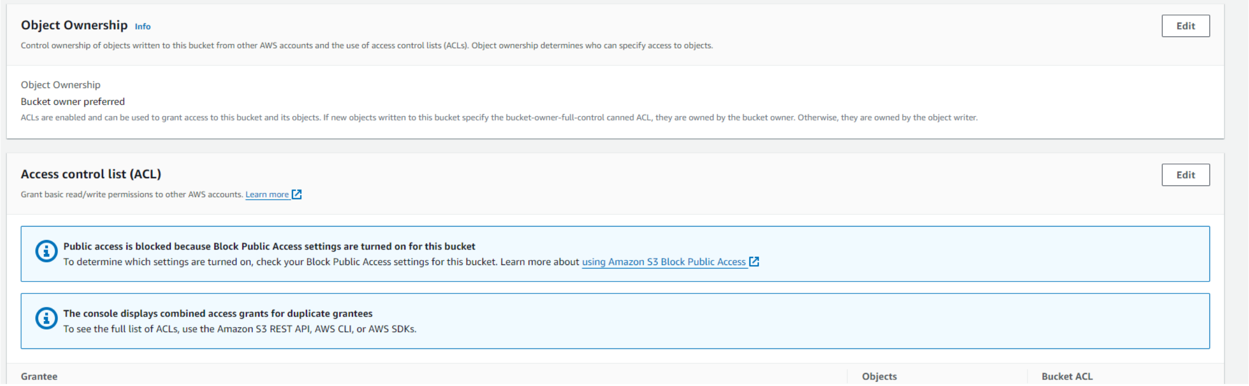
-Troubleshhot and use gurante uri to solve the problem



General purpose buckets (8)

Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
athena-results-2930	US East (N. Virginia) us-east-1	View analyzer for us-east-1	September 30, 2024, 18:11:55 (UTC+03:00)
aws-athena-query-results-147764965649-us-east-1	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 2, 2024, 22:54:11 (UTC+03:00)
aws-config-039c8e9d2cb233518	US East (N. Virginia) us-east-1	View analyzer for us-east-1	September 30, 2024, 15:24:58 (UTC+03:00)
cloudtrail-logs-039c8e9d2cb233518	US East (N. Virginia) us-east-1	View analyzer for us-east-1	September 30, 2024, 15:24:58 (UTC+03:00)
compliance-bucket-2930	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 2, 2024, 23:53:16 (UTC+03:00)
data-bucket-039c8e9d2cb233518	US East (N. Virginia) us-east-1	View analyzer for us-east-1	September 30, 2024, 16:55:11 (UTC+03:00)
s3-inventory-039c8e9d2cb233518	US East (N. Virginia) us-east-1	View analyzer for us-east-1	September 30, 2024, 15:24:57 (UTC+03:00)
s3-objects-access-log-039c8e9d2cb233518	US East (N. Virginia) us-east-1	View analyzer for us-east-1	September 30, 2024, 15:24:58 (UTC+03:00)



Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

Object Ownership
Bucket owner preferred
ACLs are enabled and can be used to grant access to this bucket and its objects. If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

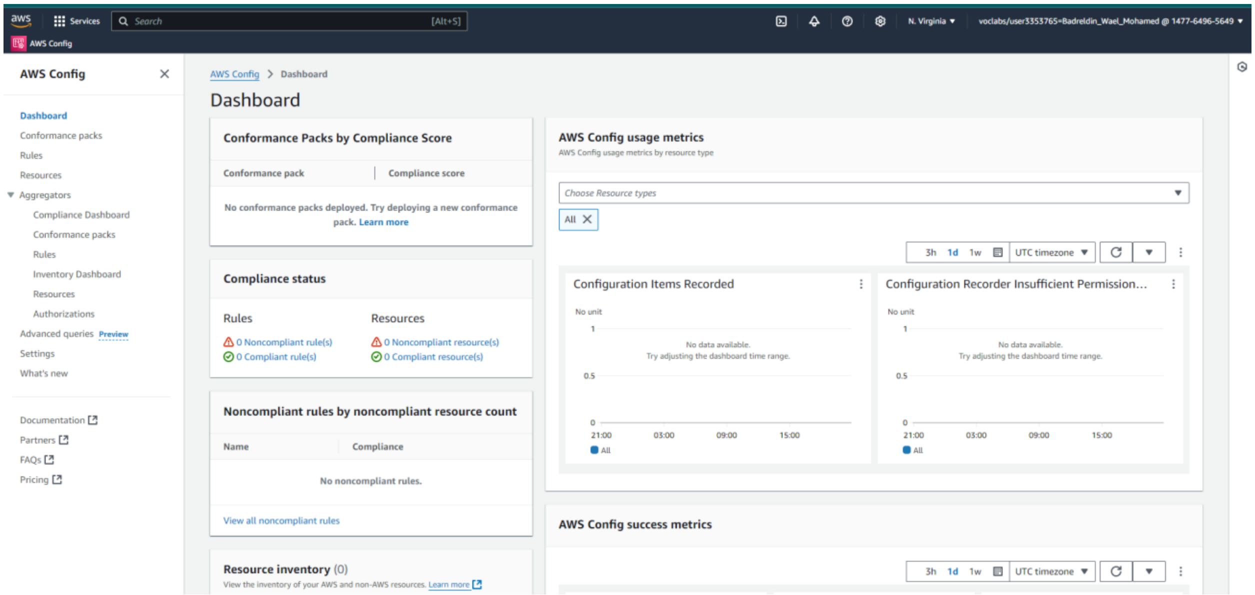
Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. Learn more

Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about using Amazon S3 Block Public Access

The console displays combined access grants for duplicate grantees
To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.

Grantee	Objects	Bucket ACL



Dashboard

Conformance Packs by Compliance Score

Conformance pack	Compliance score

No conformance packs deployed. Try deploying a new conformance pack. Learn more

Compliance status

Rules	Resources
0 Noncompliant rule(s)	0 Noncompliant resource(s)
0 Compliant rule(s)	0 Compliant resource(s)

Noncompliant rules by noncompliant resource count

Name	Compliance

No noncompliant rules.

View all noncompliant rules

Resource inventory (0)
View the inventory of your AWS and non-AWS resources. Learn more

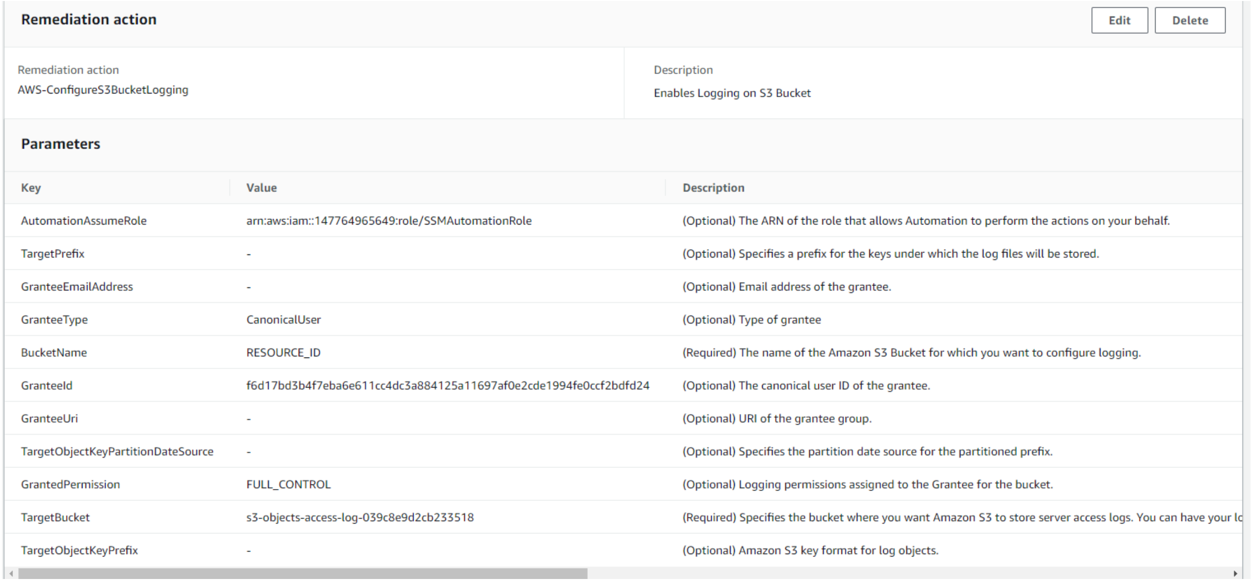
AWS Config usage metrics
AWS Config usage metrics by resource type

Choose Resource types
All

Configuration Items Recorded
No unit
No data available.
Try adjusting the dashboard time range.

Configuration Recorder Insufficient Permission...
No unit
No data available.
Try adjusting the dashboard time range.

AWS Config success metrics



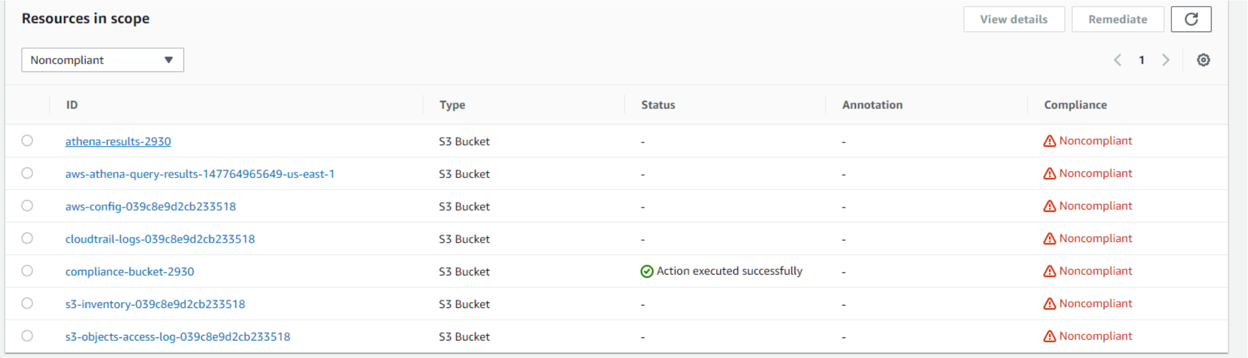
Remediation action

Remediation action
AWS-ConfigureS3BucketLogging

Description
Enables Logging on S3 Bucket

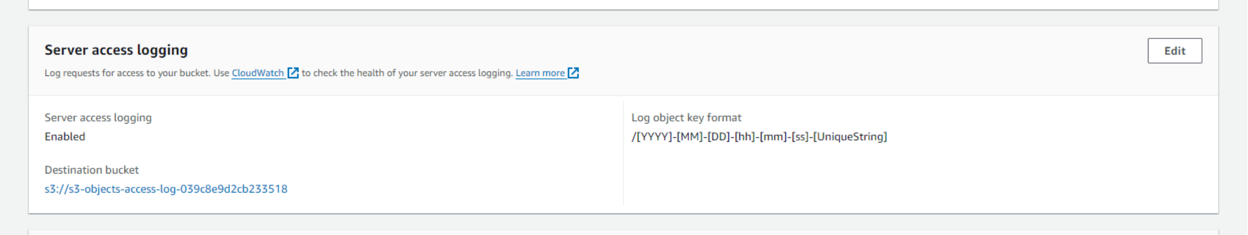
Parameters

Key	Value	Description
AutomationAssumeRole	arn:aws:iam::147764965649: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	CanonicalUser	(Optional) Type of grantee
BucketName	RESOURCE_ID	(Required) The name of the Amazon S3 Bucket for which you want to configure logging.
GranteeId	f6d17bd3b4f7eba6e611cc4dc3a884125a11697af0e2cde1994fe0ccf2bdfd24	(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-039c8e9d2cb233518	(Required) Specifies the bucket where you want Amazon S3 to store server access logs. You can have your lo
TargetObjectKeyPrefix	-	(Optional) Amazon S3 key format for log objects.



Resources in scope

	ID	Type	Status	Annotation	Compliance
○	athena-results-2930	S3 Bucket	-	-	⚠ Noncompliant
○	aws-athena-query-results-147764965649-us-east-1	S3 Bucket	-	-	⚠ Noncompliant
○	aws-config-039c8e9d2cb233518	S3 Bucket	-	-	⚠ Noncompliant
○	cloudtrail-logs-039c8e9d2cb233518	S3 Bucket	-	-	⚠ Noncompliant
○	compliance-bucket-2930	S3 Bucket	✓ Action executed successfully	-	⚠ Noncompliant
○	s3-inventory-039c8e9d2cb233518	S3 Bucket	-	-	⚠ Noncompliant
○	s3-objects-access-log-039c8e9d2cb233518	S3 Bucket	-	-	⚠ Noncompliant



Server access logging

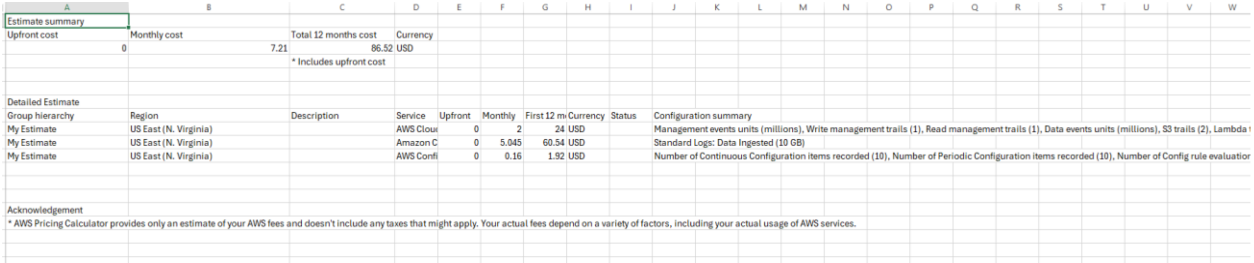
Log requests for access to your bucket. Use CloudWatch to check the health of your server access logging. Learn more

Server access logging
Enabled

Destination bucket
s3://s3-objects-access-log-039c8e9d2cb233518

Log object key format
/[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]

Cost Estmation



Estimate summary

Upfront cost	Monthly cost	Total 12 months cost	Currency
0	7.21	86.52	USD
		* Includes upfront cost	

Detailed Estimate

Group hierarchy	Region	Description	Service	Upfront	Monthly	First 12 m	Currency	Status	Configuration summary
My Estimate	US East (N. Virginia)		AWS Clou	0	2	24	USD		Management events units (millions), Write management trails (1), Read management trails (1), Data events units (millions), S3 trails (2), Lambda t
My Estimate	US East (N. Virginia)		Amazon C	0	5.045	60.54	USD		Standard Logs: Data Ingested (10 GB)
My Estimate	US East (N. Virginia)		AWS Confi	0	0.16	1.92	USD		Number of Continuous Configuration items recorded (10), Number of Periodic Configuration items recorded (10), Number of Config rule evaluatior

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.