AWS Academy lab: Securing and Monitoring Resources with AWS

This project is part of the `Cloud Infrastructure Security Course` in the `Cybersecurity Specialization` at CESAR School.

The tasks are from `AWS Academy` lab: `Securing and Monitoring Resources with AWS`. It focus on securing AWS resources such as S3, VPCs, and implementing encryption with AWS KMS, along with monitoring and logging using AWS CloudTrail, CloudWatch, and AWS Config.

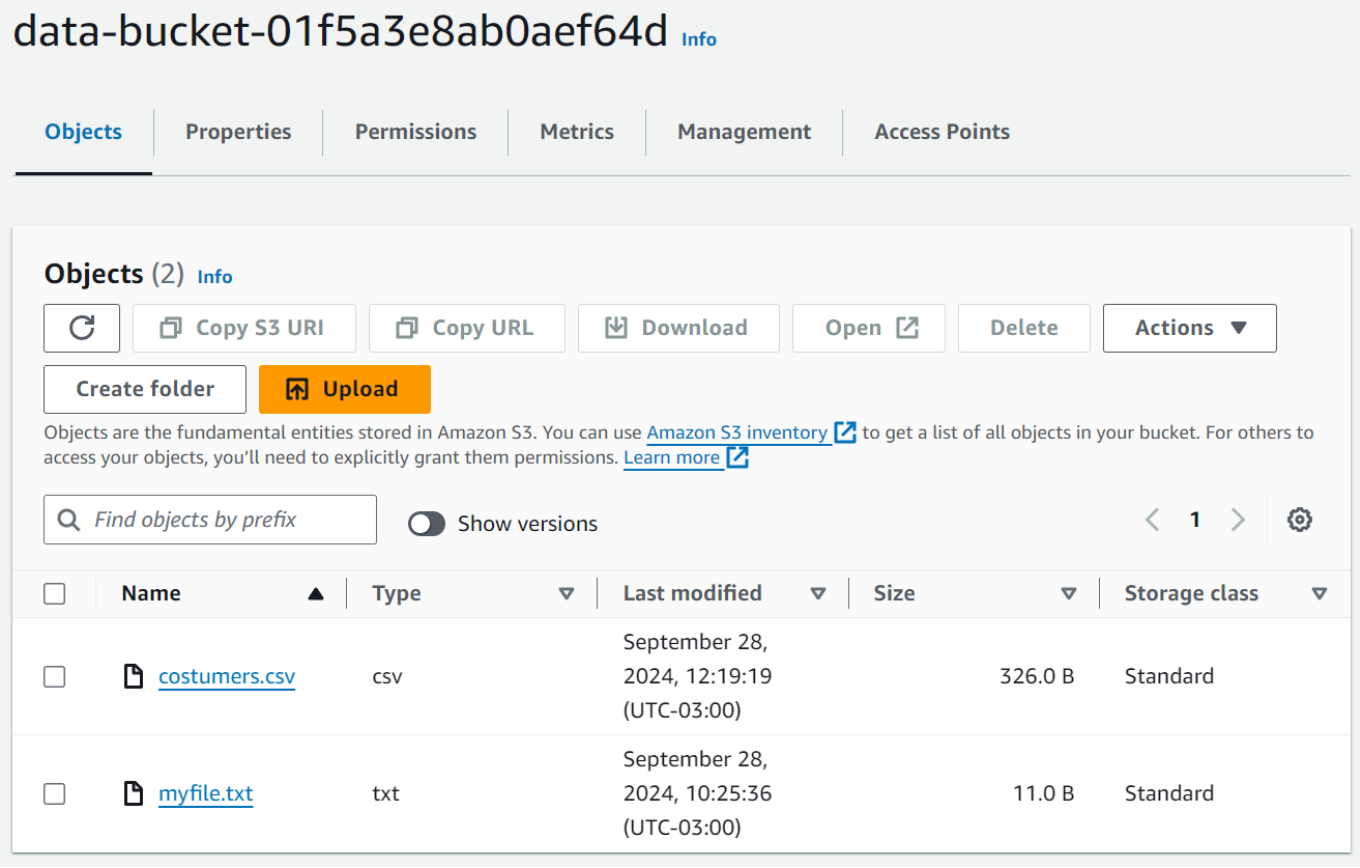
Student: `Pedro Coelho`
Instructor: `Ioram Sette`

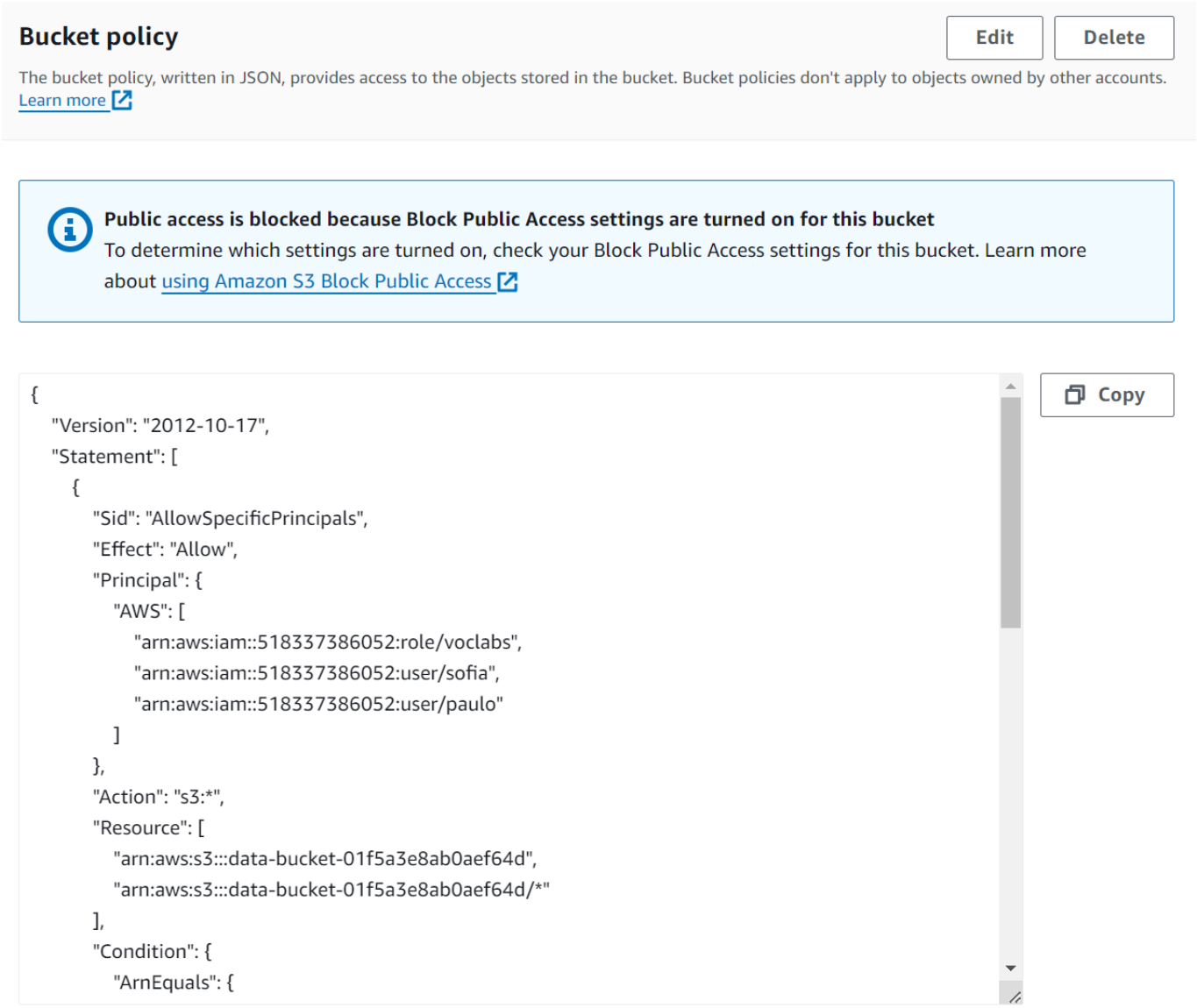
Table of Contents

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

Phase 1: Securing Data in Amazon S3

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





Bucket policy

Edit Delete

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other 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

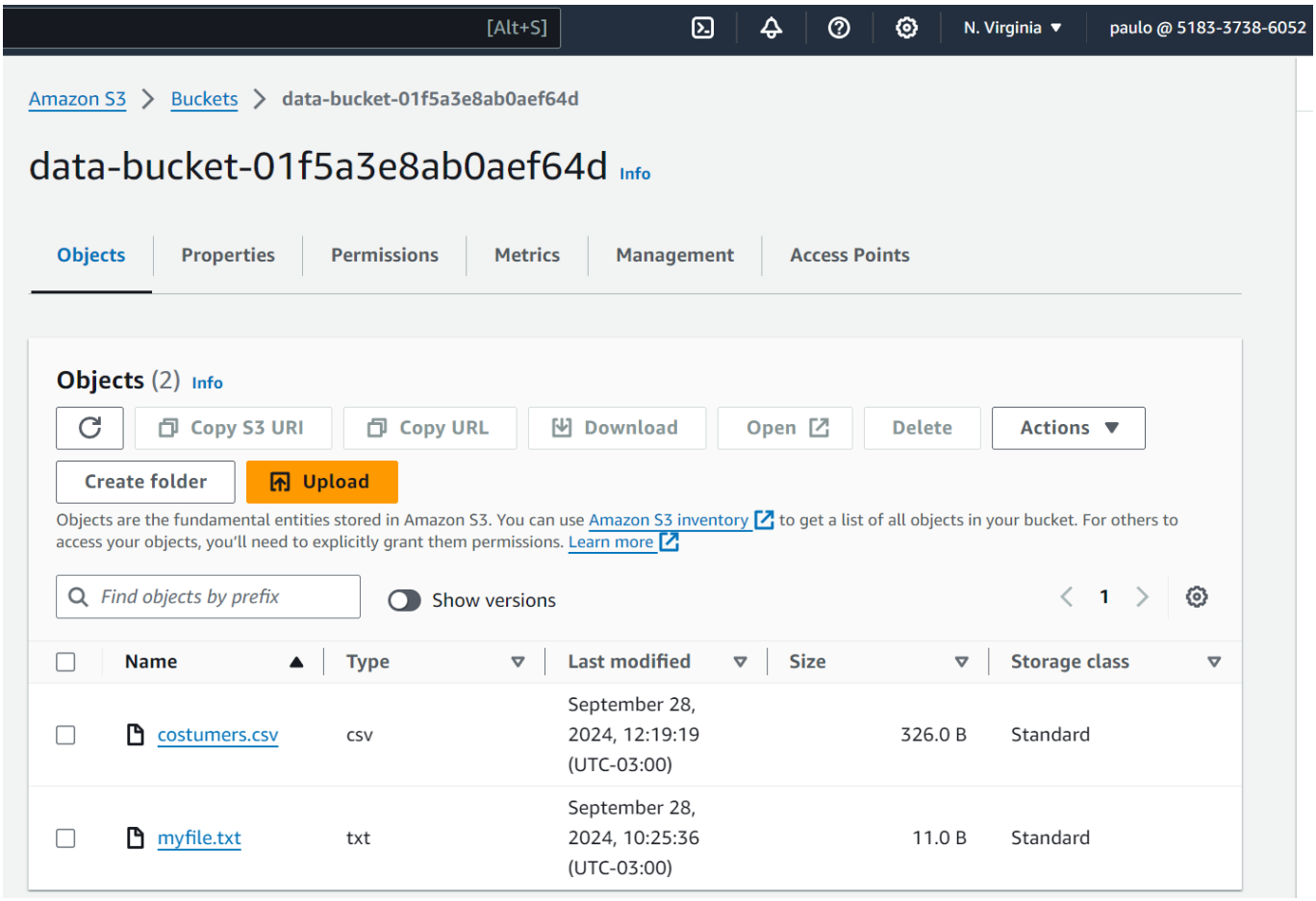
Copy

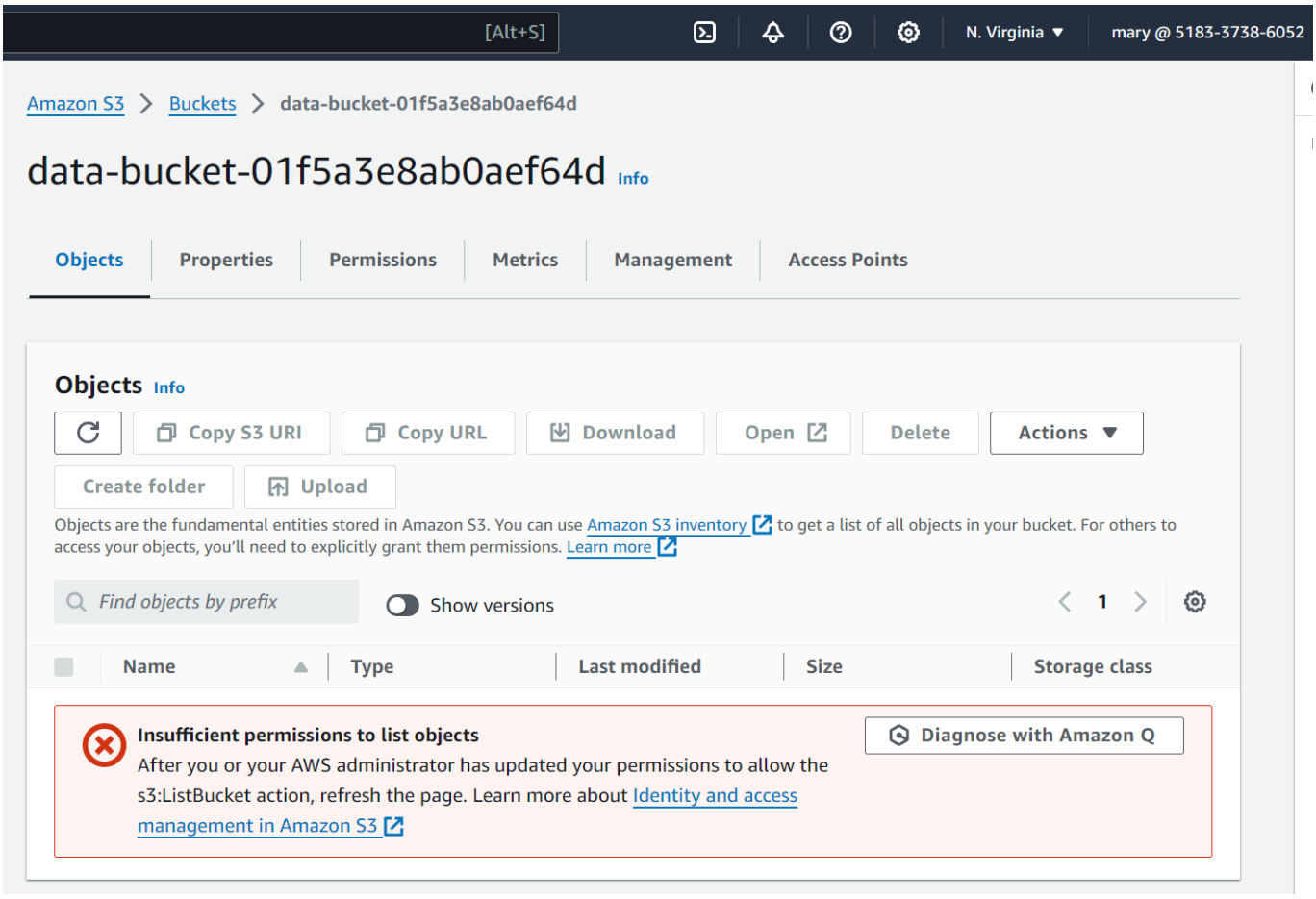

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificPrincipals",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::518337386052:role/voclabs",
          "arn:aws:iam::518337386052:user/sofia",
          "arn:aws:iam::518337386052:user/paulo"
        ]
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::data-bucket-01f5a3e8ab0aef64d",
        "arn:aws:s3:::data-bucket-01f5a3e8ab0aef64d/*"
      ],
      "Condition": {
        "ArnEquals": {
```



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSpecificPrincipals",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::518337386052:role/voclabs",
                    "arn:aws:iam::518337386052:user/sofia",
                    "arn:aws:iam::518337386052:user/paulo"
                ]
            },
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::data-bucket-01f5a3e8ab0aef64d",
                "arn:aws:s3:::data-bucket-01f5a3e8ab0aef64d/*"
            ],
            "Condition": {
                "ArnEquals": {
                    "aws:PrincipalArn": [
```

```
                        "arn:aws:iam::518337386052:user/paulo",
                        "arn:aws:iam::518337386052:user/sofia",
                        "arn:aws:iam::518337386052:role/voclabs"
                    ]
                }
            }
        },
        {
            "Sid": "DenyOtherPrincipals",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::data-bucket-01f5a3e8ab0aef64d",
                "arn:aws:s3:::data-bucket-01f5a3e8ab0aef64d/*"
            ],
            "Condition": {
                "ArnNotEquals": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::518337386052:user/paulo",
                        "arn:aws:iam::518337386052:user/sofia",
                        "arn:aws:iam::518337386052:role/voclabs"
                    ]
                }
            }
        }
    ]
}
```





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

Bucket Versioning

Edit

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning

Enabled

Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more

Disabled

Server access logging

Edit

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

Server access logging

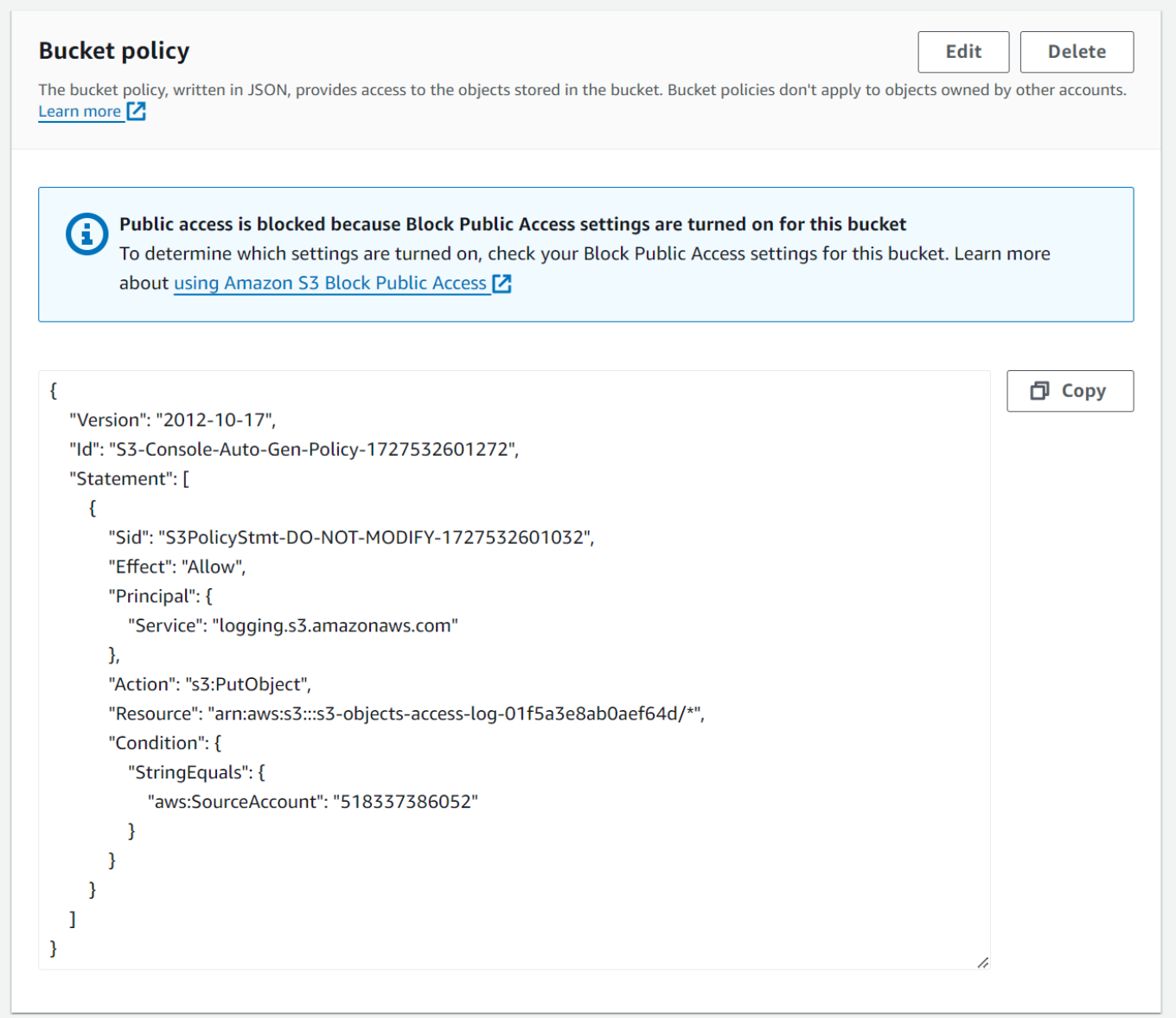
Enabled

Destination bucket

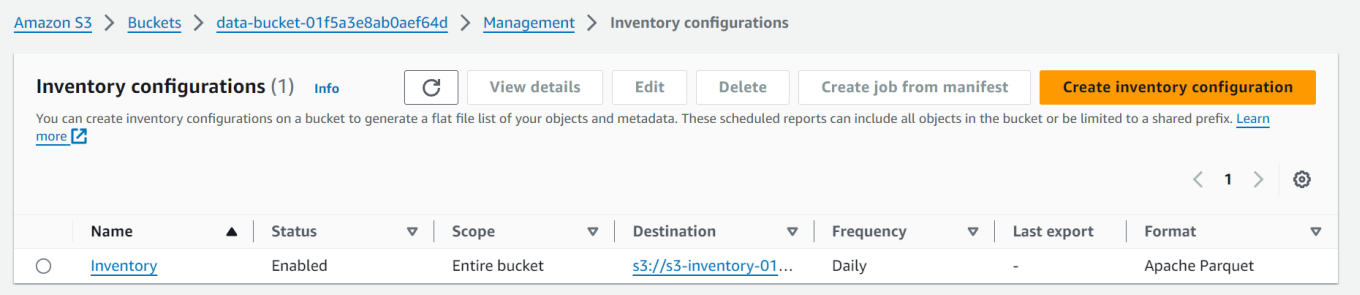
s3://s3-objects-access-log-01f5a3e8ab0aef64d

Log object key format

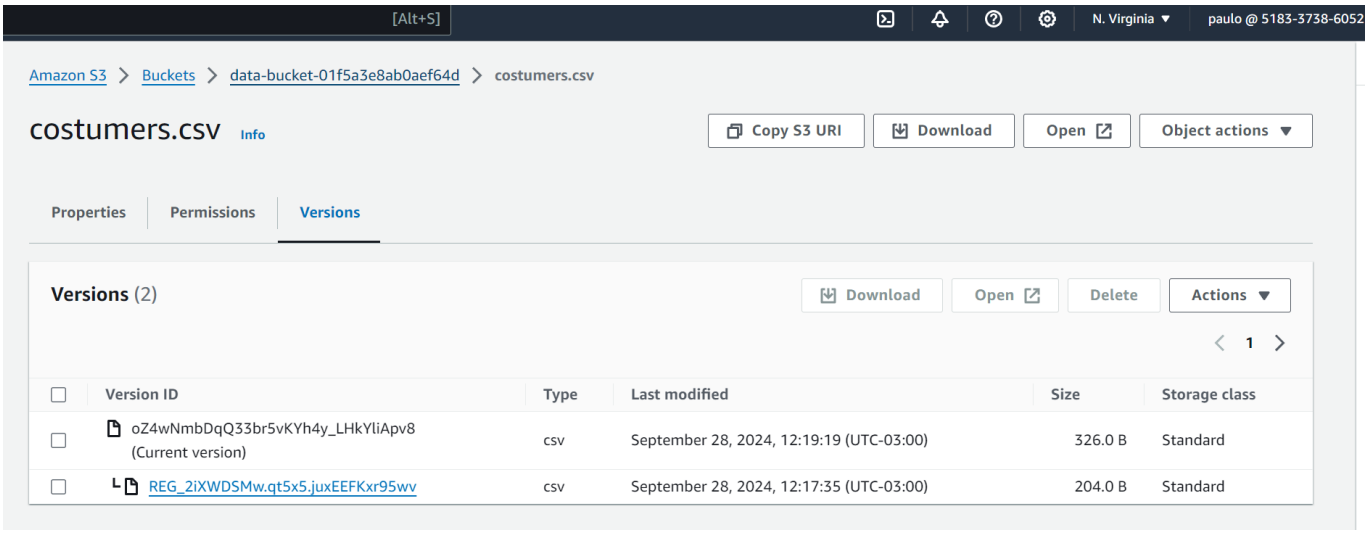
data-bucket[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]

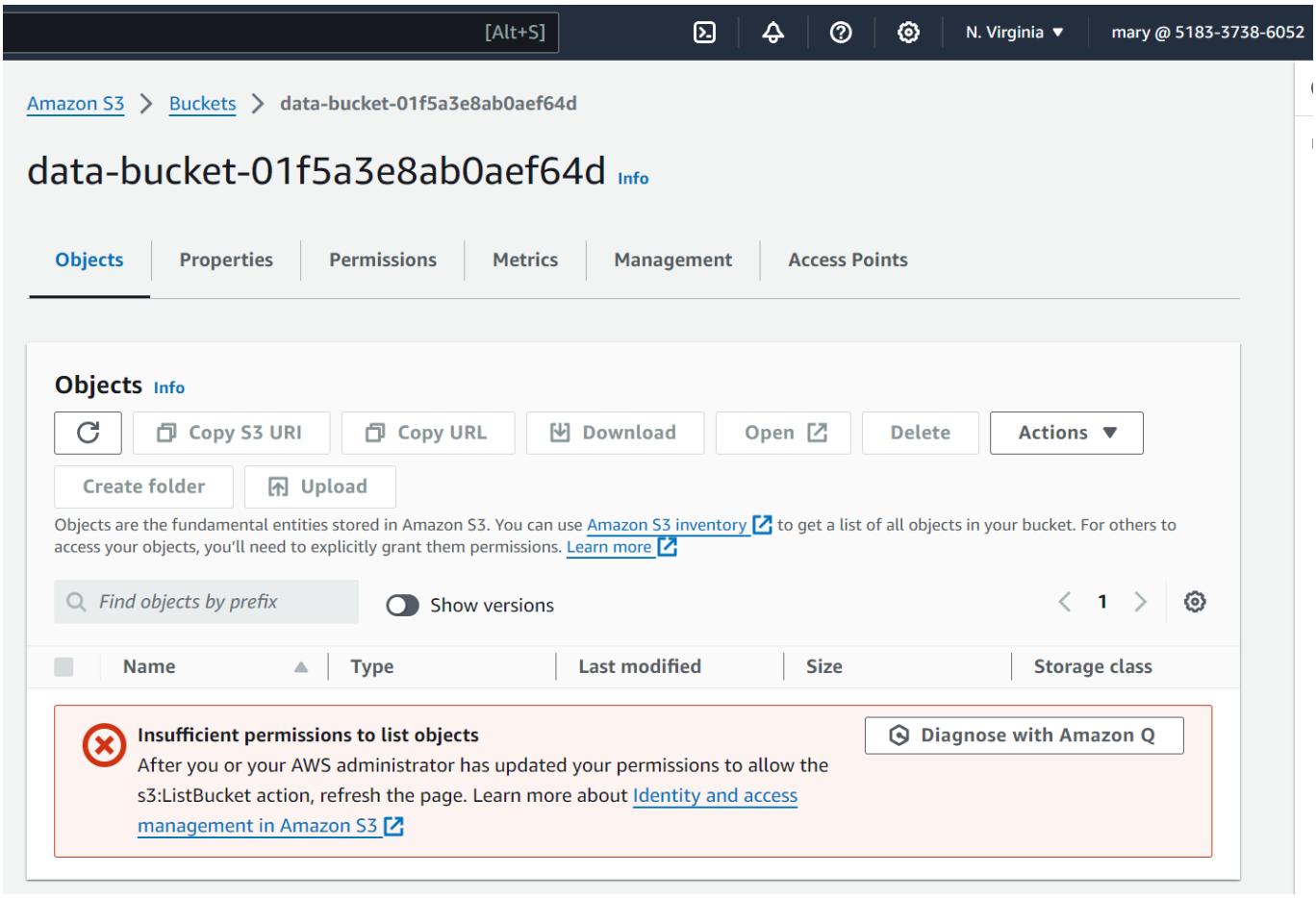


Task 1.3: Implement the S3 Inventory feature on a bucket

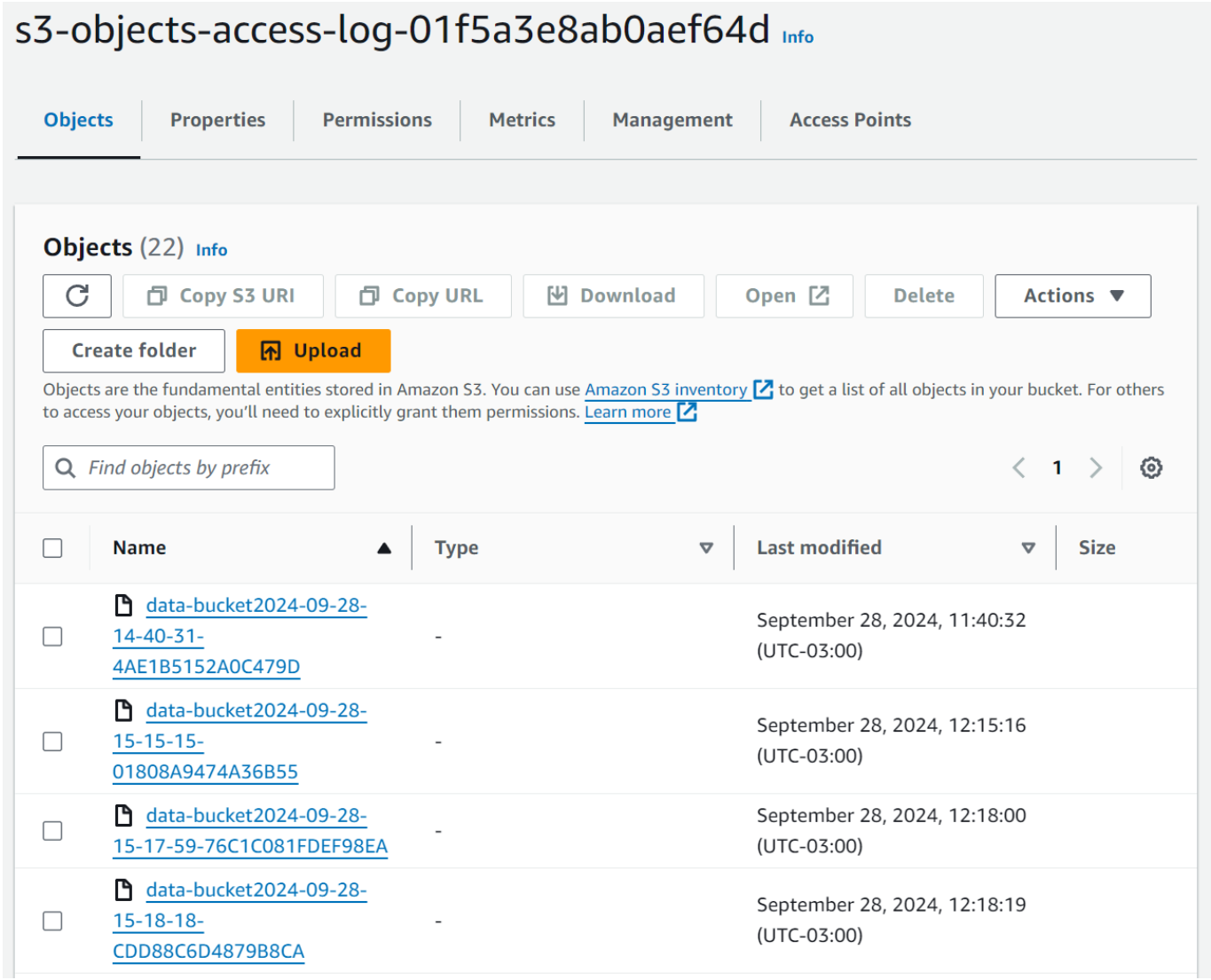


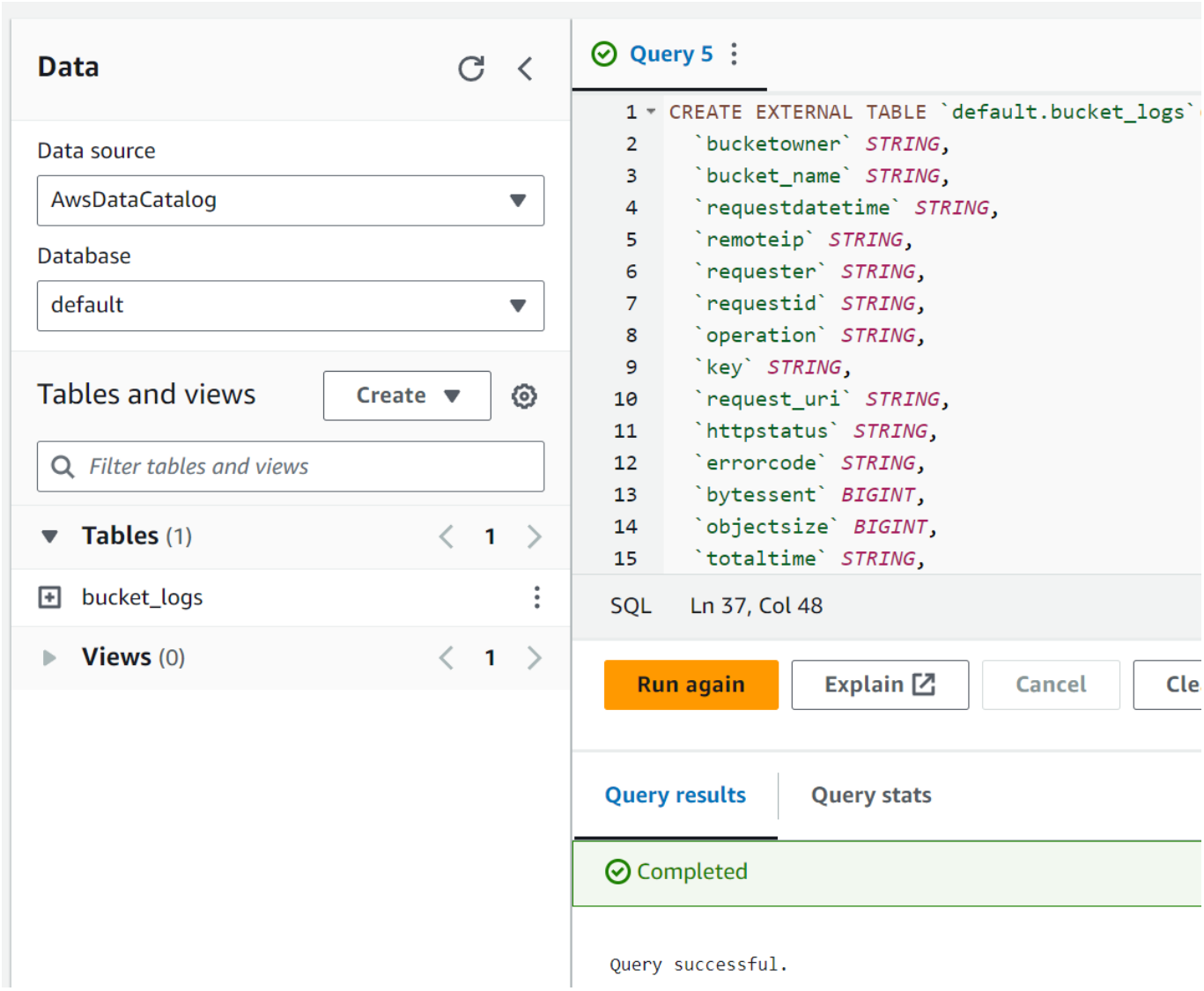
Task 1.4: Confirm that versioning works as intended

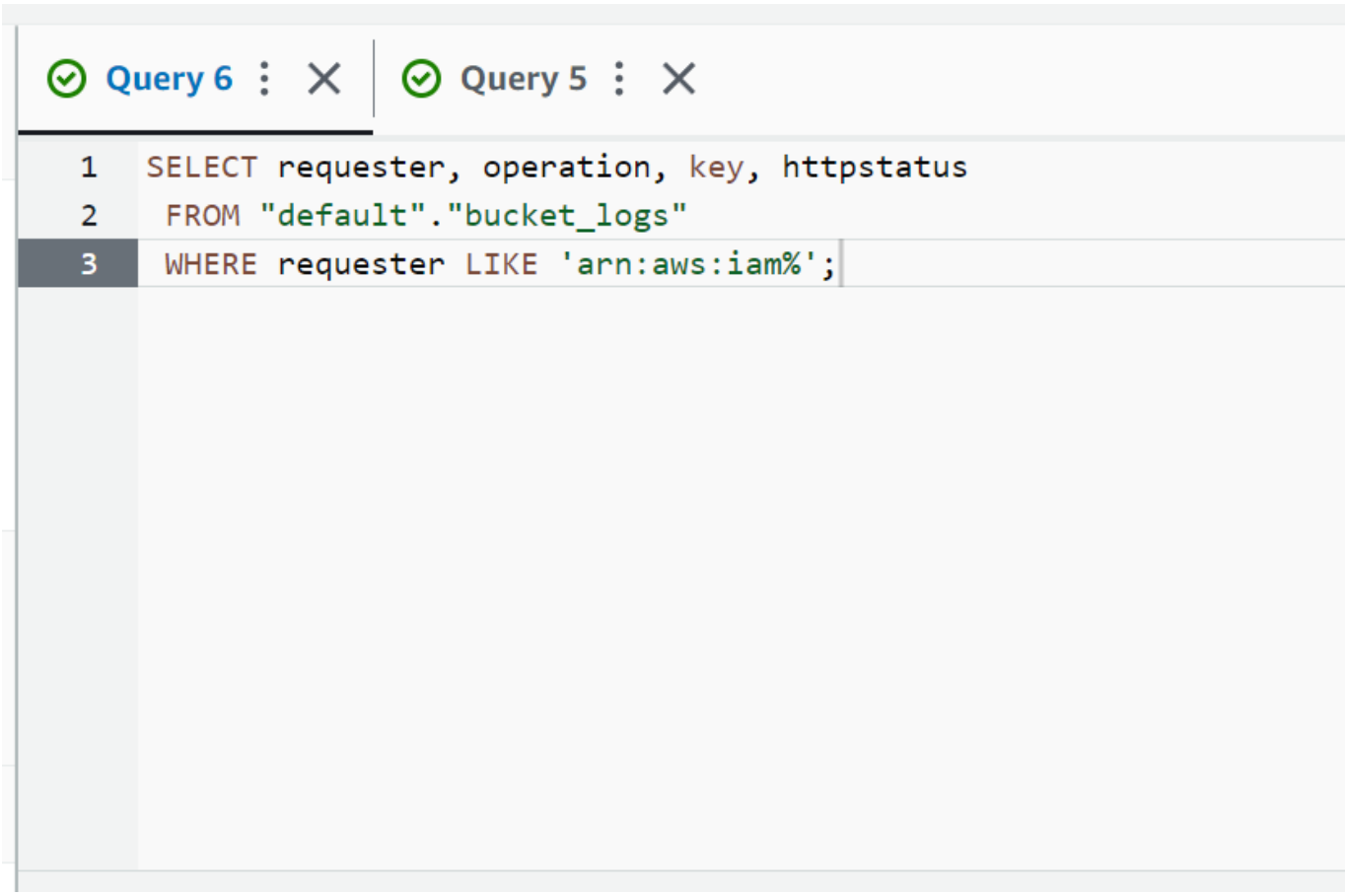


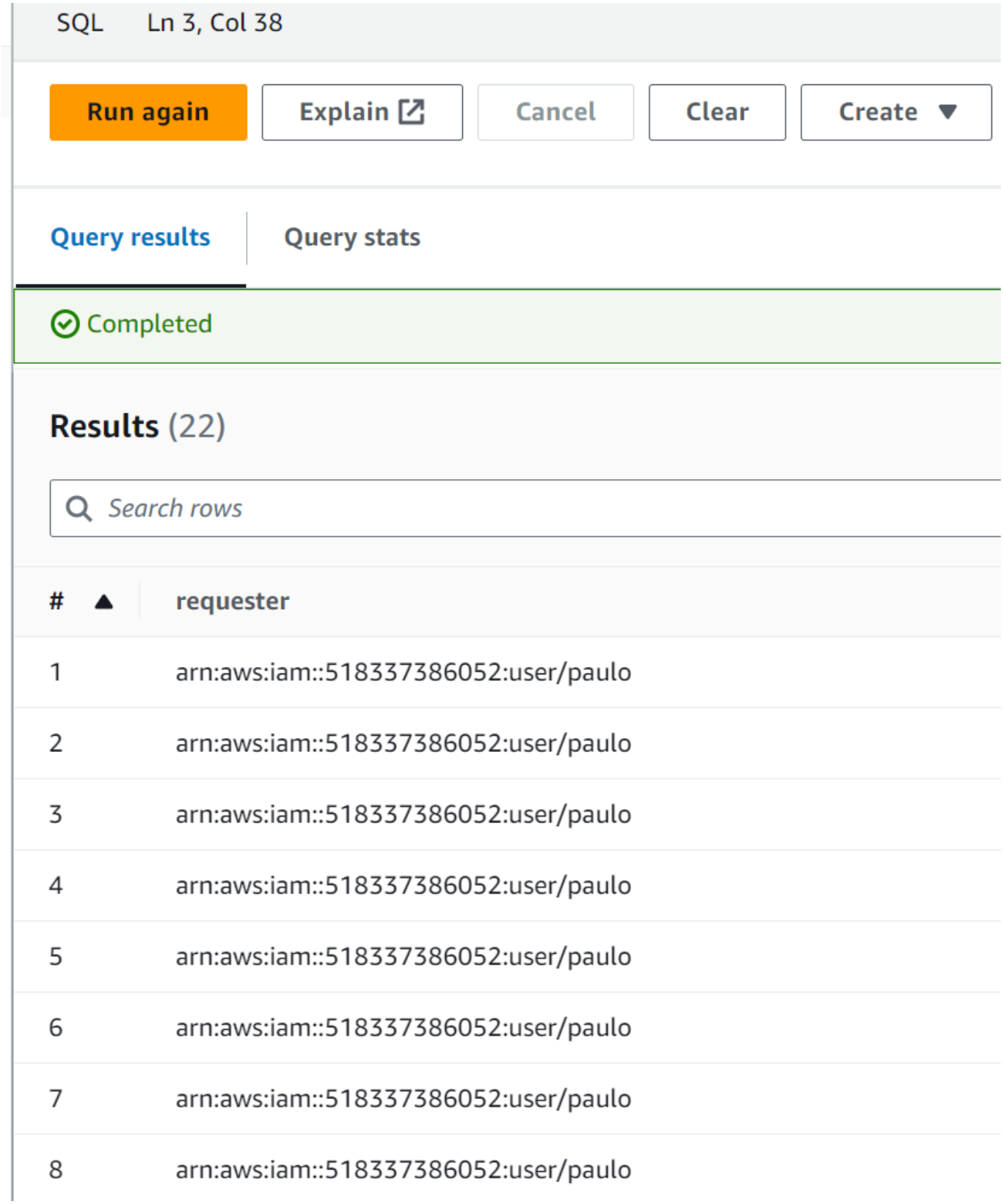


Task 1.5: Confirm object-level logging and query the access logs by using Athena


s3-objects-access-log-01f5a3e8ab0aef64d Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (22) Info
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
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
1
Name
Type
Last modified
Size
data-bucket2024-09-28-14-40-31-4AE1B5152A0C479D
-
September 28, 2024, 11:40:32 (UTC-03:00)
data-bucket2024-09-28-15-15-15-01808A9474A36B55
-
September 28, 2024, 12:15:16 (UTC-03:00)
data-bucket2024-09-28-15-17-59-76C1C081FDEF98EA
-
September 28, 2024, 12:18:00 (UTC-03:00)
data-bucket2024-09-28-15-18-18-CDD88C6D4879B8CA
-
September 28, 2024, 12:18:19 (UTC-03:00)

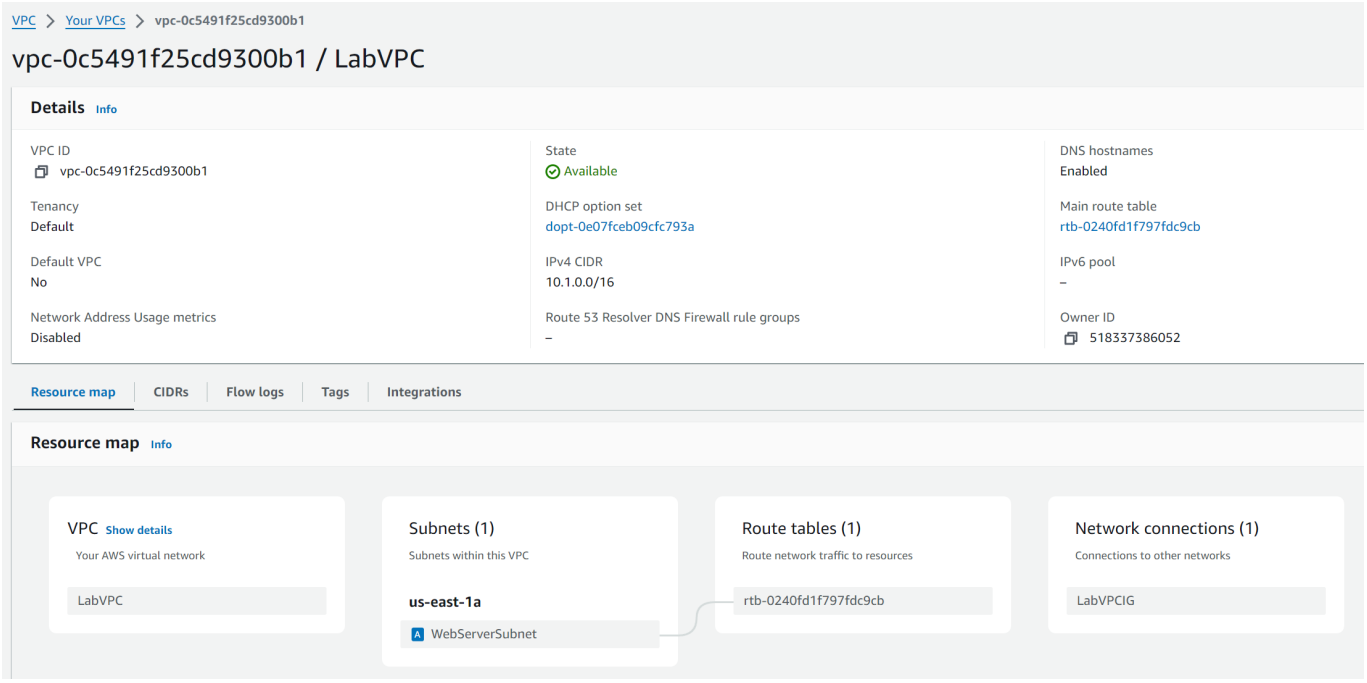

Data
Data source
AwsDataCatalog
Database
default
Tables and views
Create
Filter tables and views
Tables (1)
1
bucket_logs
Views (0)
1
Query 5
1 CREATE EXTERNAL TABLE `default.bucket_logs`
2 `bucketowner` STRING,
3 `bucket_name` STRING,
4 `requestdatetime` STRING,
5 `remoteip` STRING,
6 `requester` STRING,
7 `requestid` STRING,
8 `operation` STRING,
9 `key` STRING,
10 `request_uri` STRING,
11 `httpstatus` STRING,
12 `errorcode` STRING,
13 `bytessent` BIGINT,
14 `objectsize` BIGINT,
15 `totaltime` STRING,
SQL Ln 37, Col 48
Run again
Explain
Cancel
Cle
Query results
Query stats
Completed
Query successful.

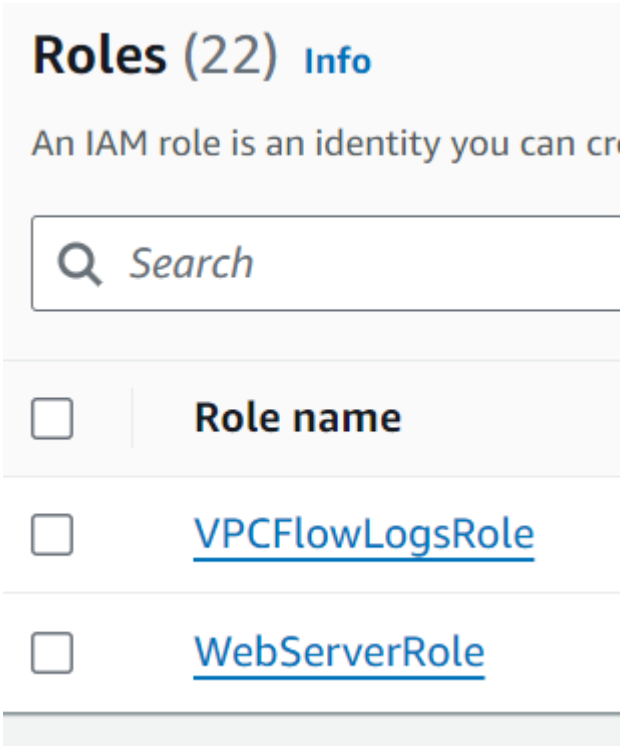

Query 6
Query 5
1 SELECT requester, operation, key, httpstatus
2 FROM "default"."bucket_logs"
3 WHERE requester LIKE 'arn:aws:iam%';



Phase 2: Securing VPCs

Task 2.1: Review LabVPC and its associated resources


VPC > Your VPCs > vpc-0c5491f25cd9300b1
vpc-0c5491f25cd9300b1 / LabVPC
Details Info
VPC ID
vpc-0c5491f25cd9300b1
State
Available
DNS hostnames
Enabled
Tenancy
Default
DHCP option set
dopt-0e07fceb09cfc793a
Main route table
rtb-0240fd1f797fdc9cb
Default VPC
No
IPv4 CIDR
10.1.0.0/16
IPv6 pool
–
Network Address Usage metrics
Disabled
Route 53 Resolver DNS Firewall rule groups
–
Owner ID
518337386052
Resource map
CIDRs
Flow logs
Tags
Integrations
Resource map Info
VPC Show details
Your AWS virtual network
LabVPC
Subnets (1)
Subnets within this VPC
us-east-1a
WebServerSubnet
Route tables (1)
Route network traffic to resources
rtb-0240fd1f797fdc9cb
Network connections (1)
Connections to other networks
LabVPCIG


Roles (22) Info
An IAM role is an identity you can cr
Search
Role name
VPCFlowLogsRole
WebServerRole

IAM > Roles > VPCFlowLogsRole

VPCFlowLogsRole Info

Summary

Creation date
September 28, 2024, 10:11 (UTC-03:00)

Last activity
-

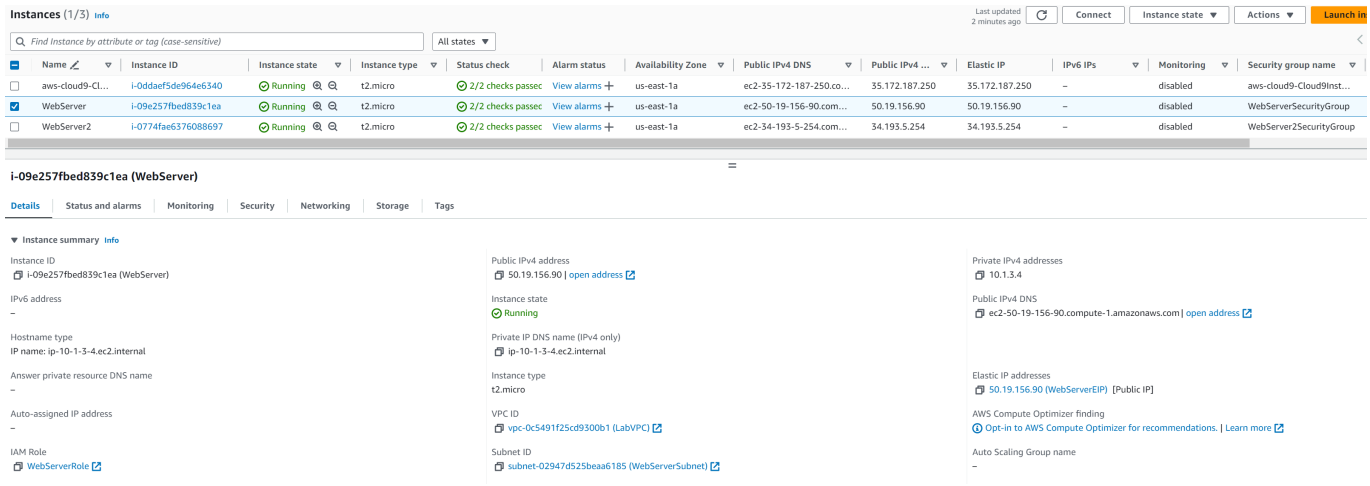
Permissions | Trust relationships | Tags (1) | Last Accessed

Permissions policies (1) Info

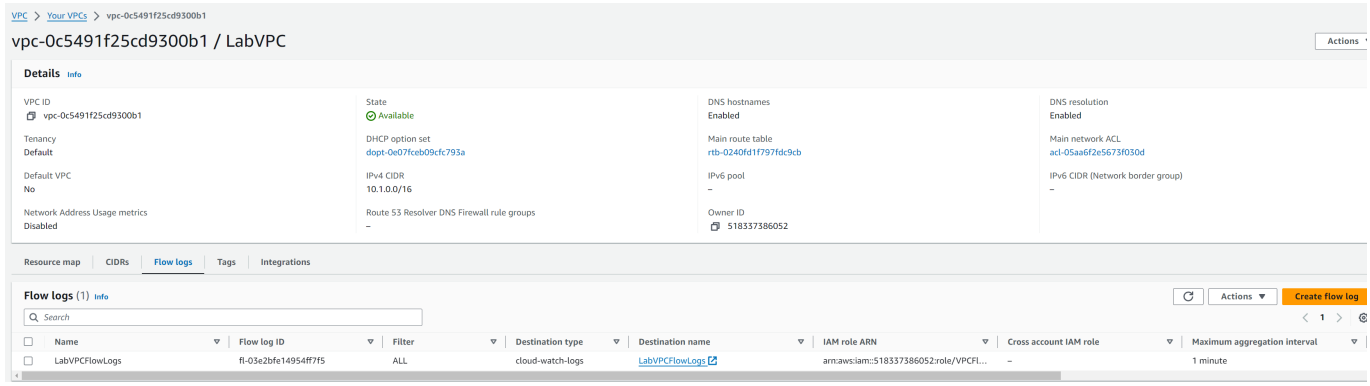
You can attach up to 10 managed policies.

Search

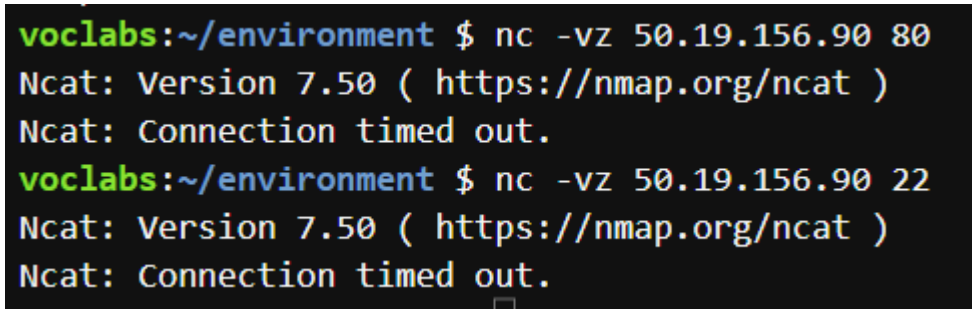
Policy name
VPCFlowLogPolicy

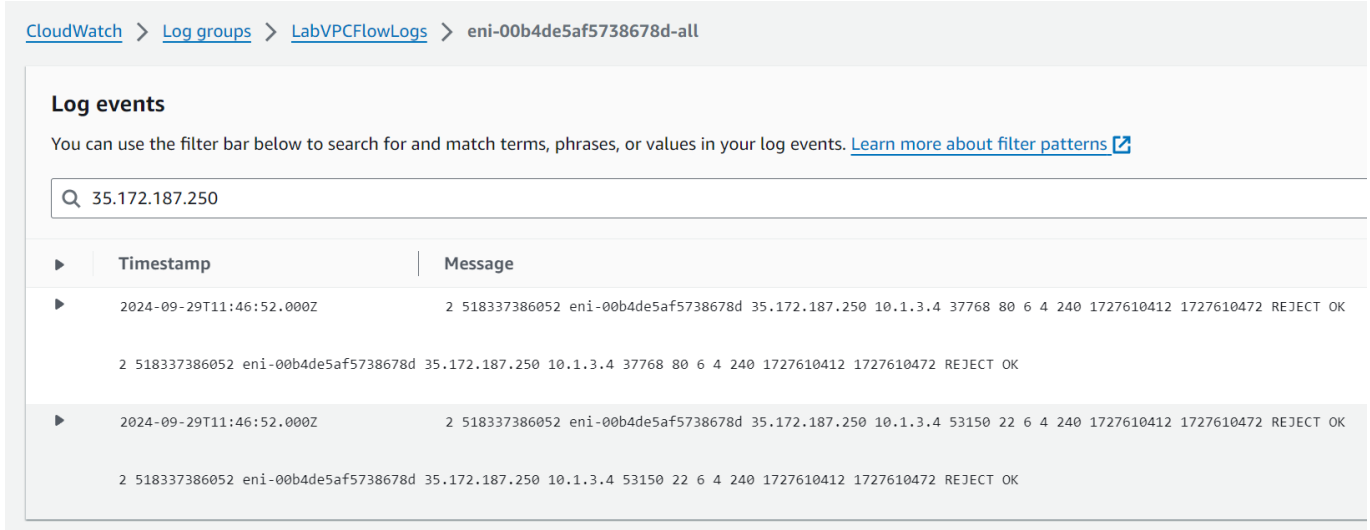


Task 2.2: Create a VPC flow log

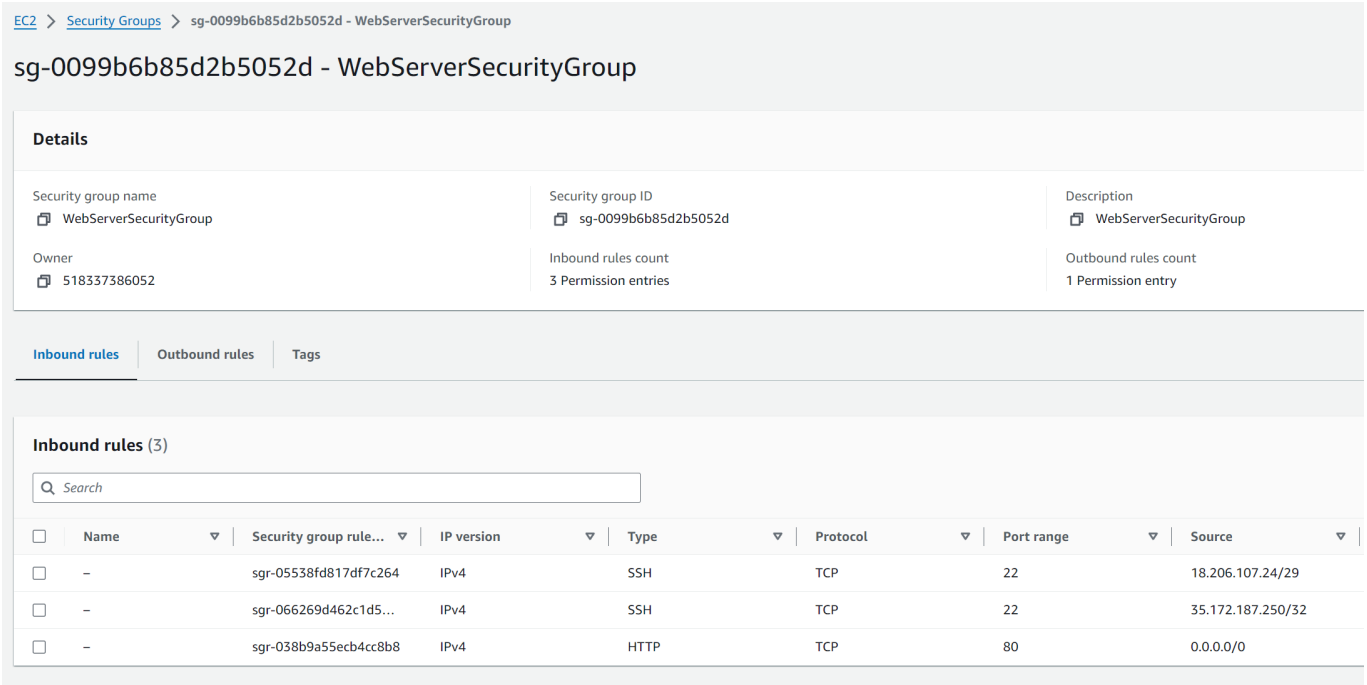


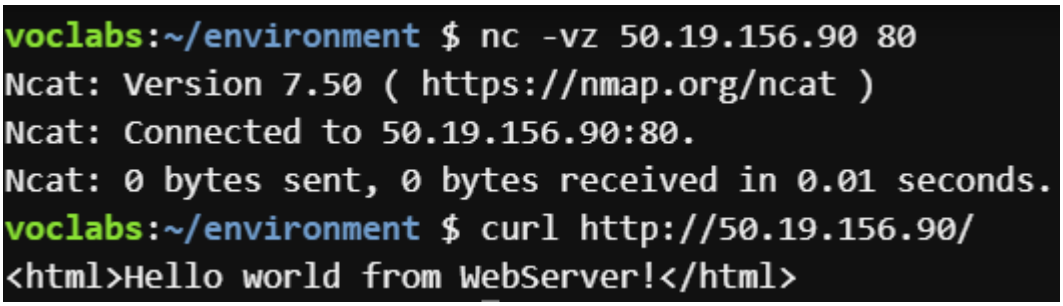
Task 2.3: Access the WebServer instance from the internet and review VPC flow logs in CloudWatch



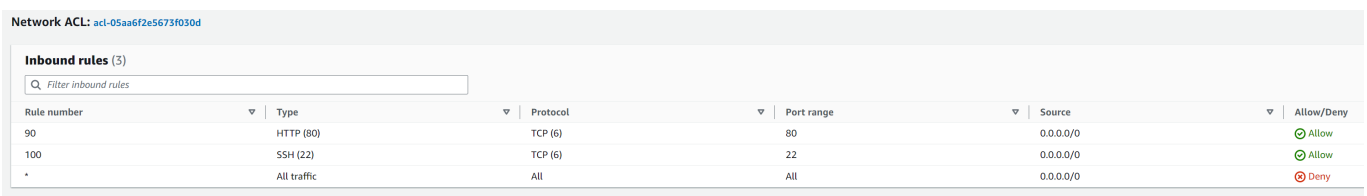


Task 2.4: Configure route table and security group settings



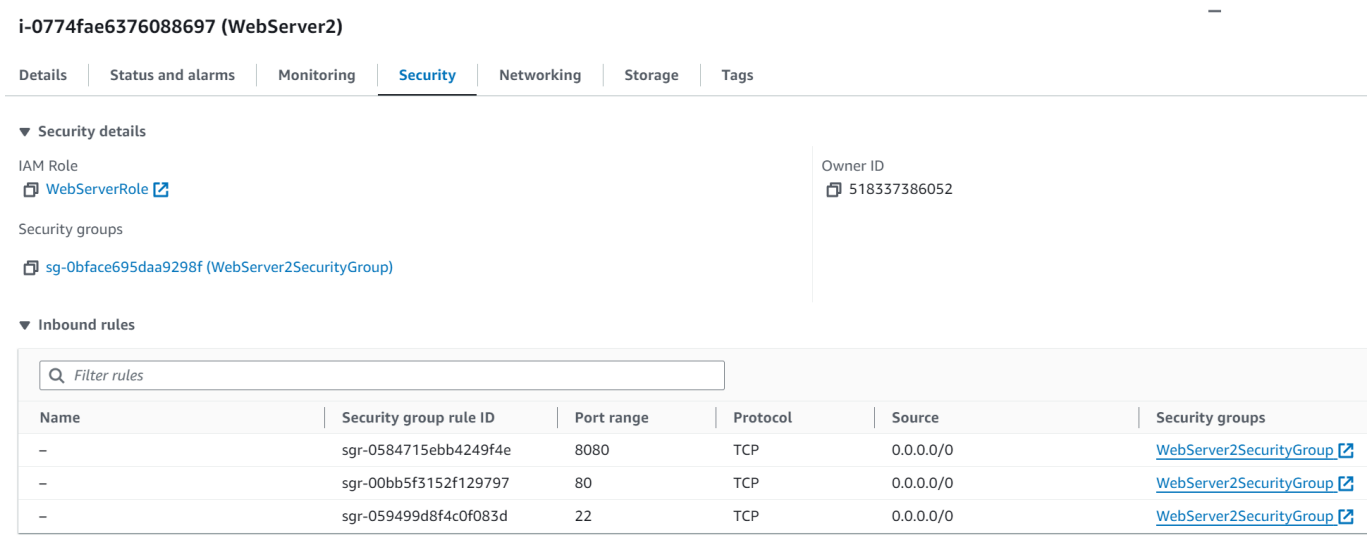


Task 2.5: Secure the WebServerSubnet with a network ACL



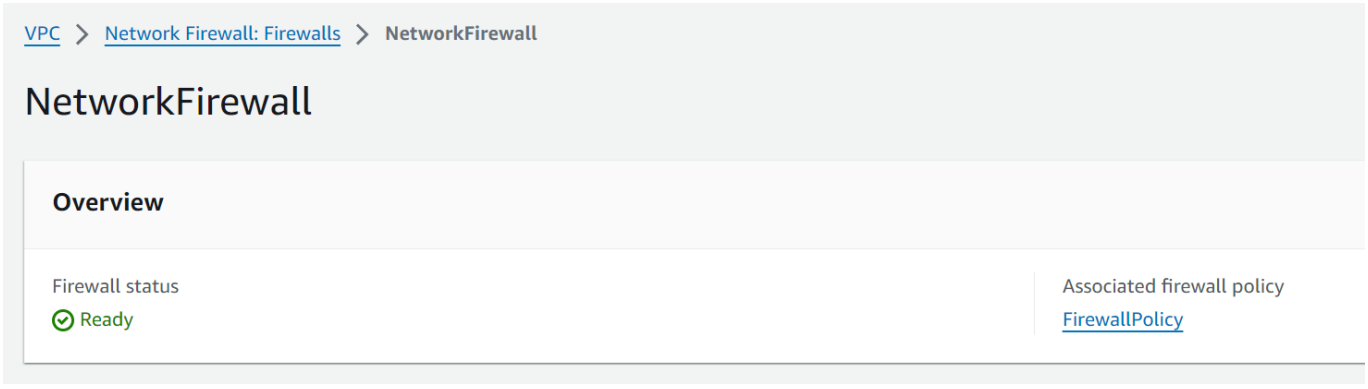
```
voclabs:~/environment $ nc -vz 50.19.156.90 22
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connected to 50.19.156.90:22.
Ncat: 0 bytes sent, 0 bytes received in 0.01 seconds.
voclabs:~/environment $ nc -vz 50.19.156.90 80
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connected to 50.19.156.90:80.
Ncat: 0 bytes sent, 0 bytes received in 0.01 seconds.
voclabs:~/environment $ curl http://50.19.156.90/
<html>Hello world from WebServer!</html>
```

Task 2.6: Review NetworkFirewallVPC and its associated resources

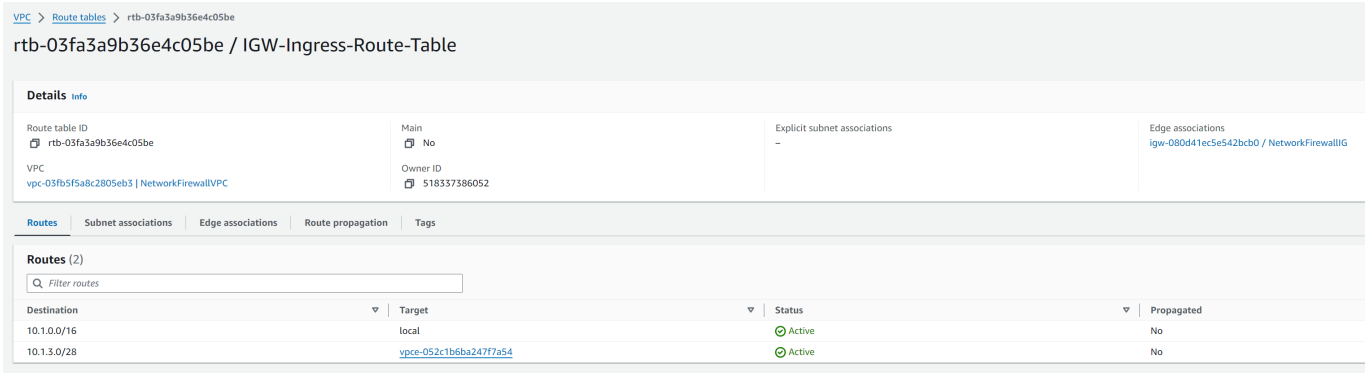


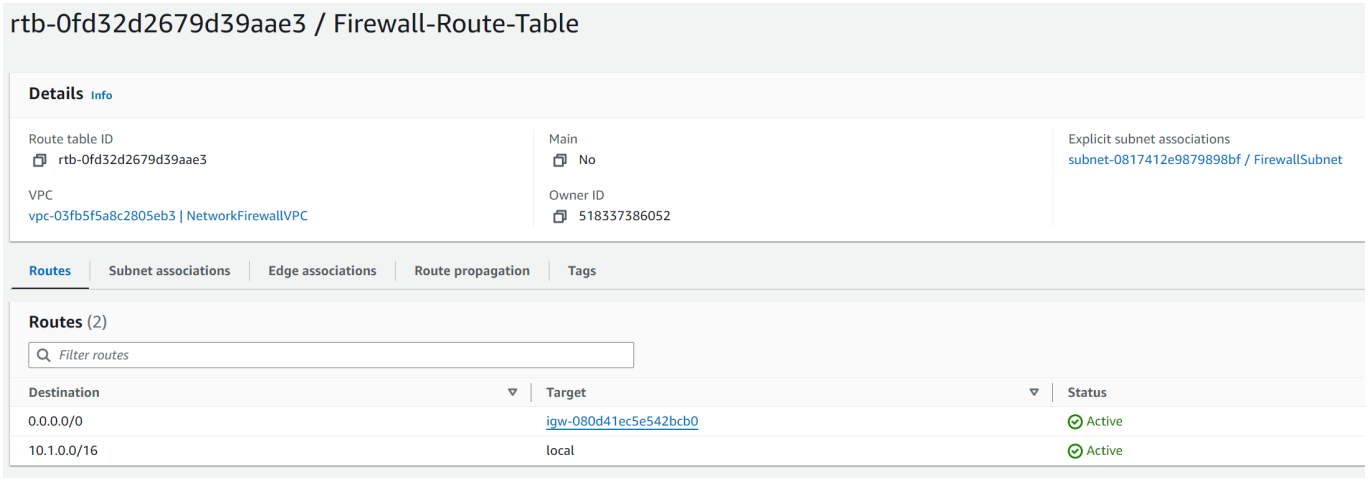

```
voclabs:~/environment $ nc -vz 34.193.5.254 22
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connected to 34.193.5.254:22.
Ncat: 0 bytes sent, 0 bytes received in 0.01 seconds.
voclabs:~/environment $ nc -vz 34.193.5.254 80
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connected to 34.193.5.254:80.
Ncat: 0 bytes sent, 0 bytes received in 0.01 seconds.
voclabs:~/environment $ curl http://34.193.5.254/
<html>Hello world from WebServer2!</html>
voclabs:~/environment $ curl http://34.193.5.254:8080
<html>Hello world from WebServer2 port 8080!</html>
```

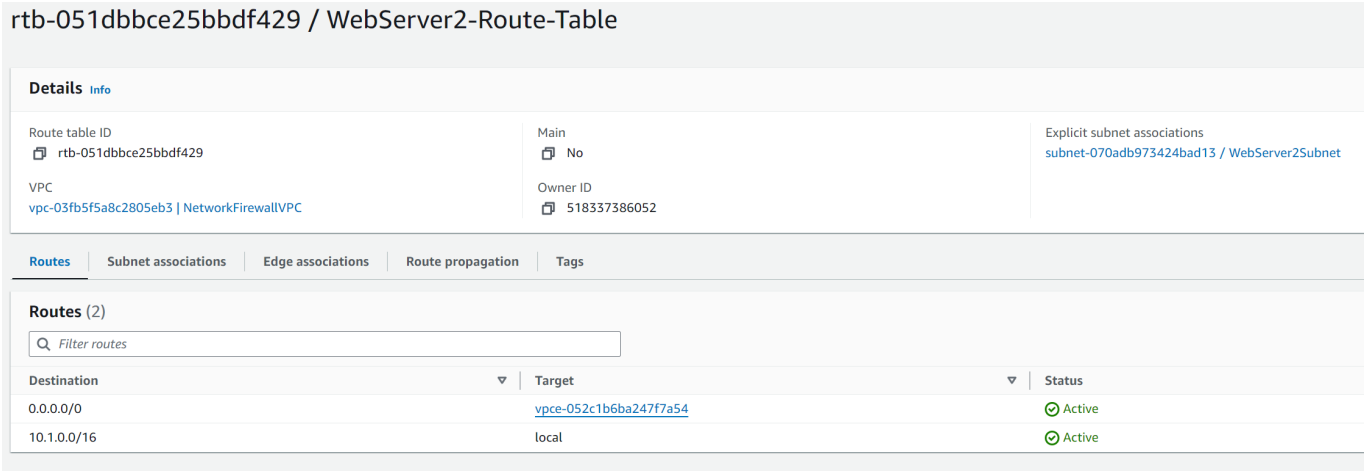
Task 2.7: Create a network firewall



Task 2.8: Create route tables







rtb-051dbbce25bbdf429 / WebServer2-Route-Table

Details Info

Route table ID rtb-051dbbce25bbdf429	Main No	Explicit subnet associations subnet-070adb973424bad13 / WebServer2Subnet
VPC vpc-03fb5f5a8c2805eb3 | NetworkFirewallVPC	Owner ID 518337386052	

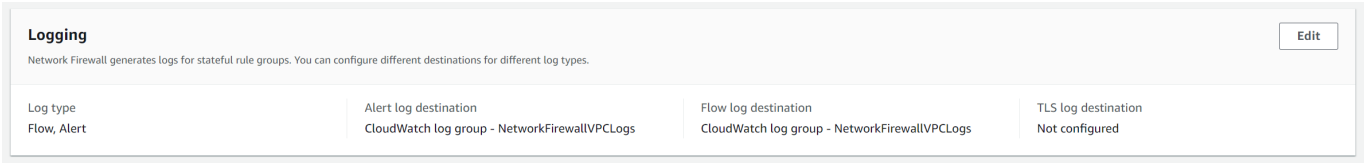
Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (2)

Filter routes

Destination	Target	Status
0.0.0.0/0	vpce-052c1b6ba247f7a54	Active
10.1.0.0/16	local	Active

Task 2.9: Configure logging for the network firewall

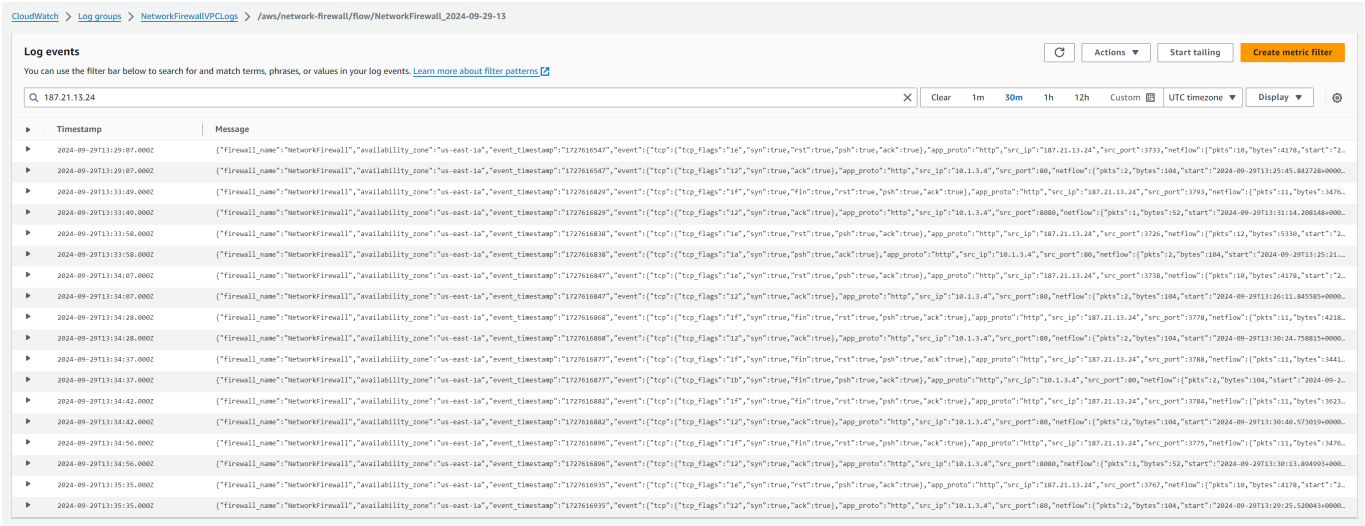


Logging

Network Firewall generates logs for stateful rule groups. You can configure different destinations for different log types.

Edit

Log type	Alert log destination	Flow log destination	TLS log destination
Flow, Alert	CloudWatch log group - NetworkFirewallVPCLogs	CloudWatch log group - NetworkFirewallVPCLogs	Not configured



CloudWatch > Log groups > NetworkFirewallVPCLogs > /aws/network-firewall/flow/NetworkFirewall_2024-09-29-13

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

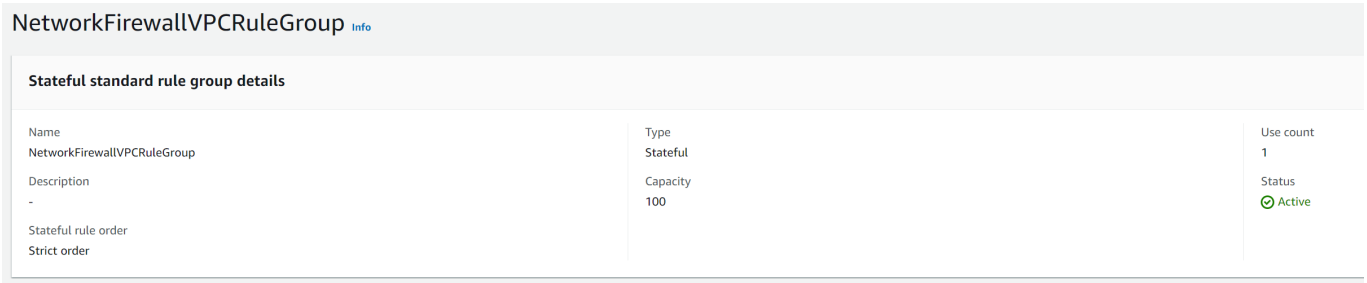
Actions | Start tailing | Create metric filter

187.21.13.24

Clear | 1m | 30m | 1h | 12h | Custom | UTC timezone | Display

Timestamp	Message
2024-09-29T13:29:07.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"1727616547","event":{"tcp":{"tcp_flags":"1e","syn":true,"rst":true,"psh":true,"ack":true},"app_proto":"http","src_ip":"187.21.13.24","src_port":3733,"netflow":{"pkts":10,"bytes":4178,"start":"2…
2024-09-29T13:29:07.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"1727616547","event":{"tcp":{"tcp_flags":"12","syn":true,"ack":true},"app_proto":"http","src_ip":"10.1.3.4","src_port":80,"netflow":{"pkts":2,"bytes":104,"start":"2024-09-29T13:25:45.842728+0000…
2024-09-29T13:33:49.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"1727616829","event":{"tcp":{"tcp_flags":"1f","syn":true,"fin":true,"rst":true,"psh":true,"ack":true},"app_proto":"http","src_ip":"187.21.13.24","src_port":3793,"netflow":{"pkts":11,"bytes":3476…
2024-09-29T13:33:49.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"1727616829","event":{"tcp":{"tcp_flags":"12","syn":true,"ack":true},"app_proto":"http","src_ip":"10.1.3.4","src_port":8080,"netflow":{"pkts":1,"bytes":52,"start":"2024-09-29T13:31:14.208148+000…
2024-09-29T13:33:58.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"1727616838","event":{"tcp":{"tcp_flags":"1e","syn":true,"rst":true,"psh":true,"ack":true},"app_proto":"http","src_ip":"187.21.13.24","src_port":3726,"netflow":{"pkts":12,"bytes":5330,"start":"2…
2024-09-29T13:33:58.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"1727616838","event":{"tcp":{"tcp_flags":"1a","syn":true,"psh":true,"ack":true},"app_proto":"http","src_ip":"10.1.3.4","src_port":80,"netflow":{"pkts":2,"bytes":104,"start":"2024-09-29T13:25:21…
2024-09-29T13:34:07.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"1727616847","event":{"tcp":{"tcp_flags":"1e","syn":true,"rst":true,"psh":true,"ack":true},"app_proto":"http","src_ip":"187.21.13.24","src_port":3738,"netflow":{"pkts":10,"bytes":4178,"start":"2…
2024-09-29T13:34:07.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"1727616847","event":{"tcp":{"tcp_flags":"12","syn":true,"ack":true},"app_proto":"http","src_ip":"10.1.3.4","src_port":80,"netflow":{"pkts":2,"bytes":104,"start":"2024-09-29T13:26:11.845585+0000…
2024-09-29T13:34:28.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"1727616868","event":{"tcp":{"tcp_flags":"1f","syn":true,"fin":true,"rst":true,"psh":true,"ack":true},"app_proto":"http","src_ip":"187.21.13.24","src_port":3778,"netflow":{"pkts":11,"bytes":4218…
2024-09-29T13:34:28.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"1727616868","event":{"tcp":{"tcp_flags":"12","syn":true,"ack":true},"app_proto":"http","src_ip":"10.1.3.4","src_port":80,"netflow":{"pkts":2,"bytes":104,"start":"2024-09-29T13:30:24.758815+0000…
2024-09-29T13:34:37.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"1727616877","event":{"tcp":{"tcp_flags":"1f","syn":true,"fin":true,"rst":true,"psh":true,"ack":true},"app_proto":"http","src_ip":"187.21.13.24","src_port":3788,"netflow":{"pkts":11,"bytes":3441…
2024-09-29T13:34:37.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"1727616877","event":{"tcp":{"tcp_flags":"1b","syn":true,"fin":true,"psh":true,"ack":true},"app_proto":"http","src_ip":"10.1.3.4","src_port":80,"netflow":{"pkts":2,"bytes":104,"start":"2024-09-2…
2024-09-29T13:34:42.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"1727616882","event":{"tcp":{"tcp_flags":"1f","syn":true,"fin":true,"rst":true,"psh":true,"ack":true},"app_proto":"http","src_ip":"187.21.13.24","src_port":3784,"netflow":{"pkts":11,"bytes":3623…
2024-09-29T13:34:42.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"1727616882","event":{"tcp":{"tcp_flags":"12","syn":true,"ack":true},"app_proto":"http","src_ip":"10.1.3.4","src_port":80,"netflow":{"pkts":2,"bytes":104,"start":"2024-09-29T13:30:40.573019+0000…
2024-09-29T13:34:56.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"1727616896","event":{"tcp":{"tcp_flags":"1f","syn":true,"fin":true,"rst":true,"psh":true,"ack":true},"app_proto":"http","src_ip":"187.21.13.24","src_port":3775,"netflow":{"pkts":11,"bytes":3476…
2024-09-29T13:34:56.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"1727616896","event":{"tcp":{"tcp_flags":"12","syn":true,"ack":true},"app_proto":"http","src_ip":"10.1.3.4","src_port":8080,"netflow":{"pkts":1,"bytes":52,"start":"2024-09-29T13:30:13.804993+000…
2024-09-29T13:35:35.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"1727616935","event":{"tcp":{"tcp_flags":"1e","syn":true,"rst":true,"psh":true,"ack":true},"app_proto":"http","src_ip":"187.21.13.24","src_port":3767,"netflow":{"pkts":10,"bytes":4178,"start":"2…
2024-09-29T13:35:35.000Z	{"firewall_name":"NetworkFirewall","availability_zone":"us-east-1a","event_timestamp":"1727616935","event":{"tcp":{"tcp_flags":"12","syn":true,"ack":true},"app_proto":"http","src_ip":"10.1.3.4","src_port":80,"netflow":{"pkts":2,"bytes":104,"start":"2024-09-29T13:29:25.520043+0000…

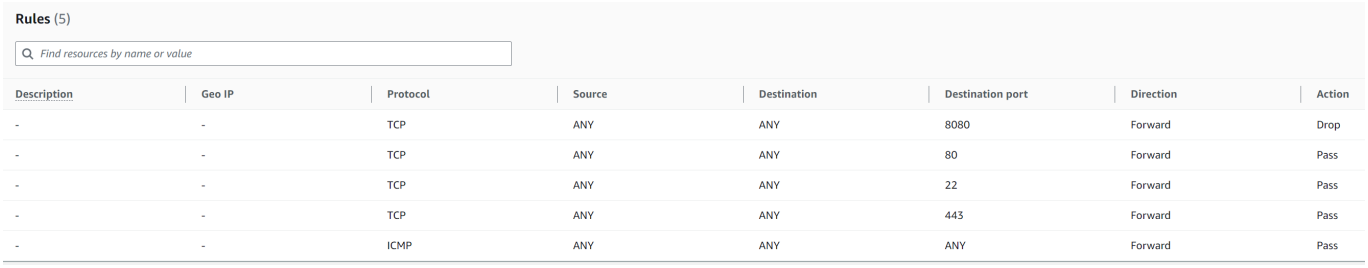
Task 2.10: Configure the firewall policy and test access



NetworkFirewallVPCRuleGroup Info

Stateful standard rule group details

Name NetworkFirewallVPCRuleGroup	Type Stateful	Use count 1
Description -	Capacity 100	Status Active
Stateful rule order Strict order		



Rules (5)

Find resources by name or value

Description	Geo IP	Protocol	Source	Destination	Destination port	Direction	Action
-	-	TCP	ANY	ANY	8080	Forward	Drop
-	-	TCP	ANY	ANY	80	Forward	Pass
-	-	TCP	ANY	ANY	22	Forward	Pass
-	-	TCP	ANY	ANY	443	Forward	Pass
-	-	ICMP	ANY	ANY	ANY	Forward	Pass

```
voclabs:~/environment $ nc -vz 34.193.5.254 80
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connected to 34.193.5.254:80.
Ncat: 0 bytes sent, 0 bytes received in 0.01 seconds.
voclabs:~/environment $ nc -vz 34.193.5.254 22
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connected to 34.193.5.254:22.
Ncat: 0 bytes sent, 0 bytes received in 0.01 seconds.
voclabs:~/environment $ curl http://34.193.5.254:8080
^C
voclabs:~/environment $ curl http://34.193.5.254:80
<html>Hello world from WebServer2!</html>
```

```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Sun Sep 29 12:39:55 2024 from 18.206.107.28
[ec2-user@webserver2 ~]$ ping -c 3 www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.154.236.231) 56(84) bytes of data.
64 bytes from server-18-154-236-231.iad55.r.cloudfront.net (18.154.236.231): icmp_seq=1 ttl=244 time=3.77 ms
64 bytes from server-18-154-236-231.iad55.r.cloudfront.net (18.154.236.231): icmp_seq=2 ttl=244 time=2.42 ms
64 bytes from server-18-154-236-231.iad55.r.cloudfront.net (18.154.236.231): icmp_seq=3 ttl=244 time=2.22 ms

--- d3ag4hukkh62yn.cloudfront.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 2.220/2.806/3.774/0.689 ms
[ec2-user@webserver2 ~]$ sudo netstat -tulpn | grep -i listen
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2331/sshd: /usr/sbi
tcp        0      0 0.0.0.0:8080            0.0.0.0:*               LISTEN      7247/python3
tcp6       0      0 :::22                   :::*                    LISTEN      2331/sshd: /usr/sbi
tcp6       0      0 :::80                   :::*                    LISTEN      1998/httpd
[ec2-user@webserver2 ~]$
```

Phase 3: Securing AWS resources by using AWS KMS

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

KMS > Customer managed keys > Key ID: ec6e4c68-5c3f-456f-b6d8-df77f09a2202

ec6e4c68-5c3f-456f-b6d8-df77f09a2202

General configuration

Alias
MyKMSKey

Status
Enabled

ARN
arn:aws:kms:us-east-1:518337386052:key/ec6e4c68-5c3f-456f-b6d8-df77f09a2202

Description
-

Key policy | Cryptographic configuration | Tags | Key rotation | Aliases

Key policy

Key administrators (1)

Choose the IAM users and roles who can administer this key through the KMS API. You might need to add additional permissions for the users or role

Search Key administrators

Name	Path
voclabs	/

Key deletion

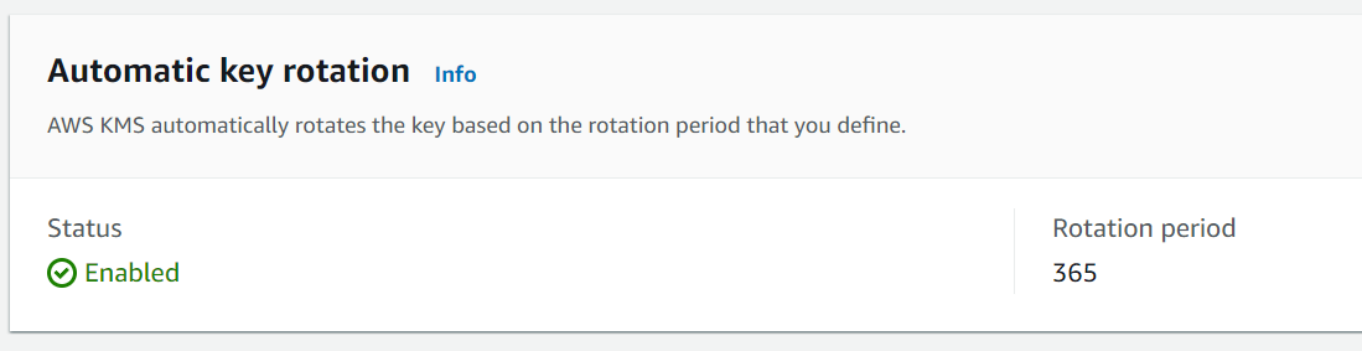
☑ Allow key administrators to delete this key

Key users (1)

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 us

Search Key users

Name	Path
voclabs	/



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

KMS > Customer managed keys > Key ID: ec6e4c68-5c3f-456f-b6d8-df77f09a2202

ec6e4c68-5c3f-456f-b6d8-df77f09a2202

General configuration

Alias

MyKMSKey

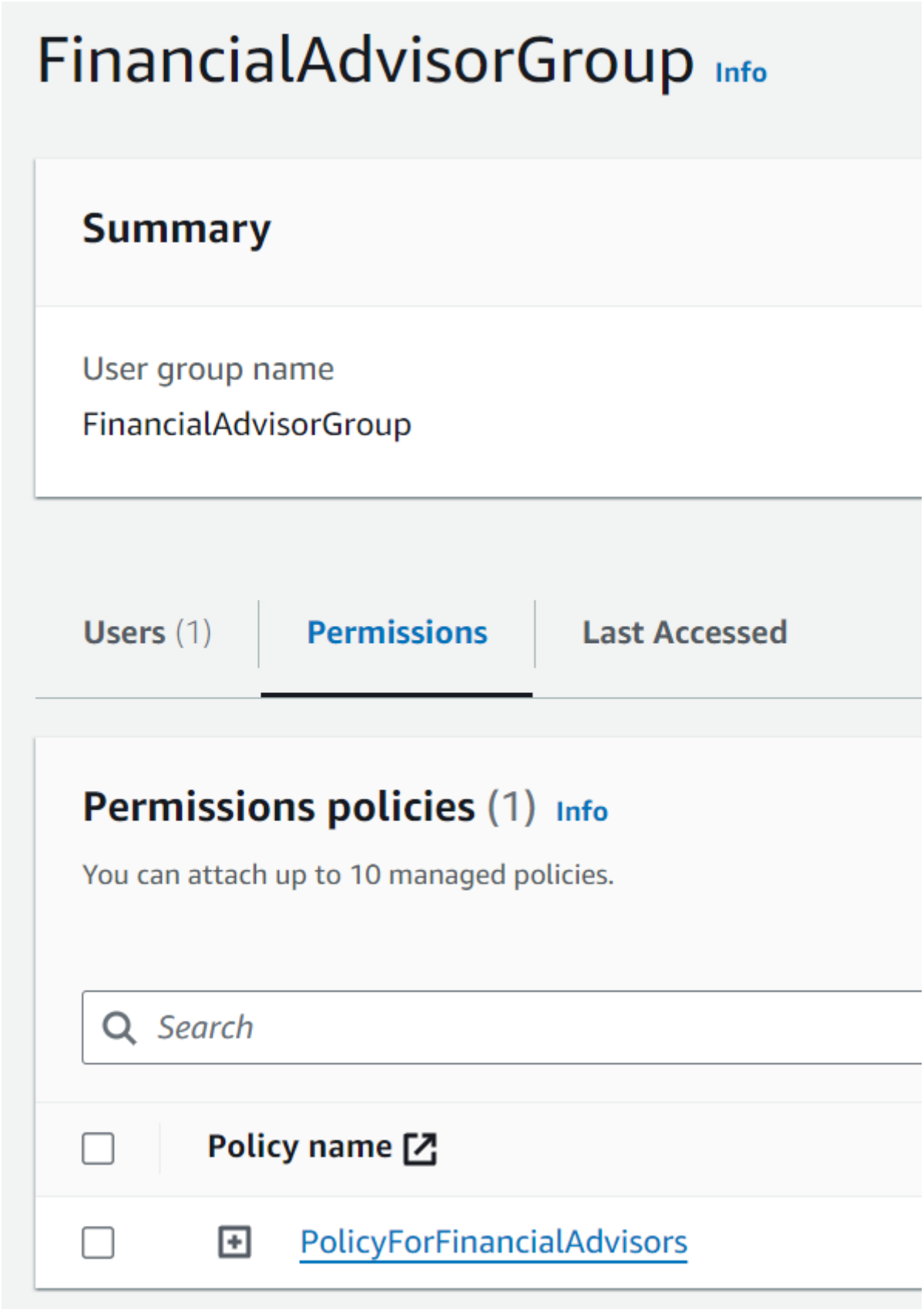
ARN

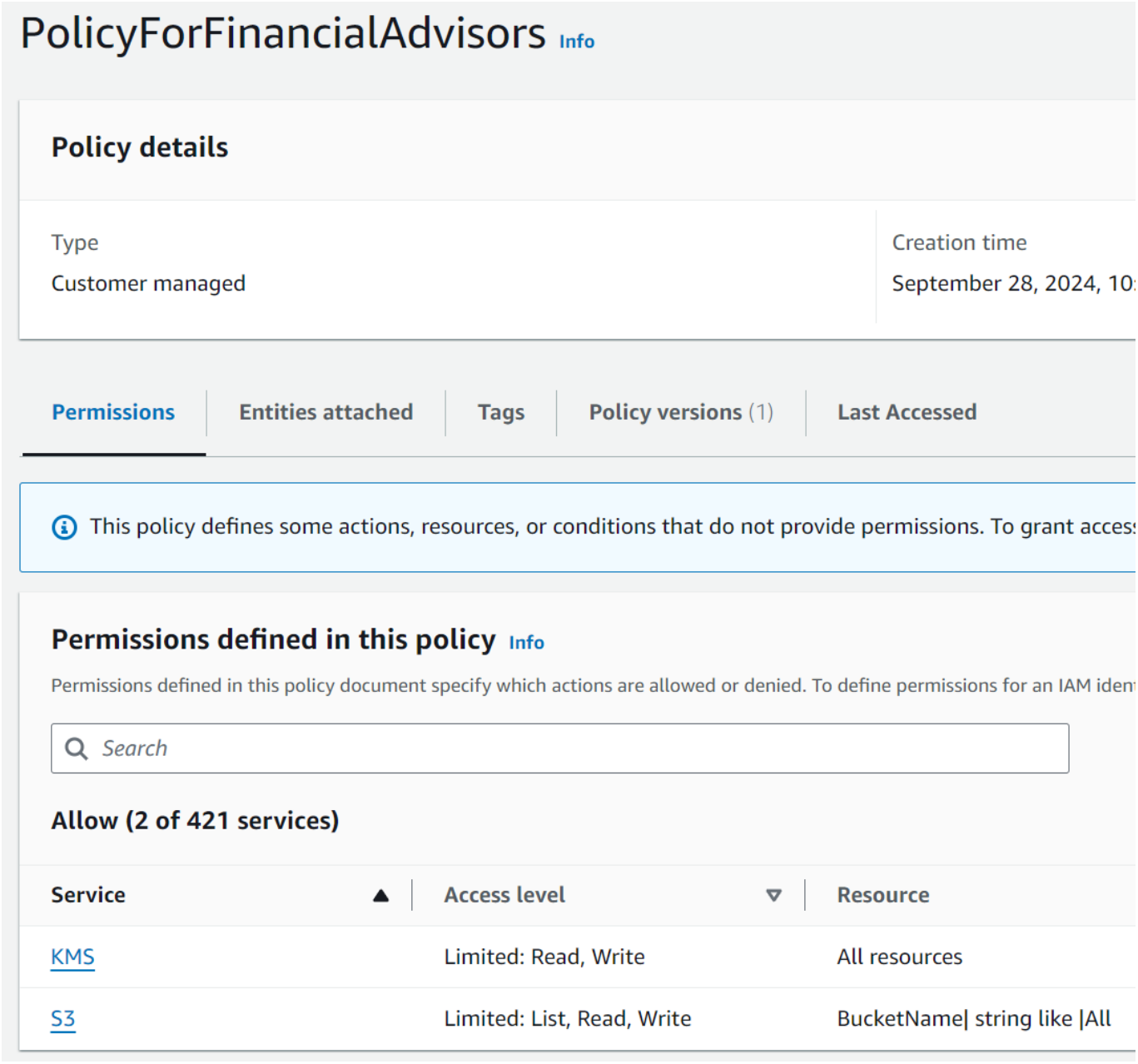
arn:aws:kms:us-east-1:518337386052:key/ec6e4c68-5c3f-456f-b6d8-df77f09a22C

Key policy | Cryptographic configuration | Tags | Key rotation | Alia

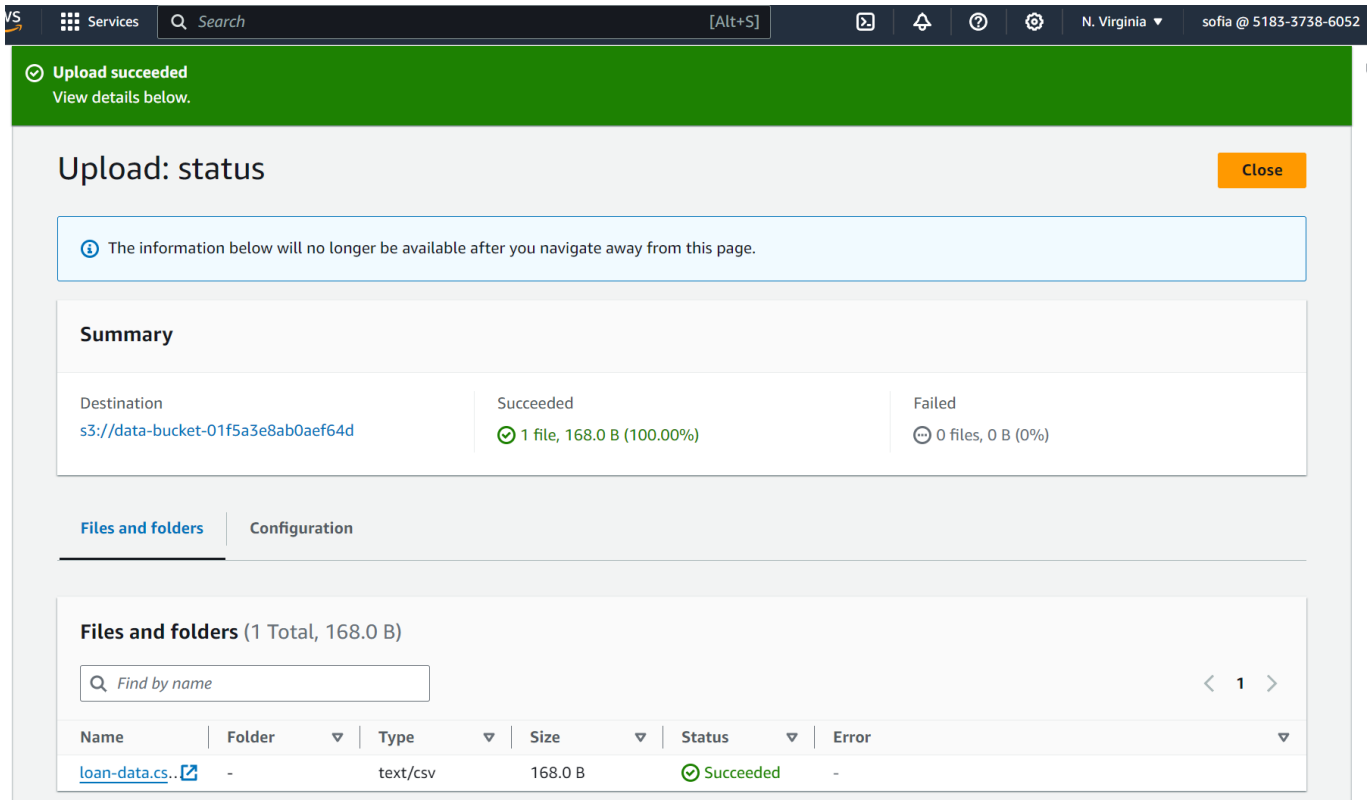
Key policy

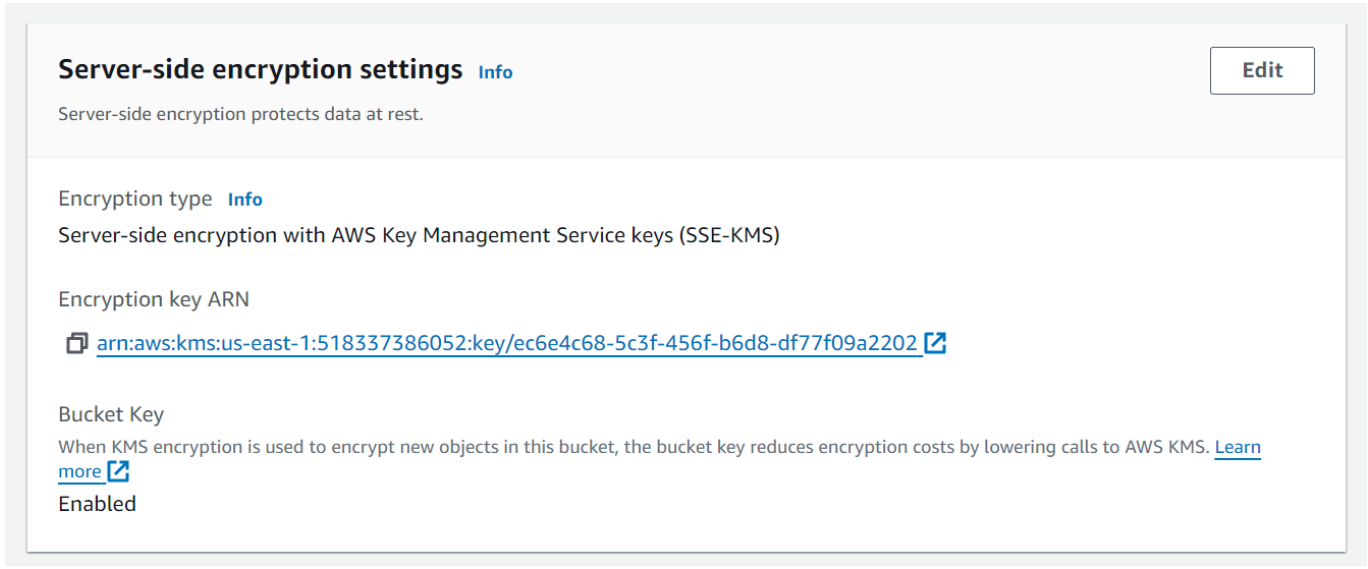
```
        ],
        "Resource": "*"
    },
    {
        "Sid": "Allow use of the key",
        "Effect": "Allow",
        "Principal": {
            "AWS": [
                "arn:aws:iam::518337386052:role/voclabs",
                "arn:aws:iam::518337386052:user/sofia"
            ]
```


FinancialAdvisorGroup Info
Summary
User group name
FinancialAdvisorGroup
Users (1)
Permissions
Last Accessed
Permissions policies (1) Info
You can attach up to 10 managed policies.
Search
Policy name
PolicyForFinancialAdvisors

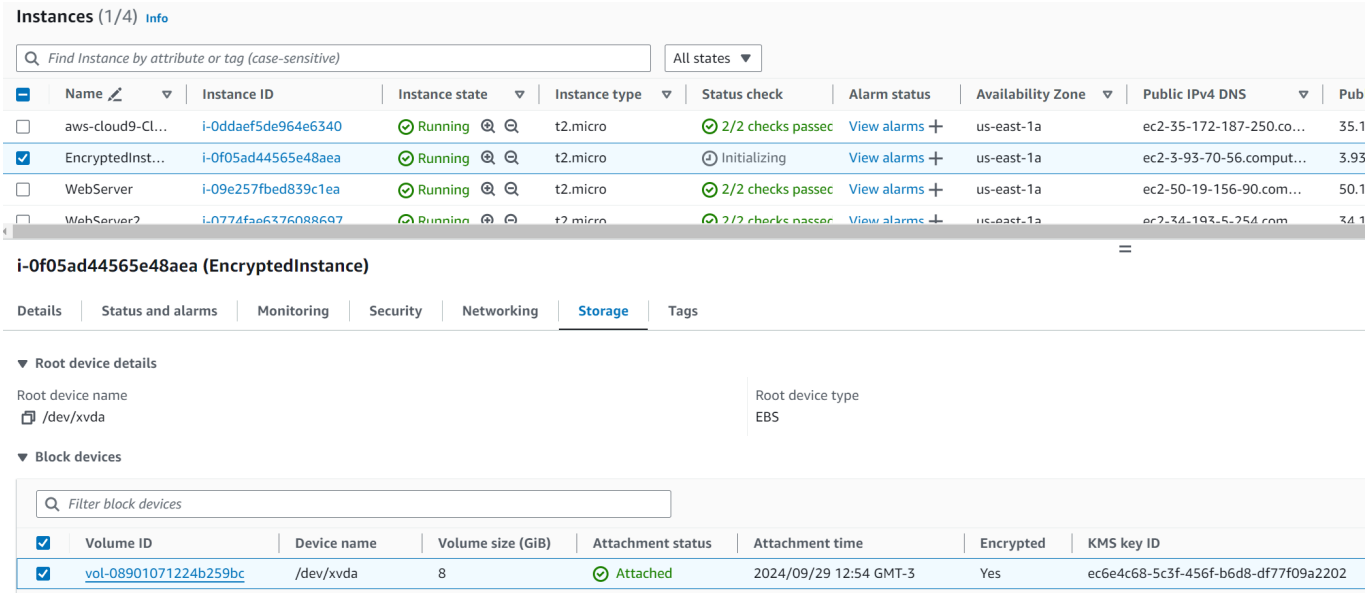


Task 3.3: Use AWS KMS to encrypt data in Amazon S3





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

```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Sun Sep 29 13:51:50 2024 from 18.206.107.27
[ec2-user@webserver2 ~]$ echo "Let's encrypt these file contents. Sensitive data here." > data_unencrypted.txt
[ec2-user@webserver2 ~]$ cat data_unencrypted.txt
Let's encrypt these file contents. Sensitive data here.
[ec2-user@webserver2 ~]$ aws kms list-keys
{
    "Keys": [
        {
            "KeyId": "2325c571-f352-4aa8-8da9-3271d070d7df",
            "KeyArn": "arn:aws:kms:us-east-1:518337386052:key/2325c571-f352-4aa8-8da9-3271d070d7df"
        },
        {
            "KeyId": "b99b66cb-bf3e-4e07-b459-48a8135f6533",
            "KeyArn": "arn:aws:kms:us-east-1:518337386052:key/b99b66cb-bf3e-4e07-b459-48a8135f6533"
        },
        {
            "KeyId": "ec6e4c68-5c3f-456f-b6d8-df77f09a2202",
            "KeyArn": "arn:aws:kms:us-east-1:518337386052:key/ec6e4c68-5c3f-456f-b6d8-df77f09a2202"
        }
    ]
}
[ec2-user@webserver2 ~]$ result=$(aws kms generate-data-key --key-id alias/MyKMSKey --key-spec AES_256)
echo $result | python3 -m json.tool
{
    "CiphertextBlob": "AQIDAHhEpCW7g3QGgj+PiTiImuyJdxXrkS812f7zcEPDgiJ/VQHqhBHo8aaGq3Lt7SLRhBpvAAAAfjB8BgkqhkiG9w0
    "Plaintext": "pzy+3UIVDHoSdm/4bbWgZpVwtv35tRpWYZRTDUmcyFI=",
    "KeyId": "arn:aws:kms:us-east-1:518337386052:key/ec6e4c68-5c3f-456f-b6d8-df77f09a2202"
}
[ec2-user@webserver2 ~]$
```

```
[ec2-user@webserver2 ~]$ dk_cipher=$(echo $result| jq '.CiphertextBlob' | cut -d '"' -f2)
echo $dk_cipher
echo $dk_cipher | base64 --decode > data_key_ciphertext
AQIDAHhEpCW7g3QGgj+PiTiImuyJdxXrkS812f7zcEPDgiJ/VQHqhBHo8aaGq3Lt7SLRhBpvAAAAfjB8BgkqhkiG9w0BBwagbzBtAgEAMGgGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMM86/8nsTtET5HPq/AgEQgDuyXYmnCYecMhtkwlW2rIrFqCQH96BQ
[ec2-user@webserver2 ~]$ cat data_key_ciphertext
0o0m0ht  e.0  %  CA"U  r  o~0|  *
          3o  aws kms decrypt --ciphertext-blob fileb://./data_key_ciphertext --query Plaintext --output text
pzy+3UIVDHoSdm/4bbWgZpVwtv35tRpWYZRTDUmcyFI=
[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 ~]$ 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__G
          ]  FS  b                  \.c  [ec2-user@webserver2 ~]$ ls -la
total 56
drwx------. 3 ec2-user ec2-user 16384 Sep 29 16:02 .
drwxr-xr-x. 3 root     root        22 Sep 28 13:14 ..
-rw-------. 1 ec2-user ec2-user    92 Sep 29 14:05 .bash_history
-rw-r--r--. 1 ec2-user ec2-user    18 Jan 28  2023 .bash_logout
-rw-r--r--. 1 ec2-user ec2-user   141 Jan 28  2023 .bash_profile
-rw-r--r--. 1 ec2-user ec2-user   492 Jan 28  2023 .bashrc
-rw-------. 1 ec2-user ec2-user    20 Sep 29 16:01 .lesshst
drwx------. 2 ec2-user ec2-user    29 Sep 28 13:14 .ssh
-rw-r--r--. 1 ec2-user ec2-user    80 Sep 29 16:02 data_encrypted
-rw-r--r--. 1 ec2-user ec2-user   184 Sep 29 16:00 data_key_ciphertext
-rw-r--r--. 1 ec2-user ec2-user    32 Sep 29 16:01 data_key_plaintext_encrypted
-rw-r--r--. 1 ec2-user ec2-user    56 Sep 29 15:58 data_unencrypted.txt
-rw-r--r--. 1 ec2-user root        52 Sep 28 13:14 index.html
[ec2-user@webserver2 ~]$ rm data_unencrypted.txt
[ec2-user@webserver2 ~]$
```

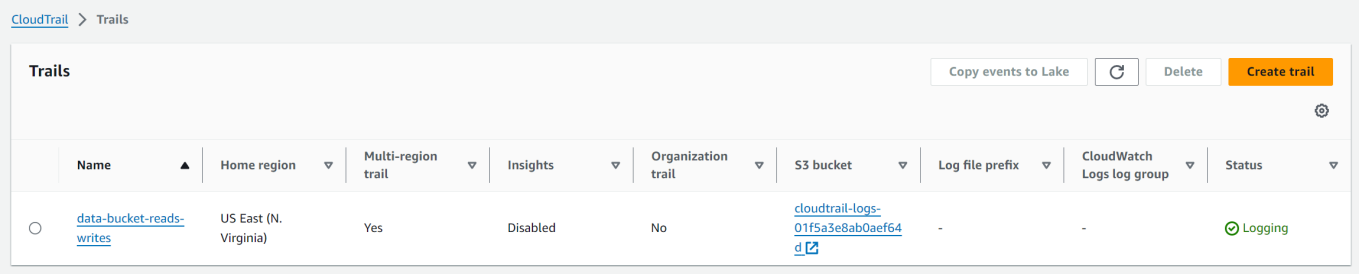
```
[ec2-user@webserver2 ~]$ openssl enc -d -aes-256-cbc -pbkdf2 -in data_encrypted -out data_decrypted.txt -pass file:./data_key_plaintext_encrypted
[ec2-user@webserver2 ~]$ cat data_decrypted.txt
Let's encrypt these file contents. Sensitive data here.
[ec2-user@webserver2 ~]$
```

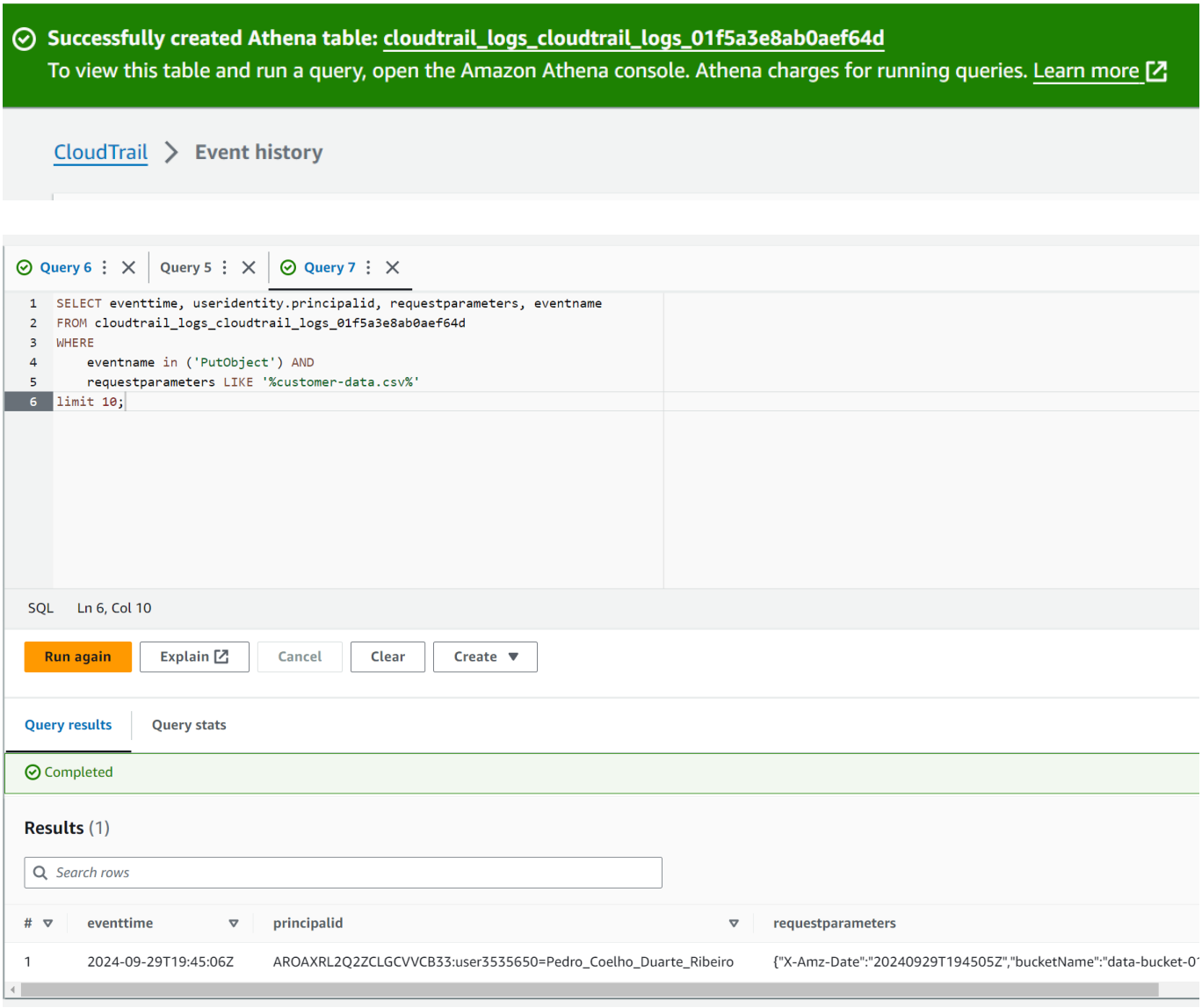
Task 3.6: Use AWS KMS to encrypt a Secrets Manager secret

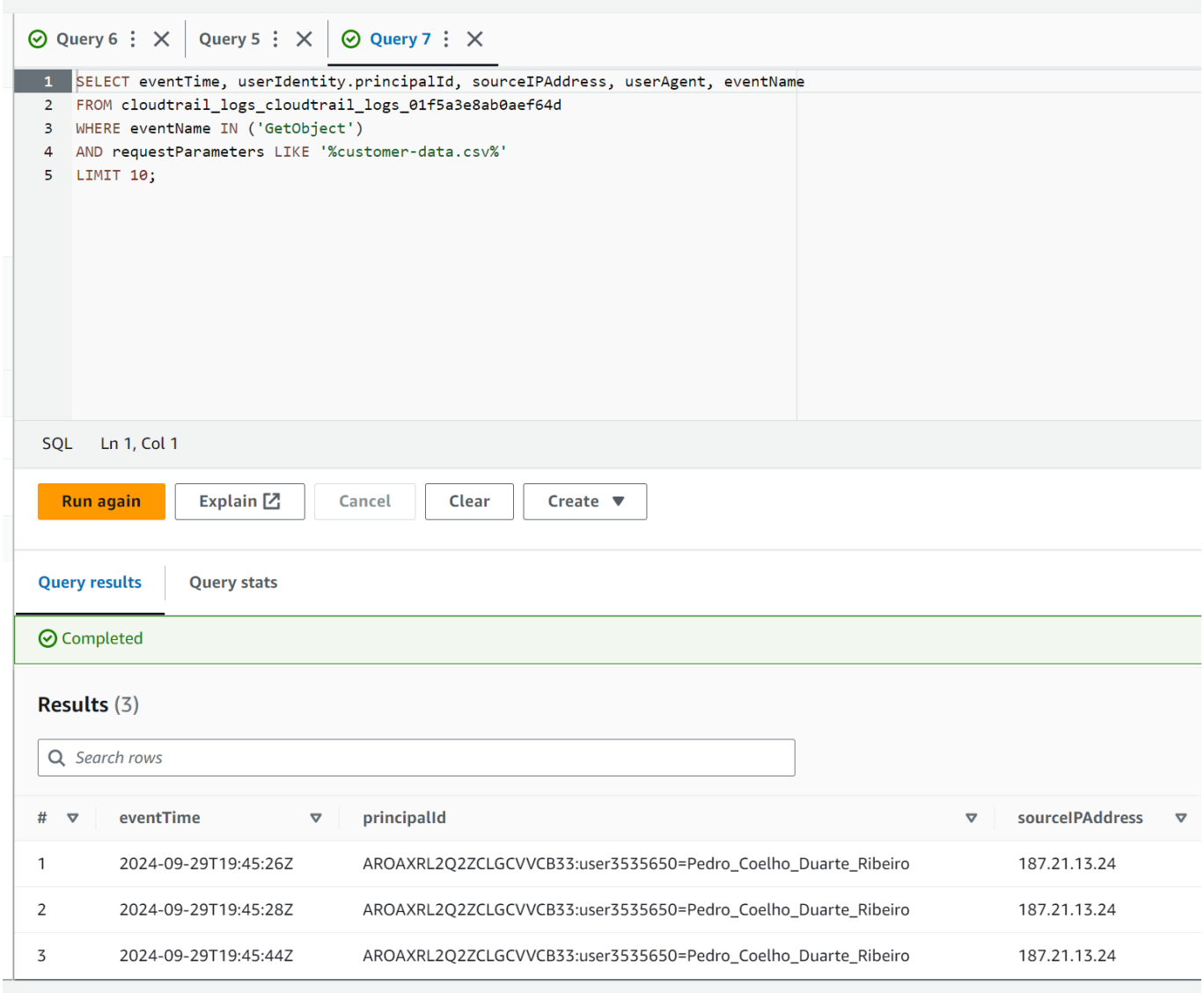
```
[ec2-user@webserver2 ~]$ aws secretsmanager list-secrets
{
    "SecretList": [
        {
            "ARN": "arn:aws:secretsmanager:us-east-1:518337386052:secret:mysecret-M3jOwd",
            "Name": "mysecret",
            "KmsKeyId": "arn:aws:kms:us-east-1:518337386052:key/ec6e4c68-5c3f-456f-b6d8-df77f09a2202",
            "LastChangedDate": "2024-09-29T16:06:50.152000+00:00",
            "Tags": [],
            "SecretVersionsToStages": {
                "2d6b815e-04d9-475d-875e-f86976acde1f": [
                    "AWSCURRENT"
                ]
            },
            "CreatedDate": "2024-09-29T16:06:50.087000+00:00"
        }
    ]
}
[ec2-user@webserver2 ~]$ aws secretsmanager get-secret-value --secret-id mysecret
{
    "ARN": "arn:aws:secretsmanager:us-east-1:518337386052:secret:mysecret-M3jOwd",
    "Name": "mysecret",
    "VersionId": "2d6b815e-04d9-475d-875e-f86976acde1f",
    "SecretString": "{\"secret\":\"my secret data\"}",
    "VersionStages": [
        "AWSCURRENT"
    ],
    "CreatedDate": "2024-09-29T16:06:50.146000+00:00"
}
[ec2-user@webserver2 ~]$
```

Phase 4: Monitoring and logging

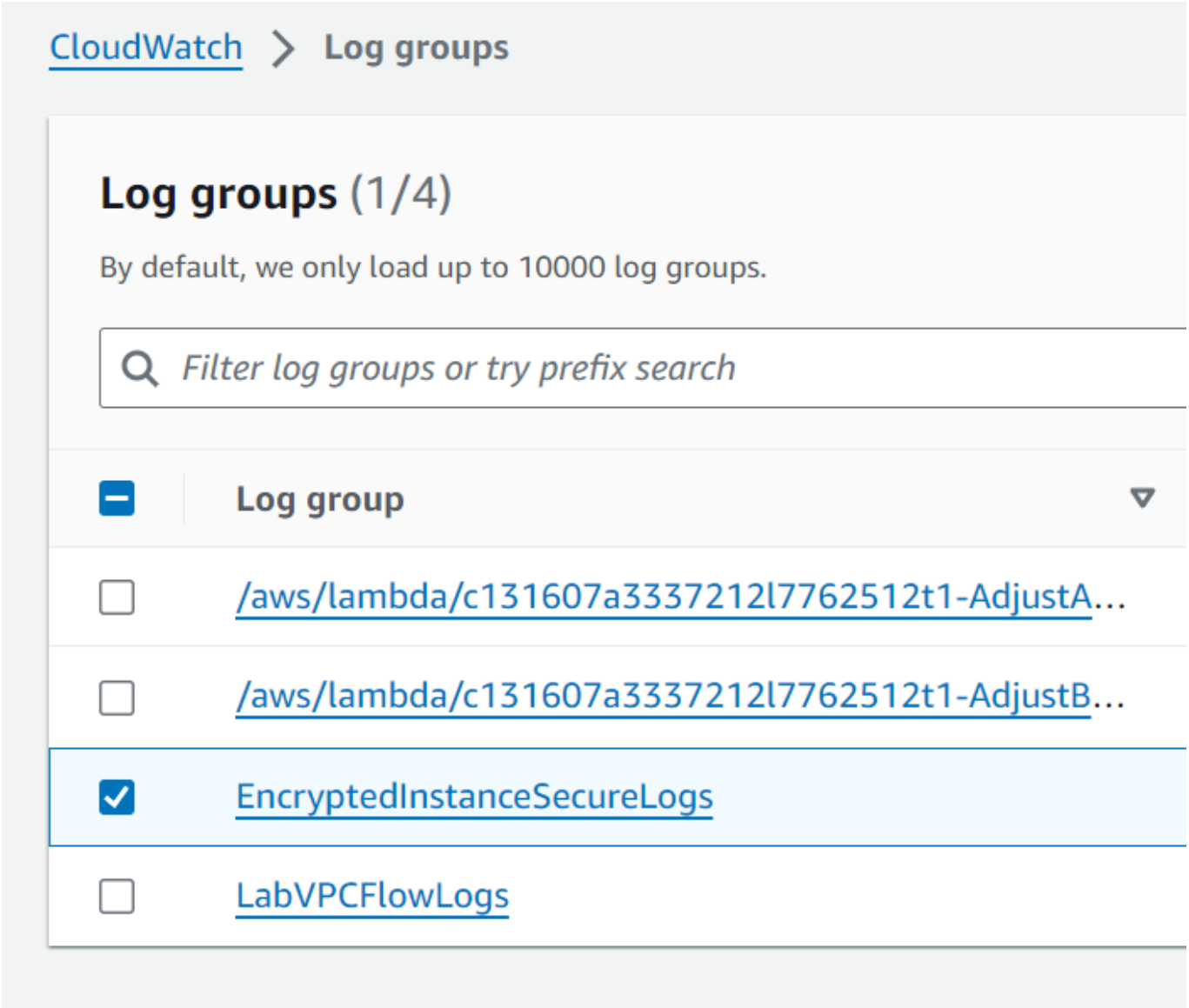
Task 4.1: Use CloudTrail to record Amazon S3 API calls

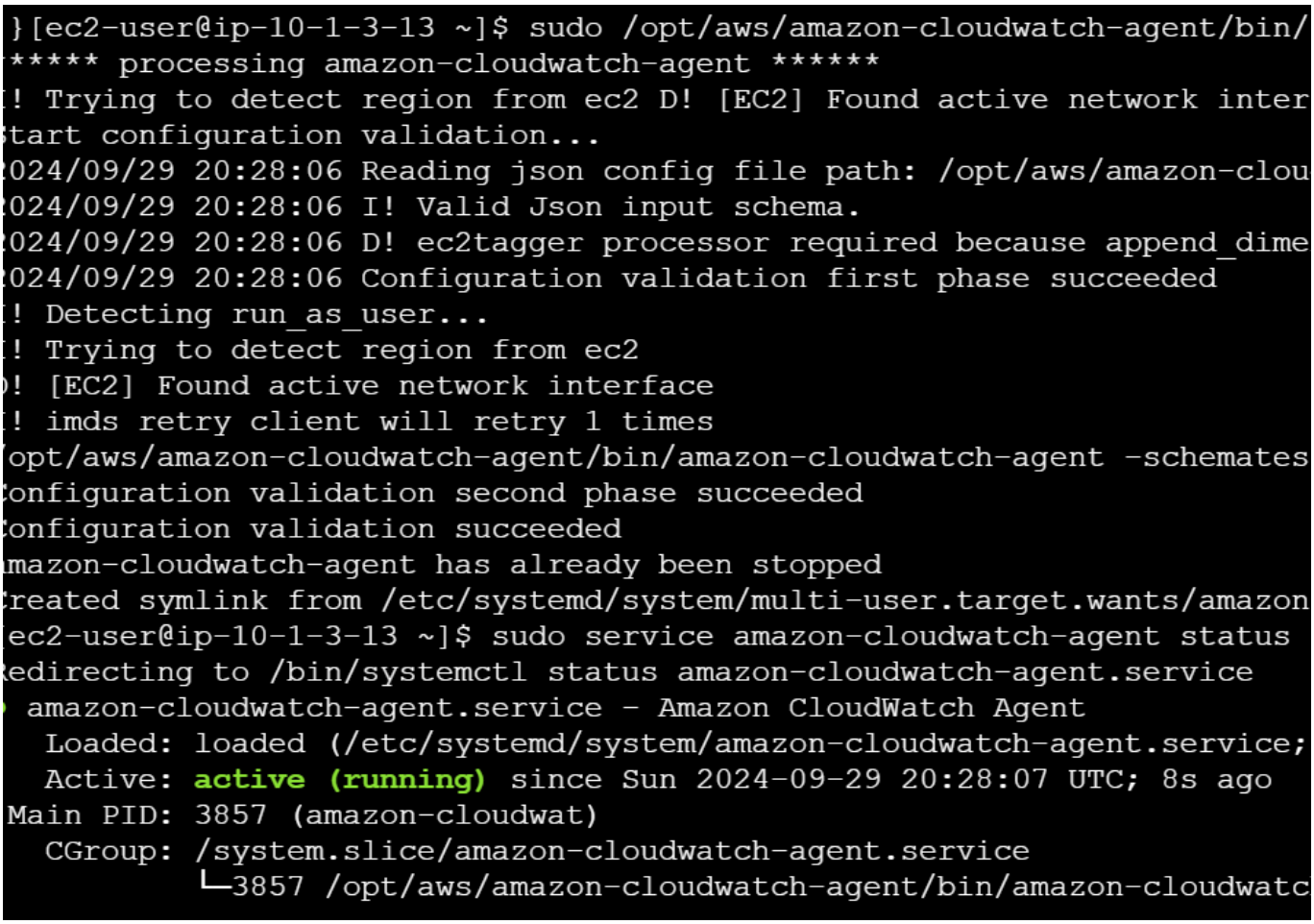


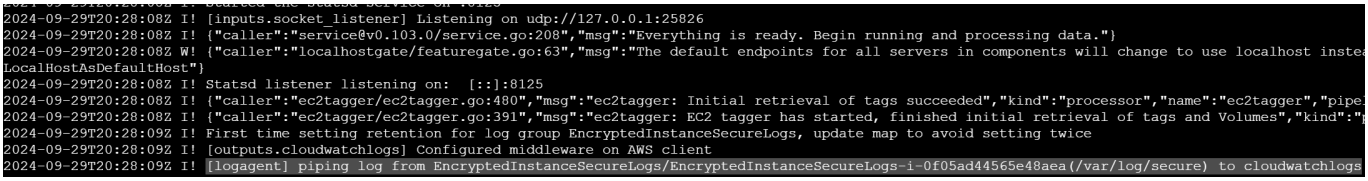

Successfully created Athena table: cloudtrail_logs_cloudtrail_logs_01f5a3e8ab0aef64d
To view this table and run a query, open the Amazon Athena console. Athena charges for running queries. Learn more
CloudTrail > Event history
Query 6
Query 5
Query 7
1 SELECT eventtime, useridentity.principalid, requestparameters, eventname
2 FROM cloudtrail_logs_cloudtrail_logs_01f5a3e8ab0aef64d
3 WHERE
4 eventname in ('PutObject') AND
5 requestparameters LIKE '%customer-data.csv%'
6 limit 10;
SQL Ln 6, Col 10
Run again
Explain
Cancel
Clear
Create
Query results
Query stats
Completed
Results (1)
Search rows
eventtime principalid requestparameters
1 2024-09-29T19:45:06Z AROAXRL2Q2ZCLGCVVCB33:user3535650=Pedro_Coelho_Duarte_Ribeiro {"X-Amz-Date":"20240929T194505Z","bucketName":"data-bucket-0



Task 4.2: Use CloudWatch Logs to monitor secure logs


CloudWatch
Log groups
Log groups (1/4)
By default, we only load up to 10000 log groups.
Filter log groups or try prefix search
Log group
/aws/lambda/c131607a3337212l7762512t1-AdjustA...
/aws/lambda/c131607a3337212l7762512t1-AdjustB...
EncryptedInstanceSecureLogs
LabVPCFlowLogs


}[ec2-user@ip-10-1-3-13 ~]$ sudo /opt/aws/amazon-cloudwatch-agent/bin/
***** processing amazon-cloudwatch-agent ******
! Trying to detect region from ec2 D! [EC2] Found active network inter
tart configuration validation...
024/09/29 20:28:06 Reading json config file path: /opt/aws/amazon-clou
024/09/29 20:28:06 I! Valid Json input schema.
024/09/29 20:28:06 D! ec2tagger processor required because append_dime
024/09/29 20:28:06 Configuration validation first phase succeeded
! Detecting run_as_user...
! Trying to detect region from ec2
! [EC2] Found active network interface
! imds retry client will retry 1 times
opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -schemates
onfiguration validation second phase succeeded
onfiguration validation succeeded
mazon-cloudwatch-agent has already been stopped
reated symlink from /etc/systemd/system/multi-user.target.wants/amazon
ec2-user@ip-10-1-3-13 ~]$ sudo service amazon-cloudwatch-agent status
edirecting to /bin/systemctl status amazon-cloudwatch-agent.service
amazon-cloudwatch-agent.service - Amazon CloudWatch Agent
Loaded: loaded (/etc/systemd/system/amazon-cloudwatch-agent.service;
Active: active (running) since Sun 2024-09-29 20:28:07 UTC; 8s ago
Main PID: 3857 (amazon-cloudwat)
CGroup: /system.slice/amazon-cloudwatch-agent.service
└3857 /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatc

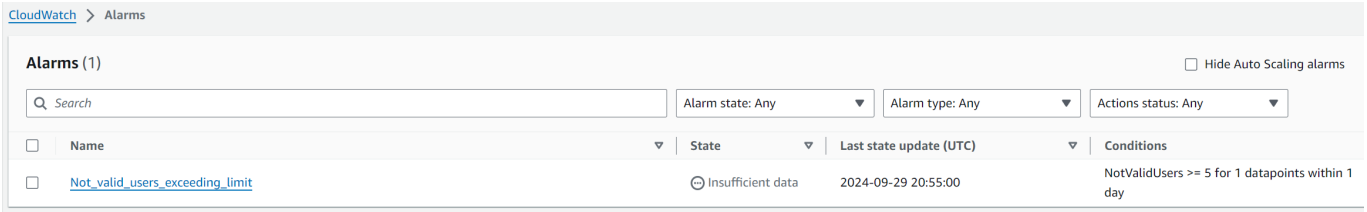

2024-09-29T20:28:08Z I! [inputs.socket_listener] Listening on udp://127.0.0.1:25826
2024-09-29T20:28:08Z I! {"caller":"service@v0.103.0/service.go:208","msg":"Everything is ready. Begin running and processing data."}
2024-09-29T20:28:08Z W! {"caller":"localhostgate/featuregate.go:63","msg":"The default endpoints for all servers in components will change to use localhost inste
LocalHostAsDefaultHost"}
2024-09-29T20:28:08Z I! Statsd listener listening on: [::]:8125
2024-09-29T20:28:08Z I! {"caller":"ec2tagger/ec2tagger.go:480","msg":"ec2tagger: Initial retrieval of tags succeeded","kind":"processor","name":"ec2tagger","pipe
2024-09-29T20:28:08Z I! {"caller":"ec2tagger/ec2tagger.go:391","msg":"ec2tagger: EC2 tagger has started, finished initial retrieval of tags and Volumes","kind":"
2024-09-29T20:28:09Z I! First time setting retention for log group EncryptedInstanceSecureLogs, update map to avoid setting twice
2024-09-29T20:28:09Z I! [outputs.cloudwatchlogs] Configured middleware on AWS client
2024-09-29T20:28:09Z I! [logagent] piping log from EncryptedInstanceSecureLogs/EncryptedInstanceSecureLogs-i-0f05ad44565e48aea(/var/log/secure) to cloudwatchlogs

```
voclabs:~/environment $ ssh -i labsuser.pem ec2-user@54.224.234.4
The authenticity of host '54.224.234.4 (54.224.234.4)' can't be established.
ECDSA key fingerprint is SHA256:HacgM1xwBjF7bhBli+X85NX1IP0N91V7yx2nLvZddyQ.
ECDSA key fingerprint is MD5:c9:29:8e:75:b5:ff:0f:b5:d9:39:06:bf:7c:f3:f0:4f.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '54.224.234.4' (ECDSA) to the list of known hosts.
Last login: Sun Sep 29 20:24:41 2024 from ec2-18-206-107-29.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-10-1-3-13 ~]$ exit
logout
Connection to 54.224.234.4 closed.
voclabs:~/environment $ ssh -i labsuser.pem ubuntu@54.224.234.4
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
```

▶	2024-09-29T20:40:43.025Z	Sep 29 20:39:56 ip-10-1-3-13 sshd[3910]: pam_unix(sshd:session): session opened for user ec2-user by (uid=0)
▶	2024-09-29T20:40:43.025Z	Sep 29 20:40:42 ip-10-1-3-13 sshd[4101]: Received disconnect from 35.172.187.250 port 51240:11: disconnected by user
▶	2024-09-29T20:40:43.025Z	Sep 29 20:40:42 ip-10-1-3-13 sshd[4101]: Disconnected from 35.172.187.250 port 51240
▶	2024-09-29T20:40:47.158Z	Sep 29 20:40:42 ip-10-1-3-13 sshd[3910]: pam_unix(sshd:session): session closed for user ec2-user
▶	2024-09-29T20:41:09.838Z	Sep 29 20:41:09 ip-10-1-3-13 sshd[4133]: Invalid user ubuntu from 35.172.187.250 port 56392
▶	2024-09-29T20:41:09.838Z	Sep 29 20:41:09 ip-10-1-3-13 sshd[4133]: input_userauth_request: invalid user ubuntu [preauth]
▶	2024-09-29T20:41:14.158Z	Sep 29 20:41:09 ip-10-1-3-13 sshd[4133]: Connection closed by 35.172.187.250 port 56392 [preauth]

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



Simple Notification Service

Subscription confirmed!

You have successfully subscribed.

Your subscription's id is:
arn:aws:sns:us-east-1:518337386052:Not_valid_users_exceeding_limit:4e2a5b8e-c3e9-4ec0-93a1-dd16d8e96036

If it was not your intention to subscribe, click here to unsubscribe.

CloudWatch > Log groups > EncryptedInstanceSecureLogs > EncryptedInstanceSecureLogs-i-0f05ad44565e48aea

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

Invalid user

Timestamp	Message
2024-09-29T20:41:09.838Z	Sep 29 20:41:09 ip-10-1-3-13 sshd[4133]: Invalid user ubuntu from 35.172.187.250 port 56392
2024-09-29T20:56:19.898Z	Sep 29 20:56:19 ip-10-1-3-13 sshd[4211]: Invalid user ubuntu from 35.172.187.250 port 36266
2024-09-29T20:56:21.152Z	Sep 29 20:56:20 ip-10-1-3-13 sshd[4213]: Invalid user ubuntu from 35.172.187.250 port 36280
2024-09-29T20:56:21.903Z	Sep 29 20:56:21 ip-10-1-3-13 sshd[4215]: Invalid user ubuntu from 35.172.187.250 port 36290
2024-09-29T20:56:22.906Z	Sep 29 20:56:22 ip-10-1-3-13 sshd[4217]: Invalid user ubuntu from 35.172.187.250 port 36302
2024-09-29T20:56:23.658Z	Sep 29 20:56:23 ip-10-1-3-13 sshd[4219]: Invalid user ubuntu from 35.172.187.250 port 36318
2024-09-29T20:56:24.408Z	Sep 29 20:56:24 ip-10-1-3-13 sshd[4221]: Invalid user ubuntu from 35.172.187.250 port 36320
2024-09-29T20:56:25.160Z	Sep 29 20:56:25 ip-10-1-3-13 sshd[4223]: Invalid user ubuntu from 35.172.187.250 port 36330
2024-09-29T20:56:26.163Z	Sep 29 20:56:25 ip-10-1-3-13 sshd[4225]: Invalid user ubuntu from 35.172.187.250 port 56492

Alarms (1)

Search

Alarm state: In alarm

Name	State
Not_valid_users_exceeding_limit	In alarm

AWS Notifications <no-reply@sns.amazonaws.com>
to me

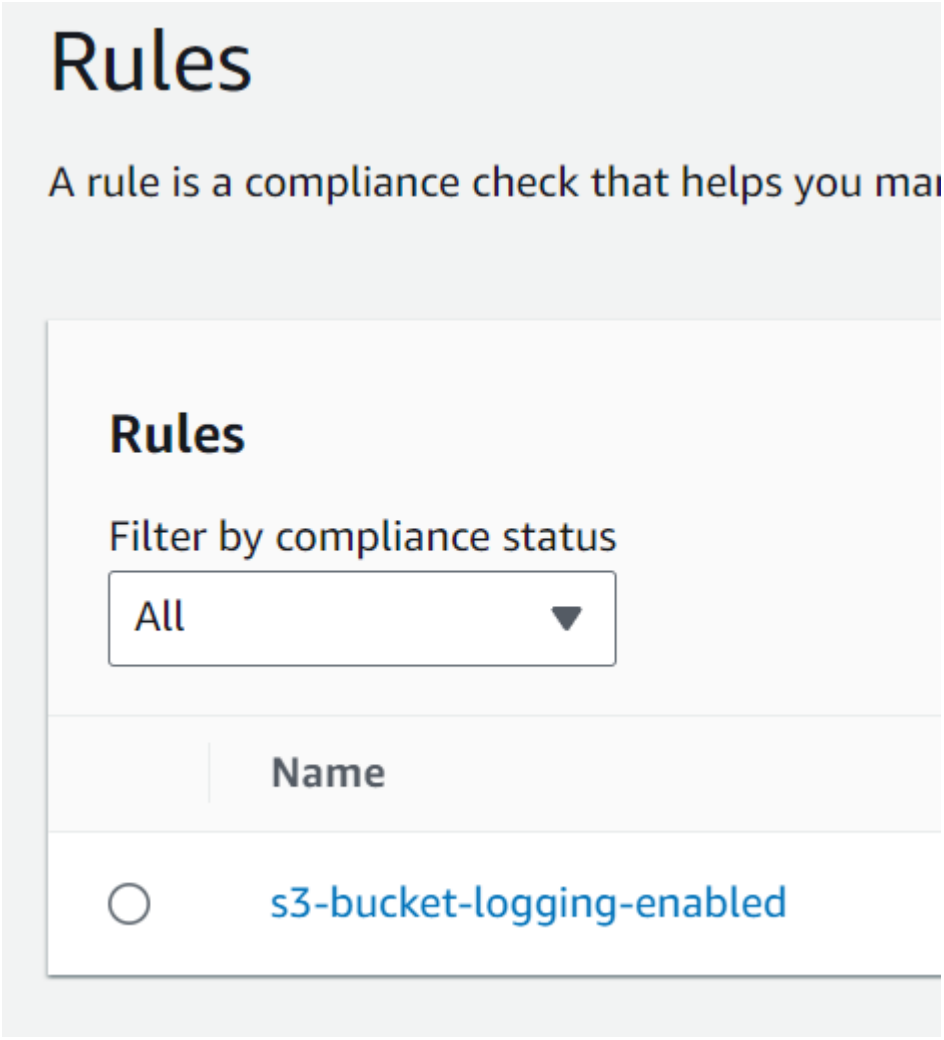
You are receiving this email because your Amazon CloudWatch Alarm "Not_valid_users_exceeding_limit" in the US East (N. Virginia) regi
29 September, 2024 20:57:06 UTC".

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_valid_users_exceeding_limit

Alarm Details:
- Name: Not_valid_users_exceeding_limit
- Description: Not valid access attempts over SSH to the EncryptedInstance server have exceeded 4 in the last 24 hours.
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [8.0 (28/09/24 20:57:00)] was greater than or equal to the
- Timestamp: Sunday 29 September, 2024 20:57:06 UTC
- AWS Account: 518337386052
- Alarm Arn: arn:aws:cloudwatch:us-east-1:518337386052:alarm:Not_valid_users_exceeding_limit

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

	Name ▲	AWS Region
○	athena-results-666	US East (N. Virginia) us-east-1
○	aws-athena-query-results-518337386052-us-east-1	US East (N. Virginia) us-east-1
○	aws-config-01f5a3e8ab0aef64d	US East (N. Virginia) us-east-1
○	cloudtrail-logs-01f5a3e8ab0aef64d	US East (N. Virginia) us-east-1
◉	compliance-bucket-01f5a3e8ab0aef64d	US East (N. Virginia) us-east-1
○	data-bucket-01f5a3e8ab0aef64d	US East (N. Virginia) us-east-1
○	s3-inventory-01f5a3e8ab0aef64d	US East (N. Virginia) us-east-1
○	s3-objects-access-log-01f5a3e8ab0aef64d	US East (N. Virginia) us-east-1



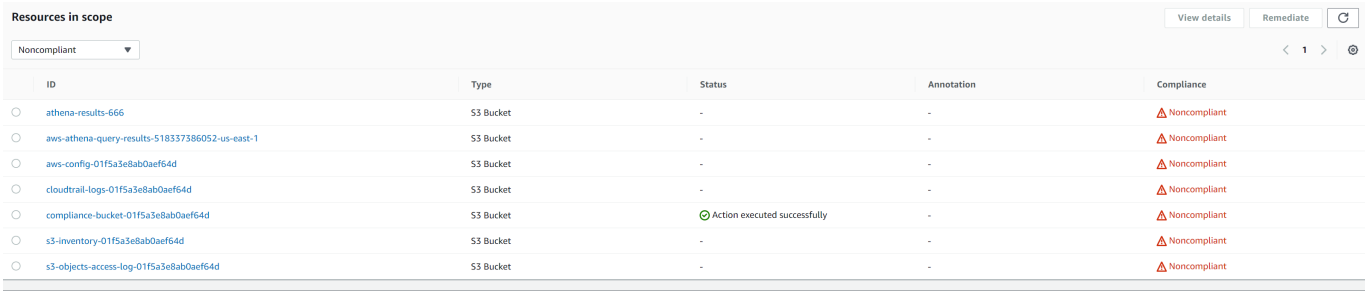
Remediation action

Remediation action
AWS-ConfigureS3BucketLogging

Description
Enables Logging on S3 Bucket

Parameters

Key	Value	Description
AutomationAssumeRole	arn:aws:iam::518337386052: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	d4bdae1ddc96f96d97d09f060f24770b6db937ed9ae76b810e47402ab7537738	(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-01f5a3e8ab0aef64d	(Required) Specifies the bucket where you want Amazon S3 to store server access logs. You can have
TargetObjectKeyPrefix	-	(Optional) Amazon S3 key format for log objects.

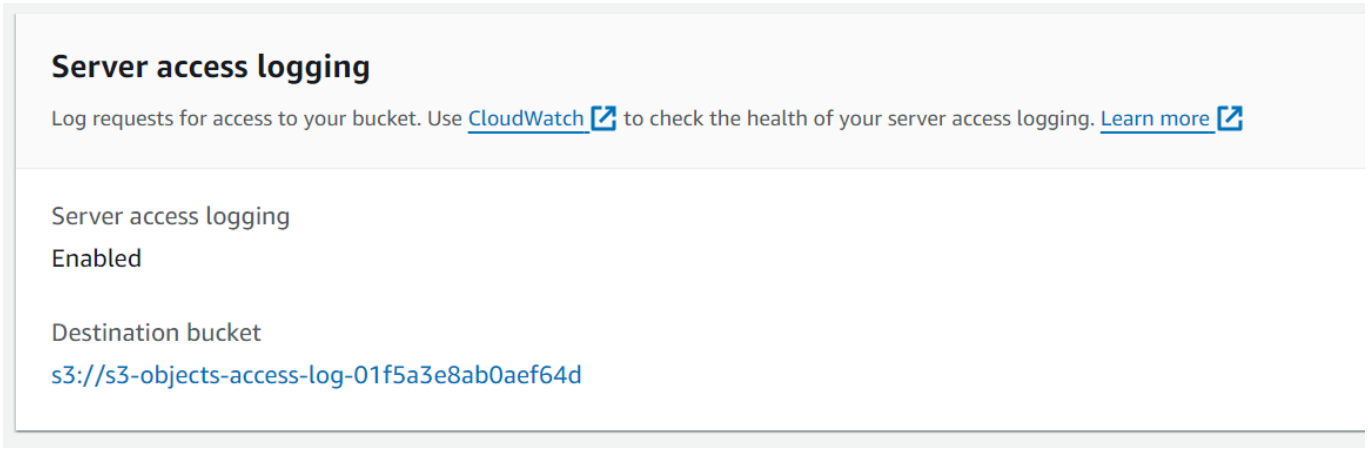


Resources in scope

View details | Remediate

Noncompliant

ID	Type	Status	Annotation	Compliance
athena-results-666	S3 Bucket	-	-	Noncompliant
aws-athena-query-results-518337386052-us-east-1	S3 Bucket	-	-	Noncompliant
aws-config-01f5a3e8ab0aef64d	S3 Bucket	-	-	Noncompliant
cloudtrail-logs-01f5a3e8ab0aef64d	S3 Bucket	-	-	Noncompliant
compliance-bucket-01f5a3e8ab0aef64d	S3 Bucket	Action executed successfully	-	Noncompliant
s3-inventory-01f5a3e8ab0aef64d	S3 Bucket	-	-	Noncompliant
s3-objects-access-log-01f5a3e8ab0aef64d	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-01f5a3e8ab0aef64d