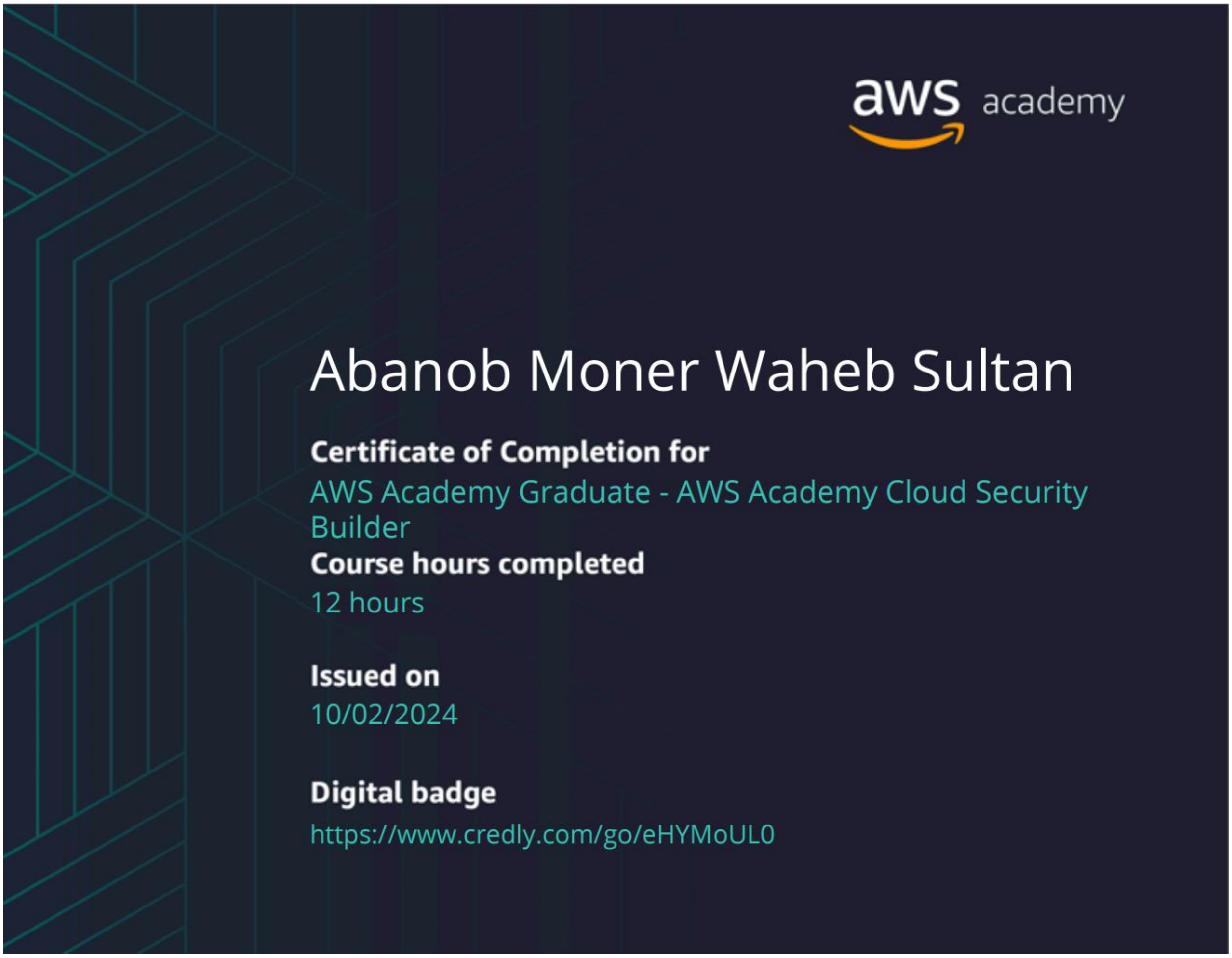
Cloud Security Builder Project



aws academy

Abanob Moner Waheb Sultan

Certificate of Completion for

AWS Academy Graduate - AWS Academy Cloud Security Builder

Course hours completed

12 hours

Issued on

10/02/2024

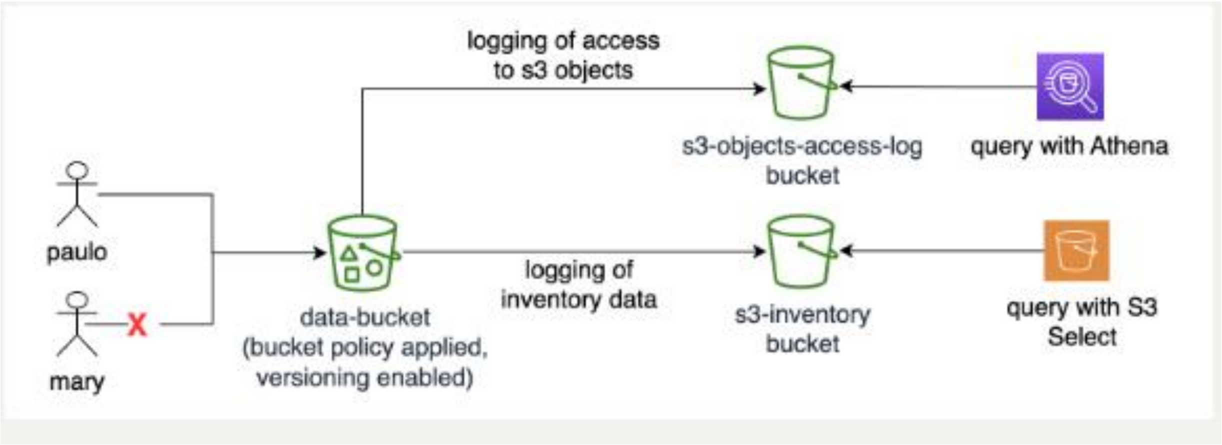
Digital badge

https://www.credly.com/go/eHYMoUL0

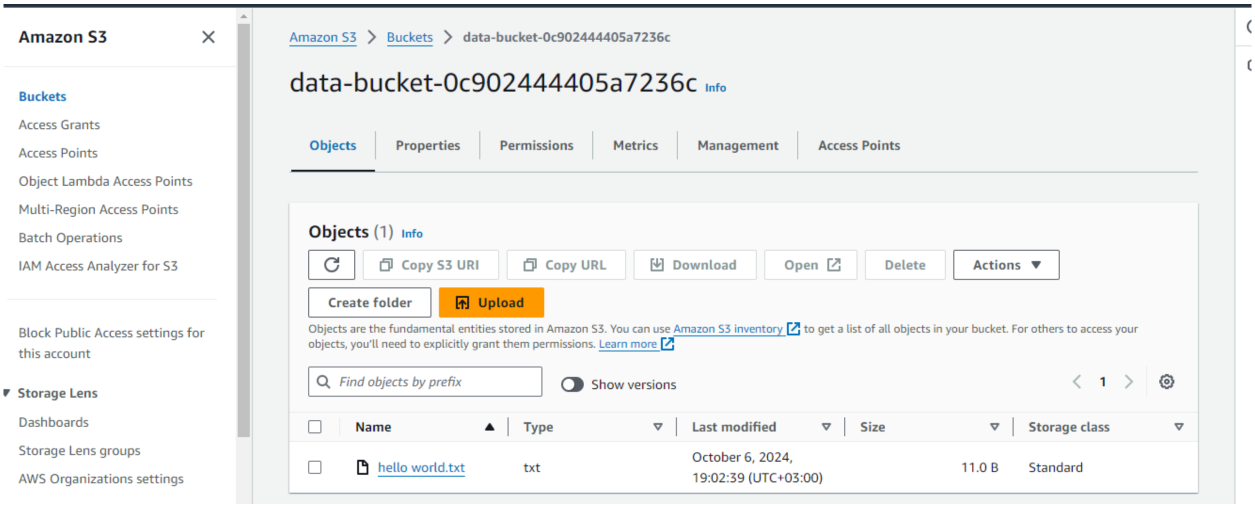
Project Overview

In this project, we’re challenged to use familiar AWS services, as well as AWS services, to create resources in AWS and to implement security on them. Throughout various AWS Academy courses, we have completed hands-on labs. We have used different AWS services and features to build a variety of solutions.

<u>Phase 1: Securing data in Amazon S3</u>



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

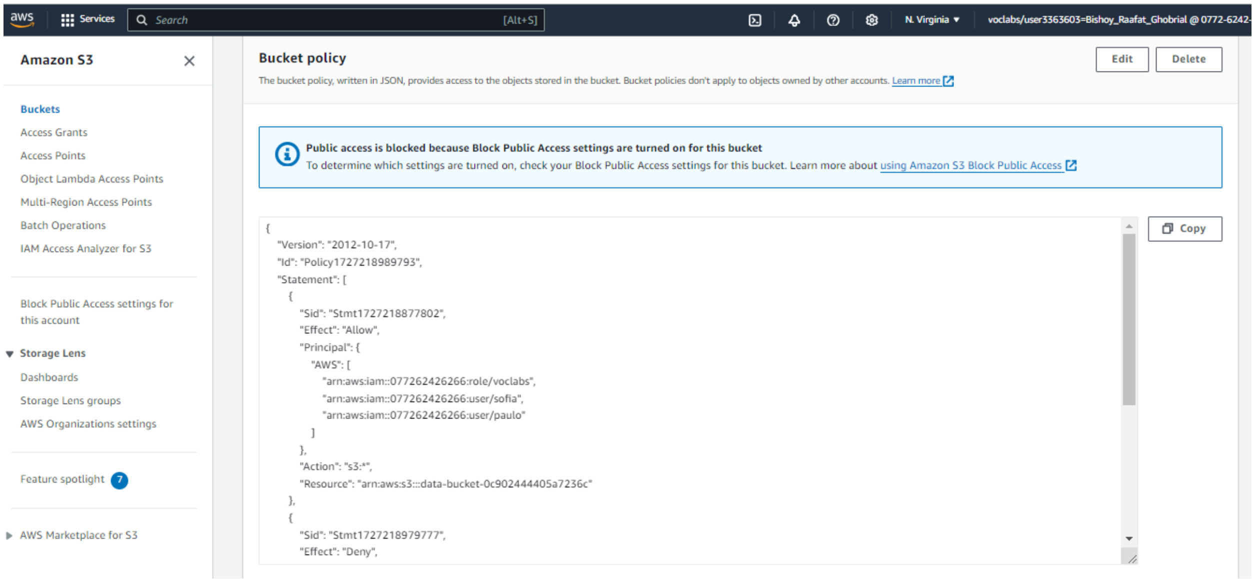


data-bucket-0c902444405a7236c Info

Objects (1) 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

	Name	Type	Last modified	Size	Storage class
□	hello world.txt	txt	October 6, 2024, 19:02:39 (UTC+03:00)	11.0 B	Standard


aws
Services
Search [Alt+S]
N. Virginia
voclabs/user3363603=Bishoy_Raafat_Ghobrial @ 0772-6242-
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight 7
AWS Marketplace for S3
Edit
Delete
Copy

Bucket policy

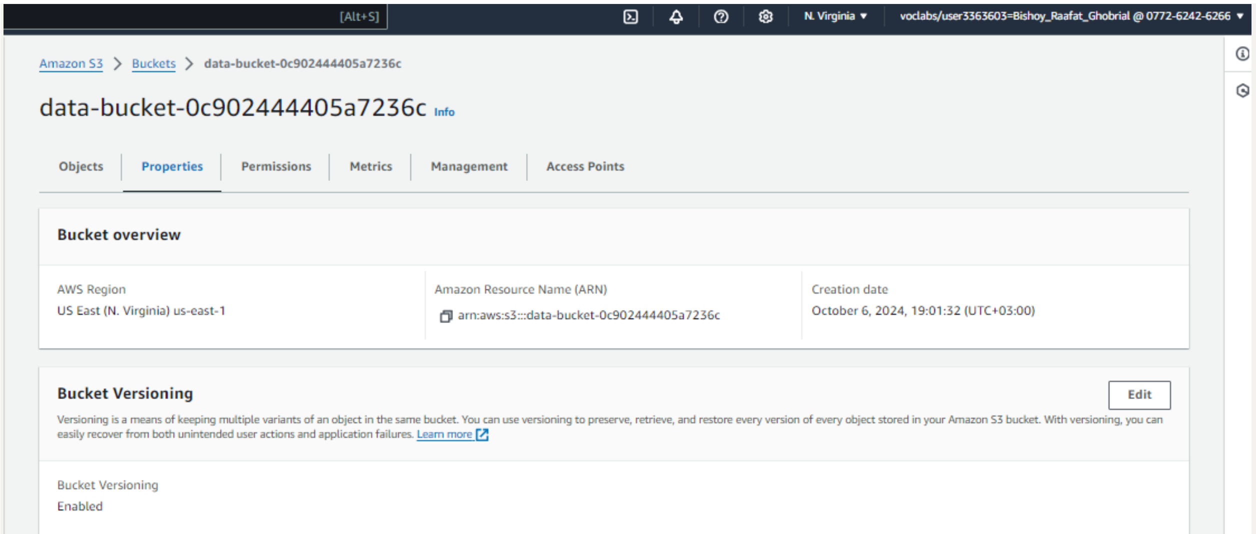
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

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

```
{
  "Version": "2012-10-17",
  "Id": "Policy1727218989793",
  "Statement": [
    {
      "Sid": "Stmt1727218877802",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::077262426266:role/voclabs",
          "arn:aws:iam::077262426266:user/sofia",
          "arn:aws:iam::077262426266:user/paulo"
        ]
      },
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::data-bucket-0c902444405a7236c"
    },
    {
      "Sid": "Stmt1727218979777",
      "Effect": "Deny",
```

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


[Alt+S]
N. Virginia
voclabs/user3363603=Bishoy_Raafat_Ghobrial @ 0772-6242-6266
Amazon S3 > Buckets > data-bucket-0c902444405a7236c
Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Edit

data-bucket-0c902444405a7236c

Bucket overview

AWS Region: US East (N. Virginia) us-east-1

Amazon Resource Name (ARN): arn:aws:s3:::data-bucket-0c902444405a7236c

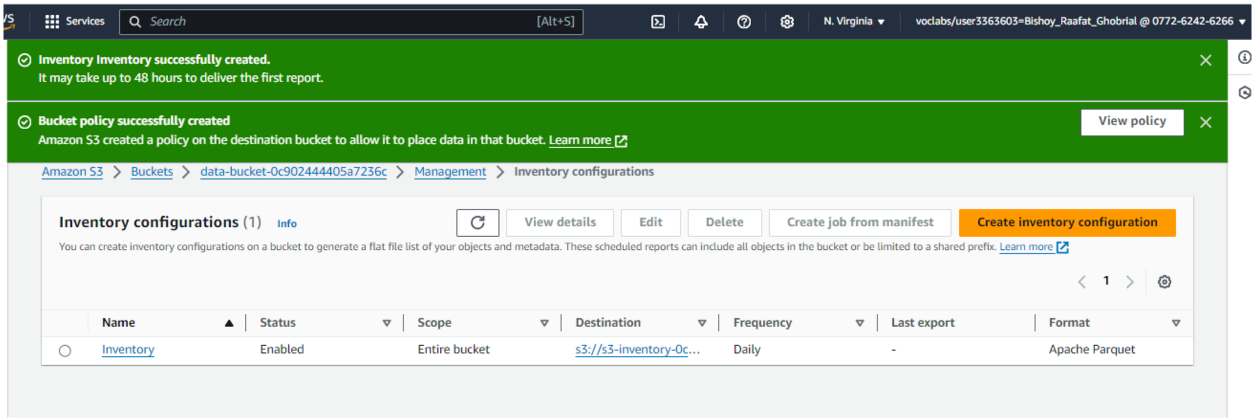
Creation date: October 6, 2024, 19:01:32 (UTC+03:00)

Bucket Versioning

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

Task 1.3: Implement the S3 Inventory feature on a bucket


Services
Search
[Alt+S]
N. Virginia
voclabs/user3363603=Bishoy_Raafat_Ghobrial @ 0772-6242-6266
View policy
Amazon S3 > Buckets > data-bucket-0c902444405a7236c > Management > Inventory configurations
View details
Edit
Delete
Create job from manifest
Create inventory configuration

Inventory Inventory successfully created.
It may take up to 48 hours to deliver the first report.

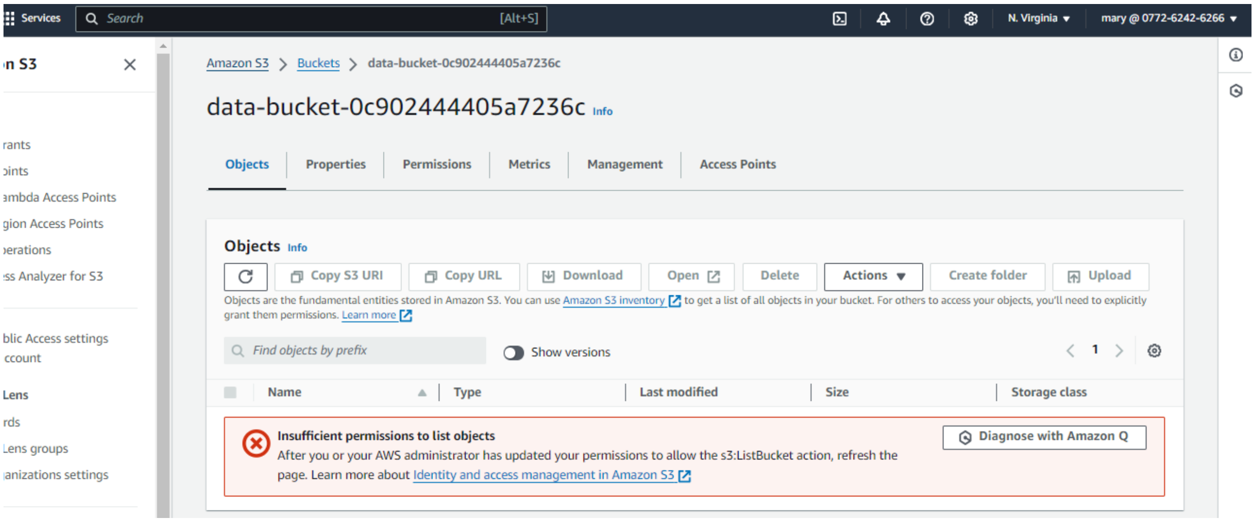
Bucket policy successfully created
Amazon S3 created a policy on the destination bucket to allow it to place data in that bucket. Learn more

Inventory configurations (1) Info

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-0c...	Daily	-	Apache Parquet

Task 1.4: Confirm that versioning works as intended



data-bucket-0c902444405a7236c Info

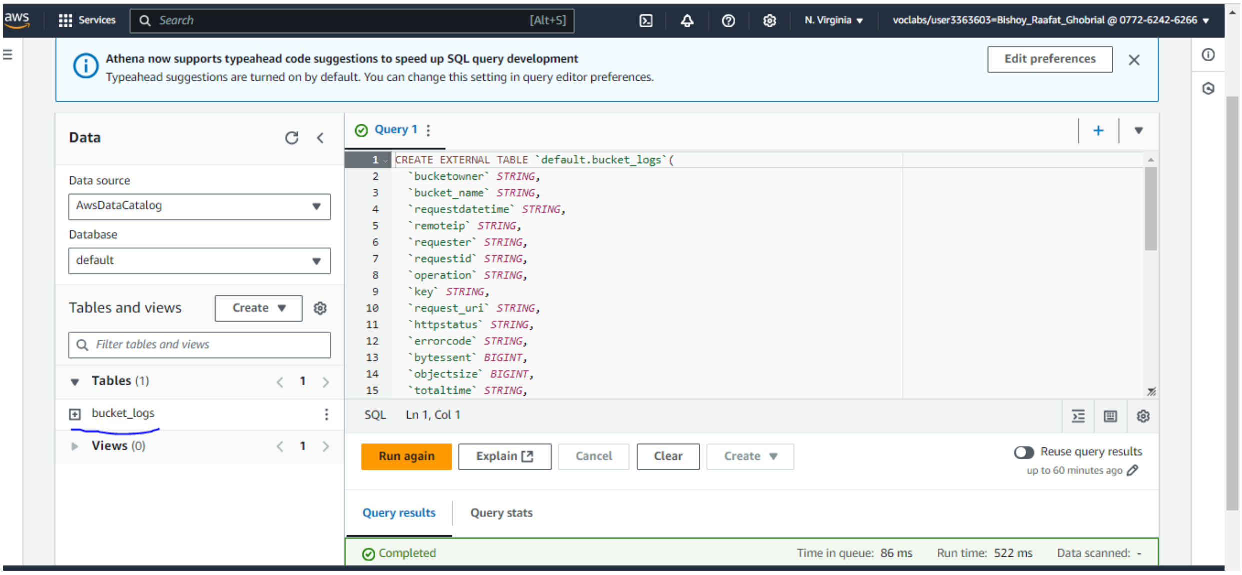
Objects Info

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

Name	Type	Last modified	Size	Storage class

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



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.

Data source: AwsDataCatalog

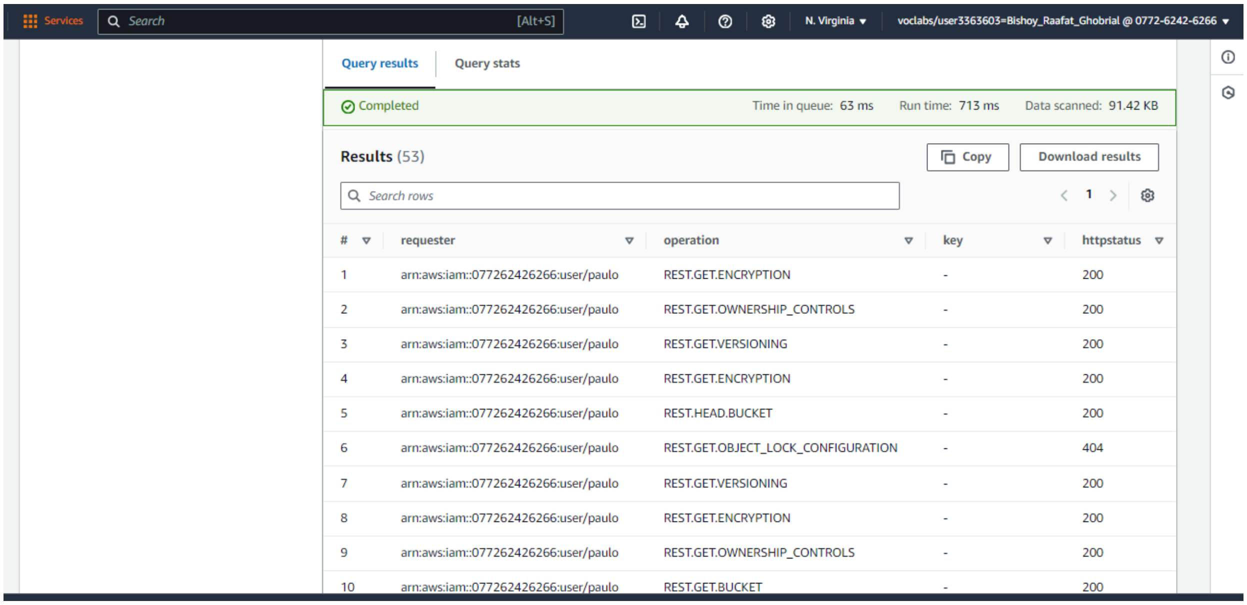
Database: default

```
CREATE EXTERNAL TABLE `default.bucket_logs`(
  `bucketowner` STRING,
  `bucket_name` STRING,
  `requestdatetime` STRING,
  `remoteip` STRING,
  `requester` STRING,
  `requestid` STRING,
  `operation` STRING,
  `key` STRING,
  `request_uri` STRING,
  `httpstatus` STRING,
  `errorcode` STRING,
  `bytessent` BIGINT,
  `objectsize` BIGINT,
  `totaltime` STRING,
```

SQL Ln 1, Col 1

Reuse query results up to 60 minutes ago

Completed Time in queue: 86 ms Run time: 522 ms Data scanned: -

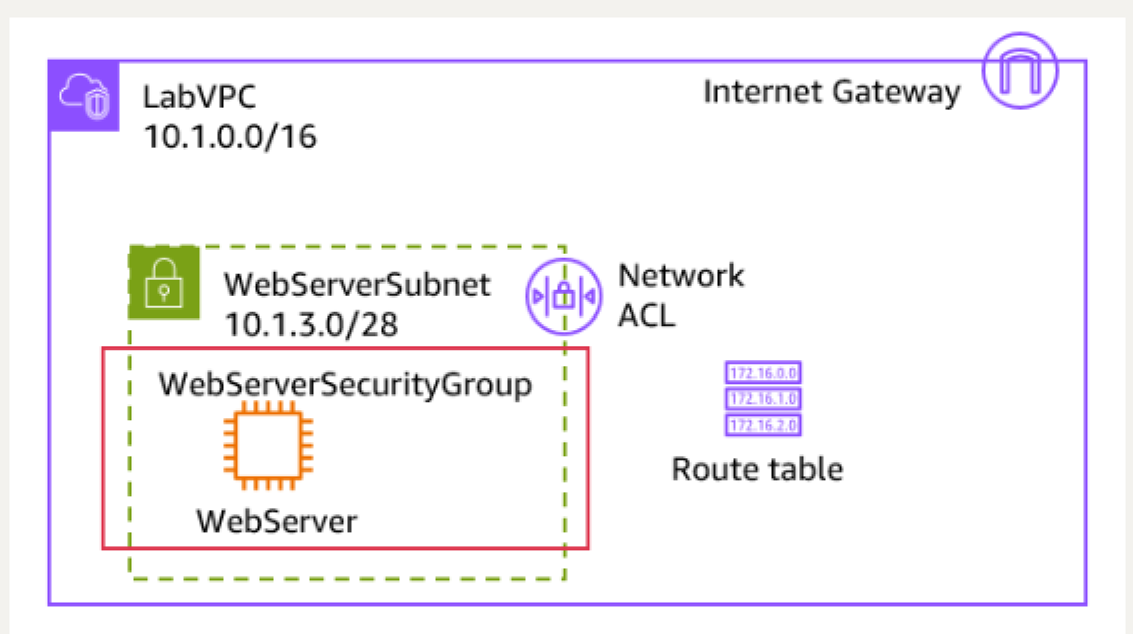


Completed Time in queue: 63 ms Run time: 713 ms Data scanned: 91.42 KB

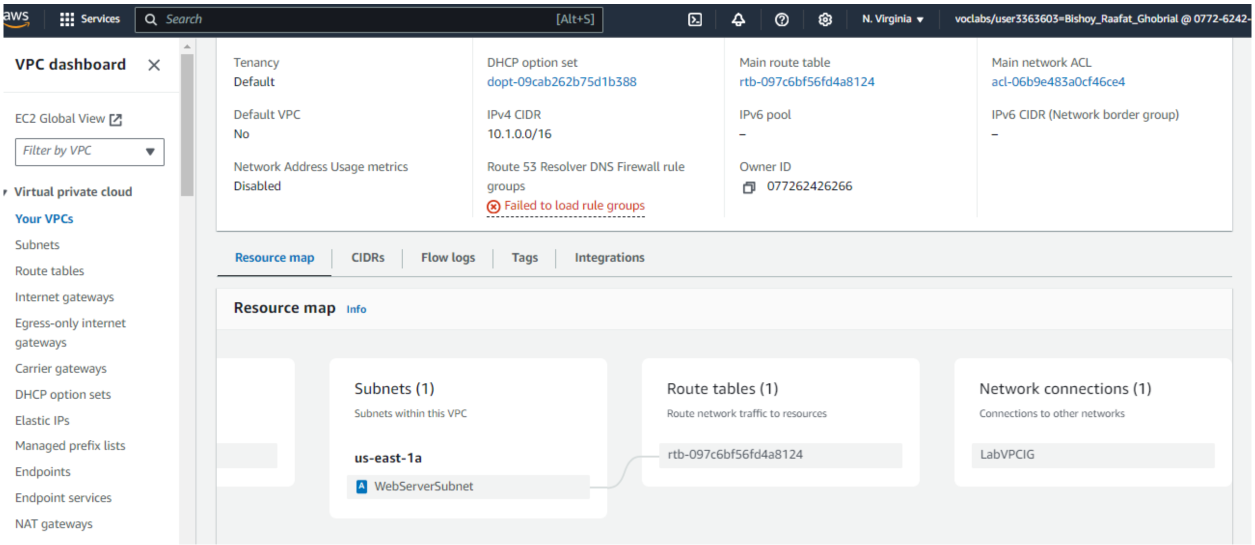
Results (53)

#	requester	operation	key	httpstatus
1	arn:aws:iam::077262426266:user/paulo	REST.GET.ENCRYPTION	-	200
2	arn:aws:iam::077262426266:user/paulo	REST.GET.OWNERSHIP_CONTROLS	-	200
3	arn:aws:iam::077262426266:user/paulo	REST.GET.VERSIONING	-	200
4	arn:aws:iam::077262426266:user/paulo	REST.GET.ENCRYPTION	-	200
5	arn:aws:iam::077262426266:user/paulo	REST.HEAD.BUCKET	-	200
6	arn:aws:iam::077262426266:user/paulo	REST.GET.OBJECT_LOCK_CONFIGURATION	-	404
7	arn:aws:iam::077262426266:user/paulo	REST.GET.VERSIONING	-	200
8	arn:aws:iam::077262426266:user/paulo	REST.GET.ENCRYPTION	-	200
9	arn:aws:iam::077262426266:user/paulo	REST.GET.OWNERSHIP_CONTROLS	-	200
10	arn:aws:iam::077262426266:user/paulo	REST.GET.BUCKET	-	200

Phase 2: Securing VPCs



Task 2.1: Review LabVPC and its associated resources



Tenancy
Default

Default VPC
No

Network Address Usage metrics
Disabled

DHCP option set
dopt-09cab262b75d1b388

IPv4 CIDR
10.1.0.0/16

Route 53 Resolver DNS Firewall rule groups
Failed to load rule groups

Main route table
rtb-097c6bf56fd4a8124

IPv6 pool
–

Owner ID
077262426266

Main network ACL
acl-06b9e483a0cf46ce4

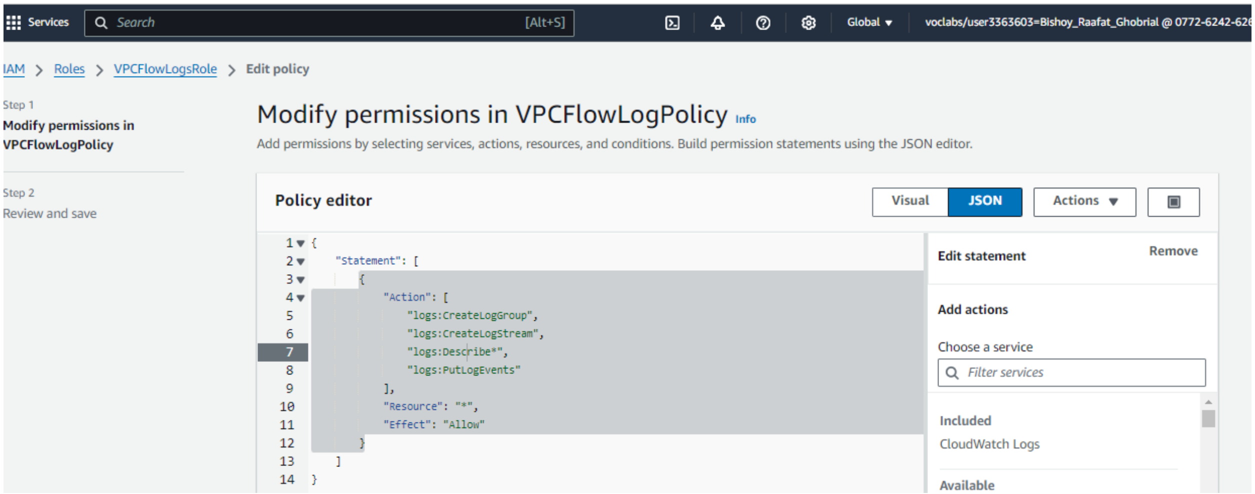
IPv6 CIDR (Network border group)
–

Resource map

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

Route tables (1)
Route network traffic to resources
rtb-097c6bf56fd4a8124

Network connections (1)
Connections to other networks
LabVPCIG



IAM > Roles > VPCFlowLogsRole > Edit policy

Step 1
Modify permissions in VPCFlowLogPolicy

Step 2
Review and save

Modify permissions in VPCFlowLogPolicy Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

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

Edit statement Remove

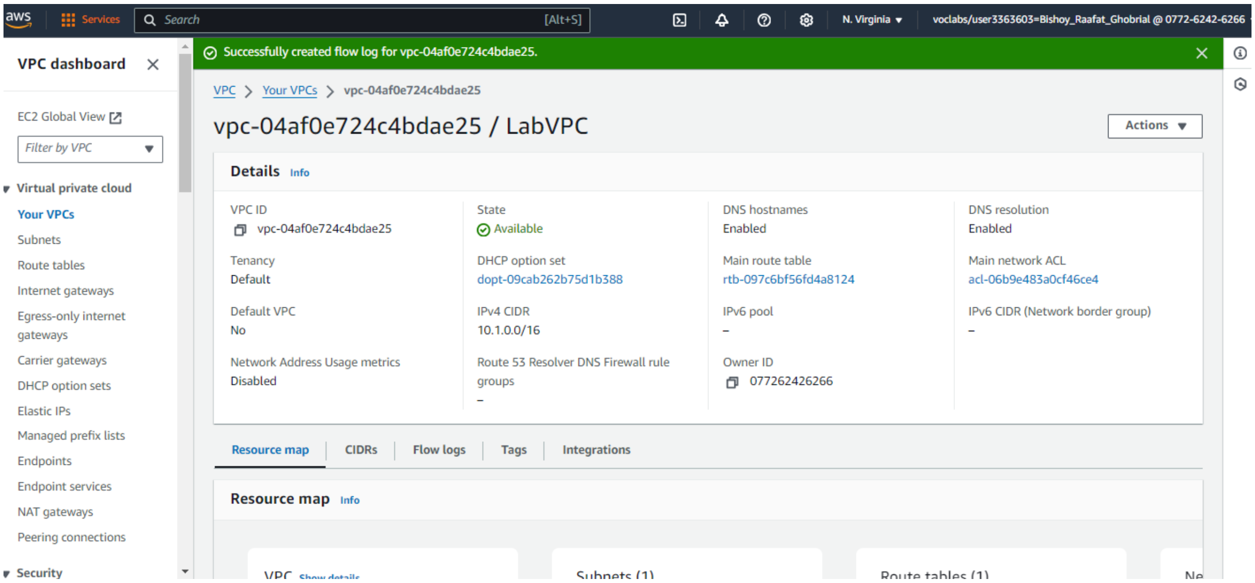
Add actions

Choose a service

Included
CloudWatch Logs

Available

Task 2.2: Create a VPC flow log



Successfully created flow log for vpc-04af0e724c4bdae25.

VPC dashboard

VPC > Your VPCs > vpc-04af0e724c4bdae25

vpc-04af0e724c4bdae25 / LabVPC

Details Info

VPC ID
vpc-04af0e724c4bdae25

State
Available

DNS hostnames
Enabled

DNS resolution
Enabled

Tenancy
Default

DHCP option set
dopt-09cab262b75d1b388

Main route table
rtb-097c6bf56fd4a8124

Main network ACL
acl-06b9e483a0cf46ce4

Default VPC
No

IPv4 CIDR
10.1.0.0/16

IPv6 pool
–

IPv6 CIDR (Network border group)
–

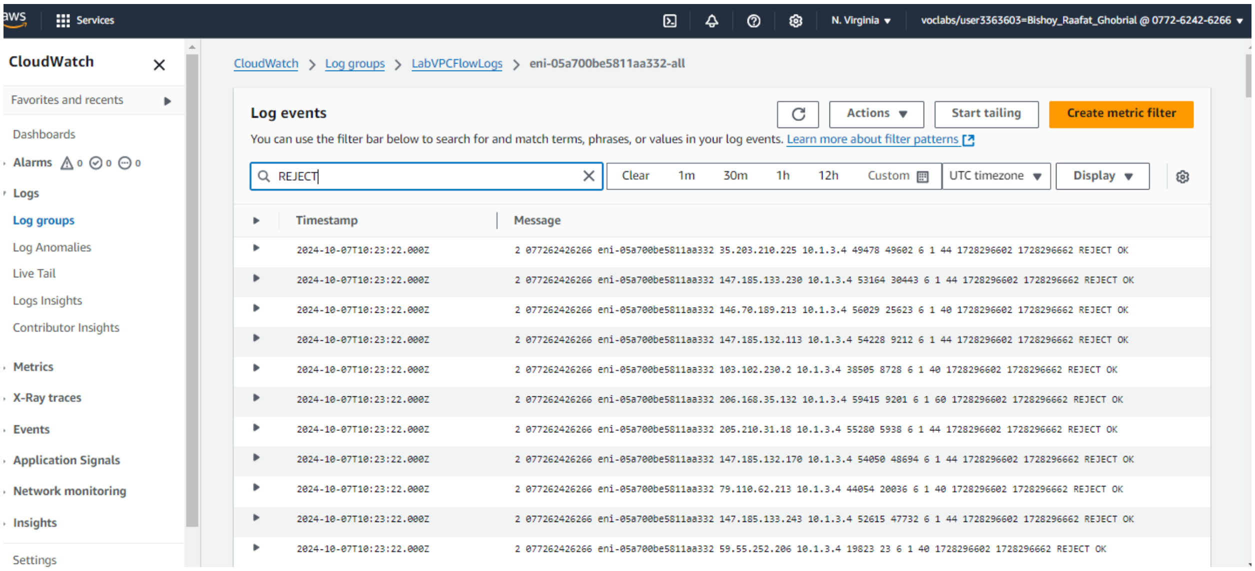
Network Address Usage metrics
Disabled

Route 53 Resolver DNS Firewall rule groups
–

Owner ID
077262426266

Resource map Info

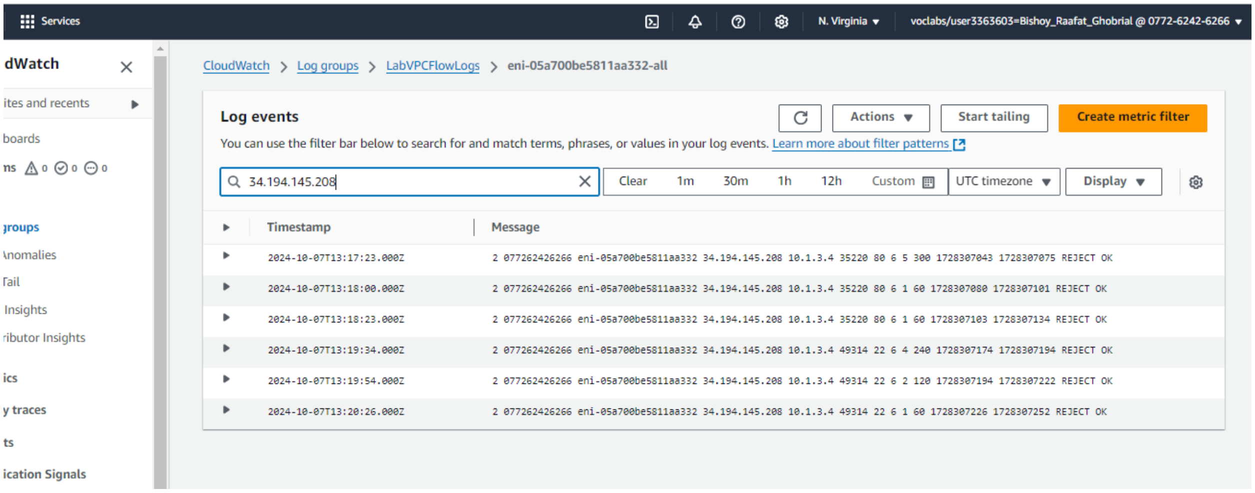
Task 2.3: Access the WebServer instance from the internet and review VPC flow logs in CloudWatch



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
2024-10-07T10:23:22.000Z   2 077262426266 eni-05a700be5811aa332 35.203.210.225 10.1.3.4 49478 49602 6 1 44 1728296602 1728296662 REJECT OK
2024-10-07T10:23:22.000Z   2 077262426266 eni-05a700be5811aa332 147.185.133.230 10.1.3.4 53164 30443 6 1 44 1728296602 1728296662 REJECT OK
2024-10-07T10:23:22.000Z   2 077262426266 eni-05a700be5811aa332 146.70.189.213 10.1.3.4 56029 25623 6 1 40 1728296602 1728296662 REJECT OK
2024-10-07T10:23:22.000Z   2 077262426266 eni-05a700be5811aa332 147.185.132.113 10.1.3.4 54228 9212 6 1 44 1728296602 1728296662 REJECT OK
2024-10-07T10:23:22.000Z   2 077262426266 eni-05a700be5811aa332 103.102.230.2 10.1.3.4 38505 8728 6 1 40 1728296602 1728296662 REJECT OK
2024-10-07T10:23:22.000Z   2 077262426266 eni-05a700be5811aa332 206.168.35.132 10.1.3.4 59415 9201 6 1 60 1728296602 1728296662 REJECT OK
2024-10-07T10:23:22.000Z   2 077262426266 eni-05a700be5811aa332 205.210.31.18 10.1.3.4 55280 5938 6 1 44 1728296602 1728296662 REJECT OK
2024-10-07T10:23:22.000Z   2 077262426266 eni-05a700be5811aa332 147.185.132.170 10.1.3.4 54050 48694 6 1 44 1728296602 1728296662 REJECT OK
2024-10-07T10:23:22.000Z   2 077262426266 eni-05a700be5811aa332 79.110.62.213 10.1.3.4 44054 20036 6 1 40 1728296602 1728296662 REJECT OK
2024-10-07T10:23:22.000Z   2 077262426266 eni-05a700be5811aa332 147.185.133.243 10.1.3.4 52615 47732 6 1 44 1728296602 1728296662 REJECT OK
2024-10-07T10:23:22.000Z   2 077262426266 eni-05a700be5811aa332 59.55.252.206 10.1.3.4 19823 23 6 1 40 1728296602 1728296662 REJECT OK
```

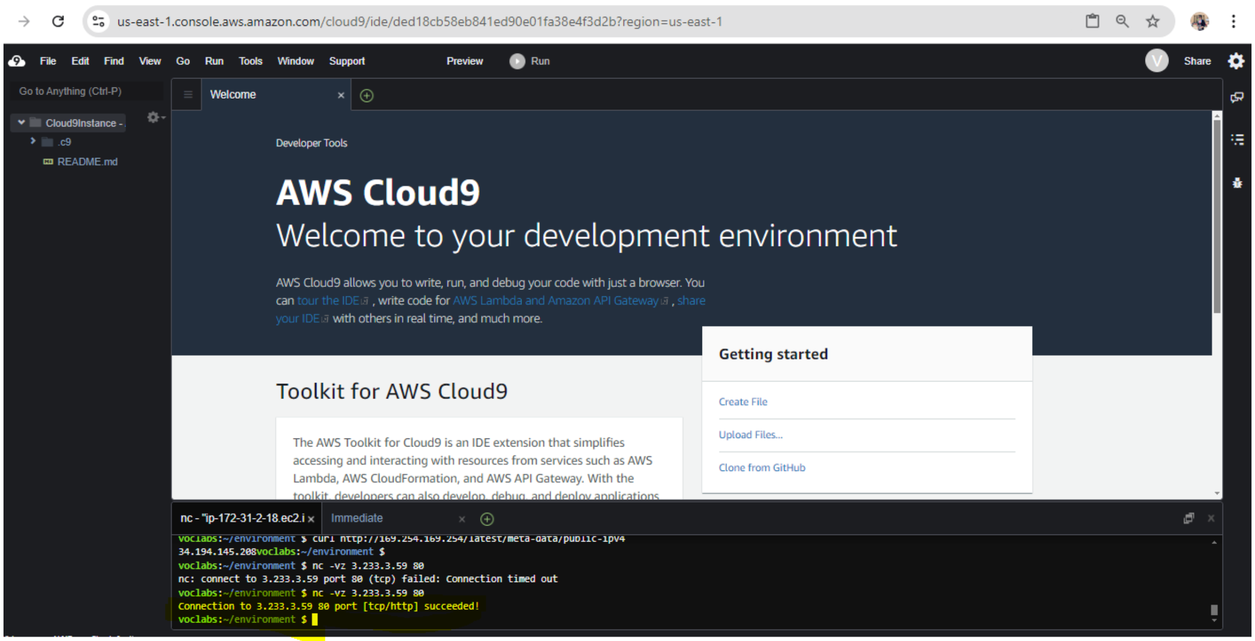


You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns

34.194.145.208

```
Timestamp                  Message
2024-10-07T13:17:23.000Z   2 077262426266 eni-05a700be5811aa332 34.194.145.208 10.1.3.4 35220 80 6 5 300 1728307043 1728307075 REJECT OK
2024-10-07T13:18:00.000Z   2 077262426266 eni-05a700be5811aa332 34.194.145.208 10.1.3.4 35220 80 6 1 60 1728307080 1728307101 REJECT OK
2024-10-07T13:18:23.000Z   2 077262426266 eni-05a700be5811aa332 34.194.145.208 10.1.3.4 35220 80 6 1 60 1728307103 1728307134 REJECT OK
2024-10-07T13:19:34.000Z   2 077262426266 eni-05a700be5811aa332 34.194.145.208 10.1.3.4 49314 22 6 4 240 1728307174 1728307194 REJECT OK
2024-10-07T13:19:54.000Z   2 077262426266 eni-05a700be5811aa332 34.194.145.208 10.1.3.4 49314 22 6 2 120 1728307194 1728307222 REJECT OK
2024-10-07T13:20:26.000Z   2 077262426266 eni-05a700be5811aa332 34.194.145.208 10.1.3.4 49314 22 6 1 60 1728307226 1728307252 REJECT OK
```

Task 2.4: Configure route table and security group settings



Developer Tools

AWS Cloud9

Welcome to your development environment

AWS Cloud9 allows you to write, run, and debug your code with just a browser. You can tour the IDE, write code for AWS Lambda and Amazon API Gateway, share your IDE with others in real time, and much more.

Toolkit for AWS Cloud9

The AWS Toolkit for Cloud9 is an IDE extension that simplifies accessing and interacting with resources from services such as AWS Lambda, AWS CloudFormation, and AWS API Gateway. With the toolkit, developers can also develop, debug, and deploy applications

Getting started

Create File

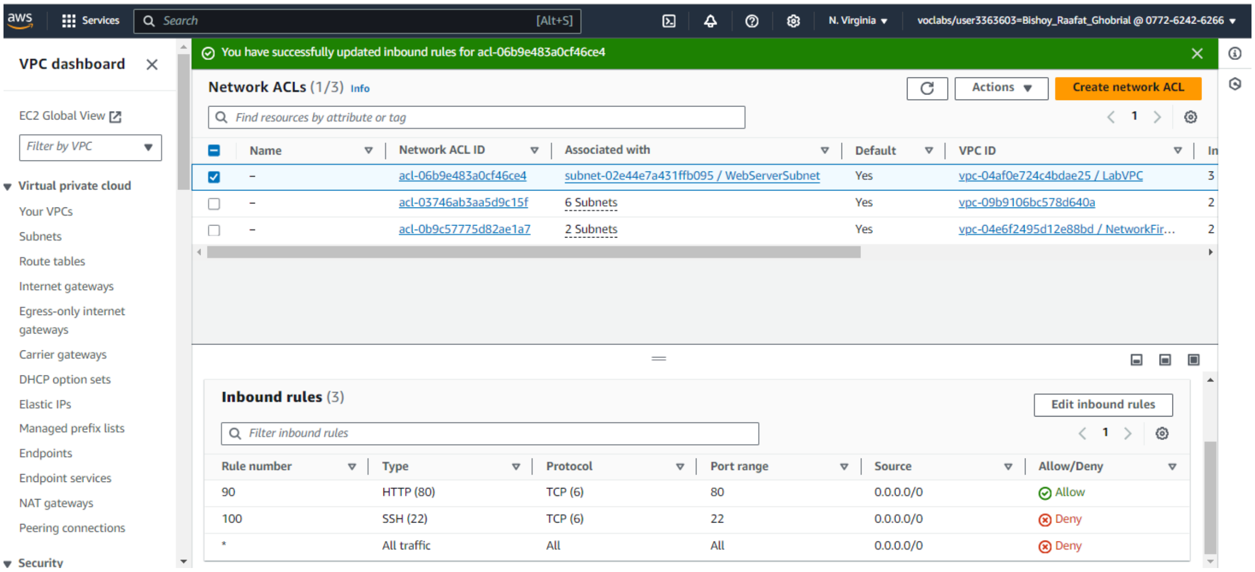
Upload Files...

Clone from GitHub

```
voclabs:~/environment $ curl http://169.254.169.254/latest/meta-data/public-ipv4
34.194.145.208voclabs:~/environment $
voclabs:~/environment $ nc -vz 3.233.3.59 80
nc: connect to 3.233.3.59 port 80 (tcp) failed: Connection timed out
voclabs:~/environment $ nc -vz 3.233.3.59 80
Connection to 3.233.3.59 80 port [tcp/http] succeeded!
voclabs:~/environment $
```

us-east-1.console.aws.amazon.com/cloud9/ide/ded18cb58eb841ed90e01fa38e4f3d2b?region=us-east-1
File Edit Find View Go Run Tools Window Support
Preview
Run
Share
Go to Anything (Ctrl-P)
Welcome
Cloud9Instance -
.c9
README.md
nc - "ip-172-31-2-18.ec2.i
Immediate

Task 2.5: Secure the WebServerSubnet with a network ACL



You have successfully updated inbound rules for acl-06b9e483a0cf46ce4

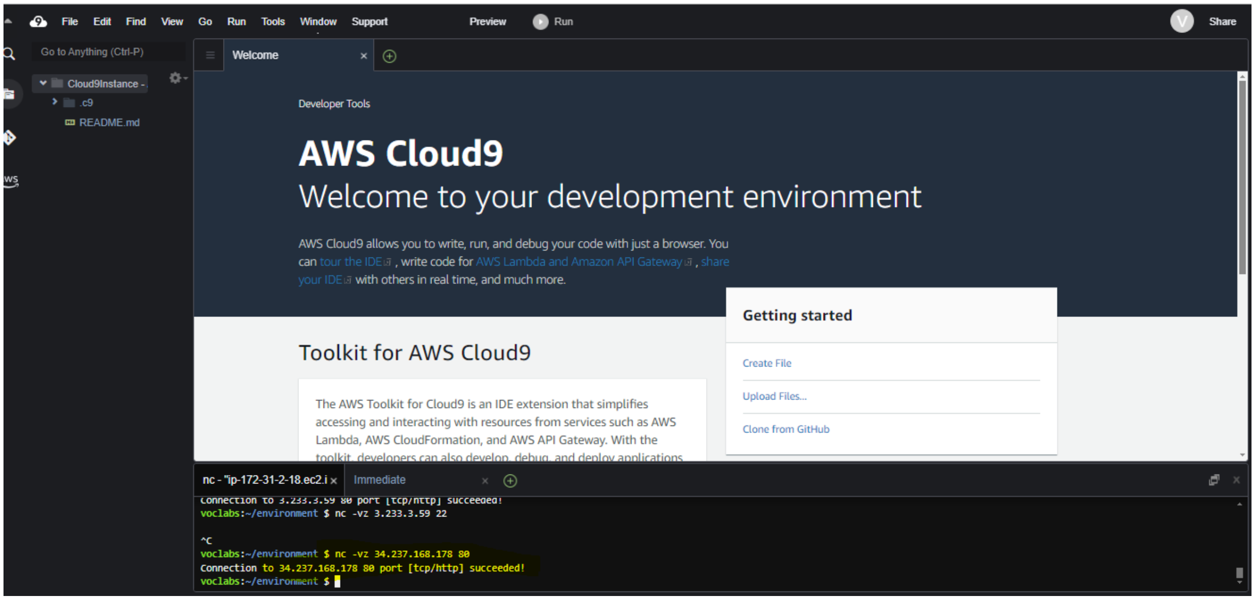
Network ACLs (1/3)

☐	Name	Network ACL ID	Associated with	Default	VPC ID	In
☑	–	acl-06b9e483a0cf46ce4	subnet-02e44e7a431ffb095 / WebServerSubnet	Yes	vpc-04af0e724c4bdae25 / LabVPC	3
☐	–	acl-03746ab3aa5d9c15f	6 Subnets	Yes	vpc-09b9106bc578d640a	2
☐	–	acl-0b9c57775d82ae1a7	2 Subnets	Yes	vpc-04e6f2495d12e88bd / NetworkFir...	2

Inbound rules (3)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
90	HTTP (80)	TCP (6)	80	0.0.0.0/0	✓ Allow
100	SSH (22)	TCP (6)	22	0.0.0.0/0	⊗ Deny
*	All traffic	All	All	0.0.0.0/0	⊗ Deny

Task 2.6: Review NetworkFirewallVPC and its associated resources



Developer Tools

AWS Cloud9

Welcome to your development environment

AWS Cloud9 allows you to write, run, and debug your code with just a browser. You can tour the IDE, write code for AWS Lambda and Amazon API Gateway, share your IDE with others in real time, and much more.

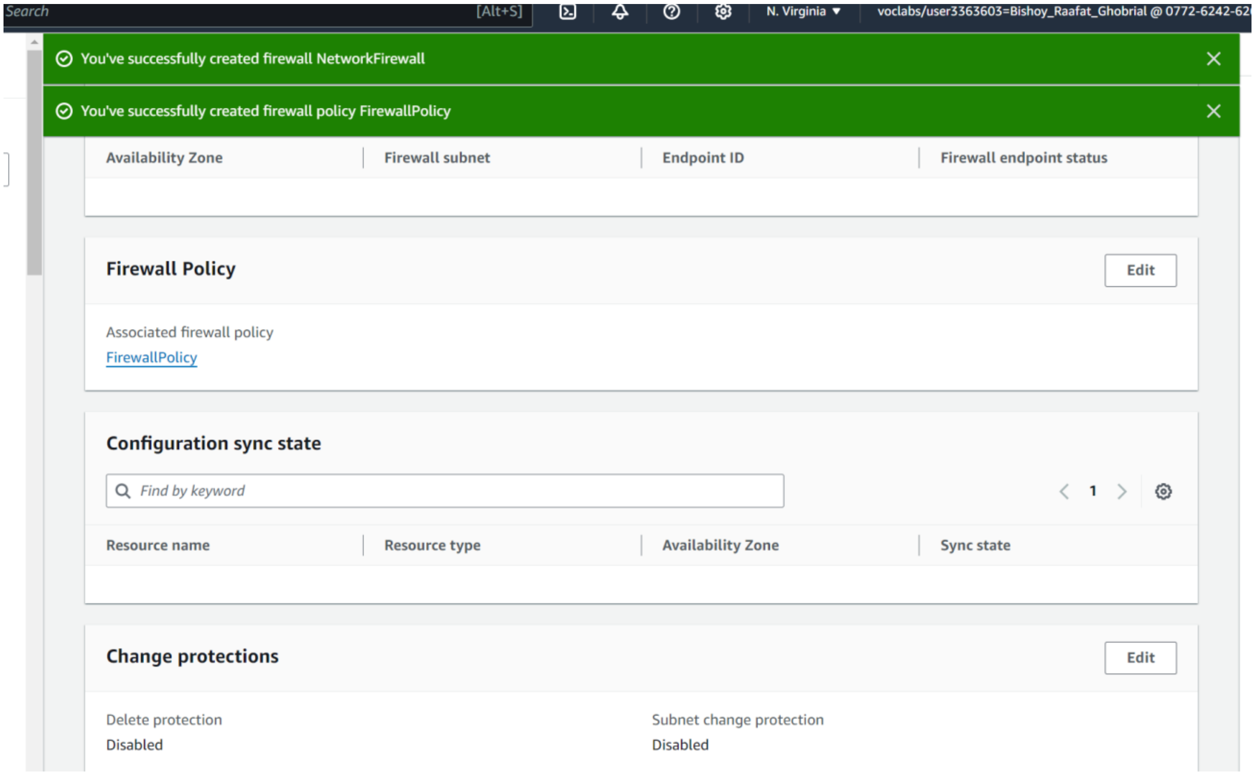
Toolkit for AWS Cloud9

The AWS Toolkit for Cloud9 is an IDE extension that simplifies accessing and interacting with resources from services such as AWS Lambda, AWS CloudFormation, and AWS API Gateway. With the toolkit, developers can also develop, debug, and deploy applications

```
Connection to 3.233.3.59 80 port [tcp/http] succeeded!
voclabs:~/environment $ nc -vz 3.233.3.59 22

^C
voclabs:~/environment $ nc -vz 34.237.168.178 80
Connection to 34.237.168.178 80 port [tcp/http] succeeded!
voclabs:~/environment $ 
```

Task 2.7: Create a network firewall



You've successfully created firewall NetworkFirewall

You've successfully created firewall policy FirewallPolicy

Availability Zone	Firewall subnet	Endpoint ID	Firewall endpoint status

Firewall Policy

Associated firewall policy
FirewallPolicy

Configuration sync state

Find by keyword

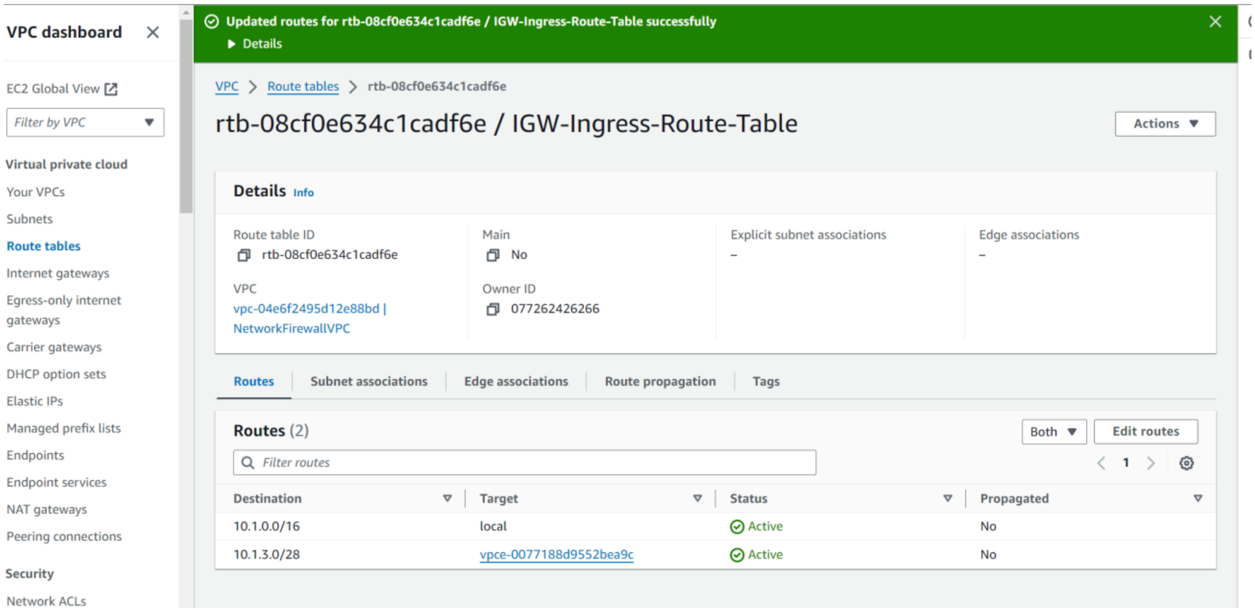
Resource name	Resource type	Availability Zone	Sync state

Change protections

Delete protection
Disabled

Subnet change protection
Disabled

Task 2.8: Create route tables



Updated routes for rtb-08cf0e634c1cadf6e / IGW-Ingress-Route-Table successfully

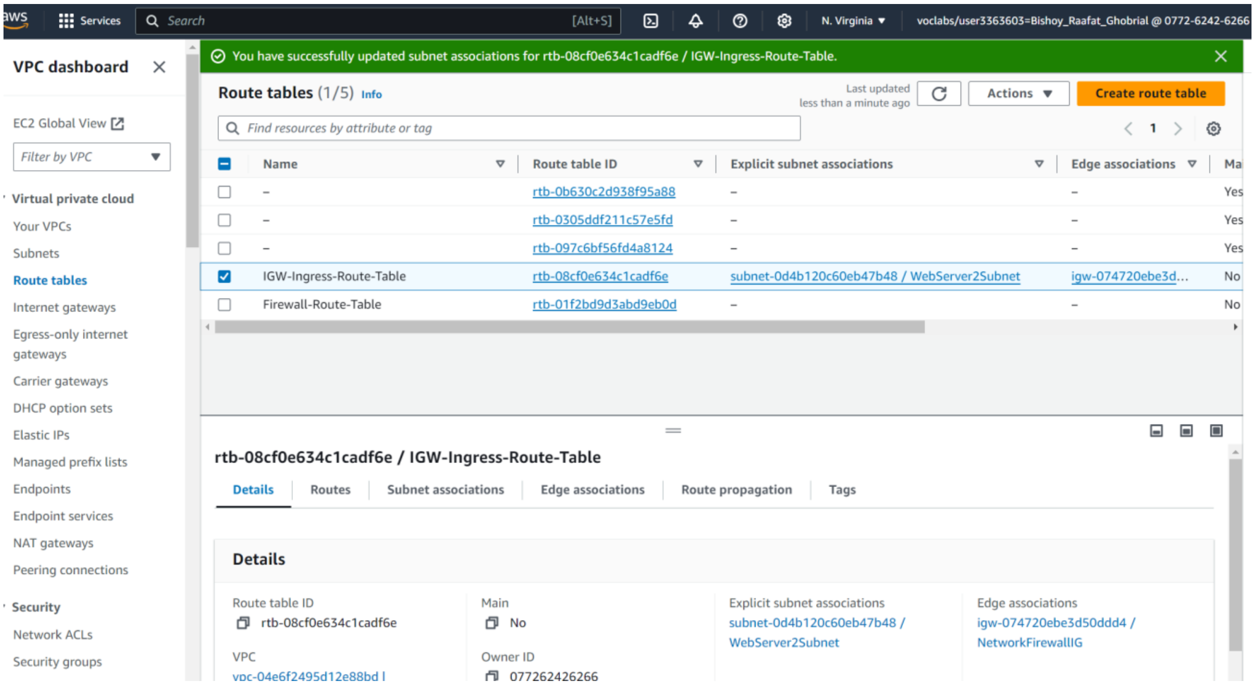
rtb-08cf0e634c1cadf6e / IGW-Ingress-Route-Table

Details Info

Route table ID: rtb-08cf0e634c1cadf6e
Main: No
Explicit subnet associations: –
Edge associations: –
VPC: vpc-04e6f2495d12e88bd | NetworkFirewallVPC
Owner ID: 077262426266

Routes (2)

Destination	Target	Status	Propagated
10.1.0.0/16	local	Active	No
10.1.3.0/28	vpce-0077188d9552bea9c	Active	No



You have successfully updated subnet associations for rtb-08cf0e634c1cadf6e / IGW-Ingress-Route-Table.

Route tables (1/5) Info

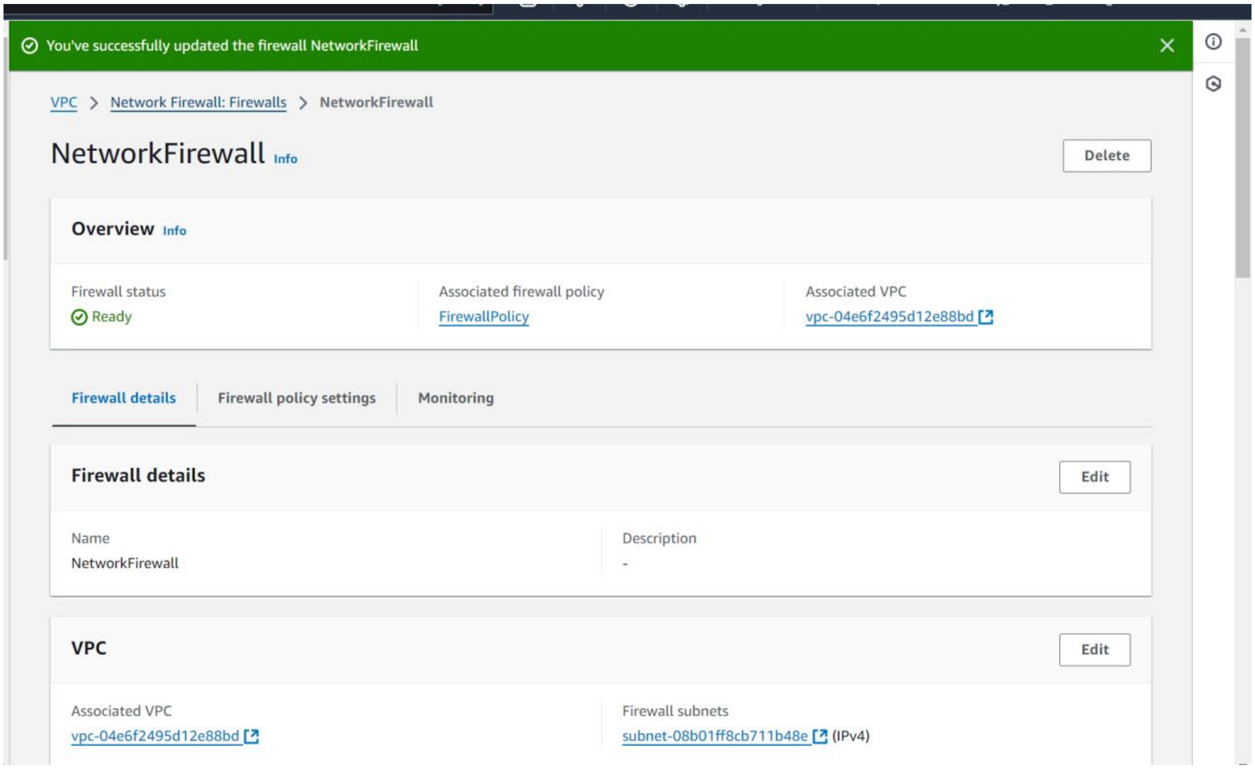
	Name	Route table ID	Explicit subnet associations	Edge associations	Ma
□	–	rtb-0b630c2d938f95a88	–	–	Yes
□	–	rtb-0305ddf211c57e5fd	–	–	Yes
□	–	rtb-097c6bf56fd4a8124	–	–	Yes
☑	IGW-Ingress-Route-Table	rtb-08cf0e634c1cadf6e	subnet-0d4b120c60eb47b48 / WebServer2Subnet	igw-074720ebe3d…	No
□	Firewall-Route-Table	rtb-01f2bd9d3abd9eb0d	–	–	No

rtb-08cf0e634c1cadf6e / IGW-Ingress-Route-Table

Details

Route table ID: rtb-08cf0e634c1cadf6e
Main: No
Explicit subnet associations: subnet-0d4b120c60eb47b48 / WebServer2Subnet
Edge associations: igw-074720ebe3d50ddd4 / NetworkFirewallIG
VPC: vpc-04e6f2495d12e88bd |
Owner ID: 077262426266

Task 2.9: Configure logging for the network firewall



You've successfully updated the firewall NetworkFirewall

VPC > Network Firewall: Firewalls > NetworkFirewall

NetworkFirewall Info

Overview Info

Firewall status: Ready

Associated firewall policy: FirewallPolicy

Associated VPC: vpc-04e6f2495d12e88bd

Firewall details

Name: NetworkFirewall

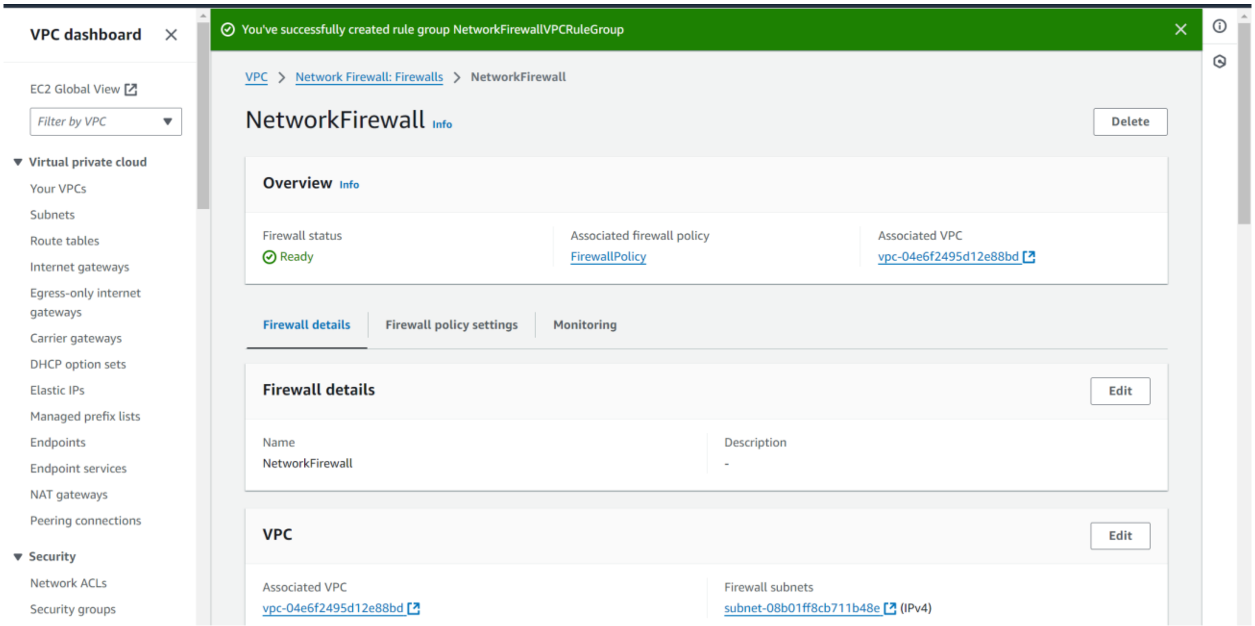
Description: -

VPC

Associated VPC: vpc-04e6f2495d12e88bd

Firewall subnets: subnet-08b01ff8cb711b48e (IPv4)

Task 2.10: Configure the firewall policy and test access



You've successfully created rule group NetworkFirewallVPCRuleGroup

NetworkFirewall Info

Overview Info

Firewall status	Associated firewall policy	Associated VPC
Ready	FirewallPolicy	vpc-04e6f2495d12e88bd

Firewall details

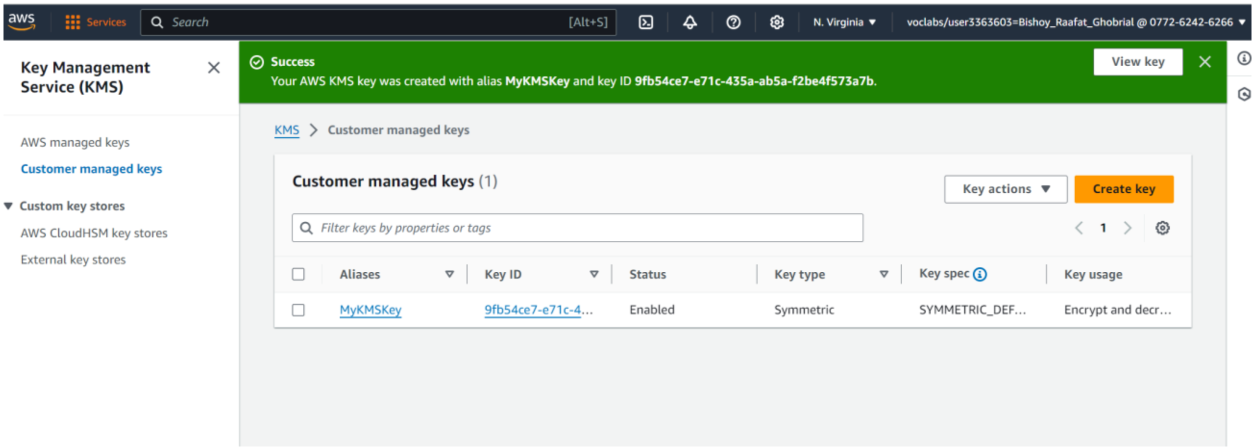
Name	Description
NetworkFirewall	-

VPC

Associated VPC	Firewall subnets
vpc-04e6f2495d12e88bd	subnet-08b01ff8cb711b48e (IPv4)

Phase 3: Securing AWS resources by using AWS KMS

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

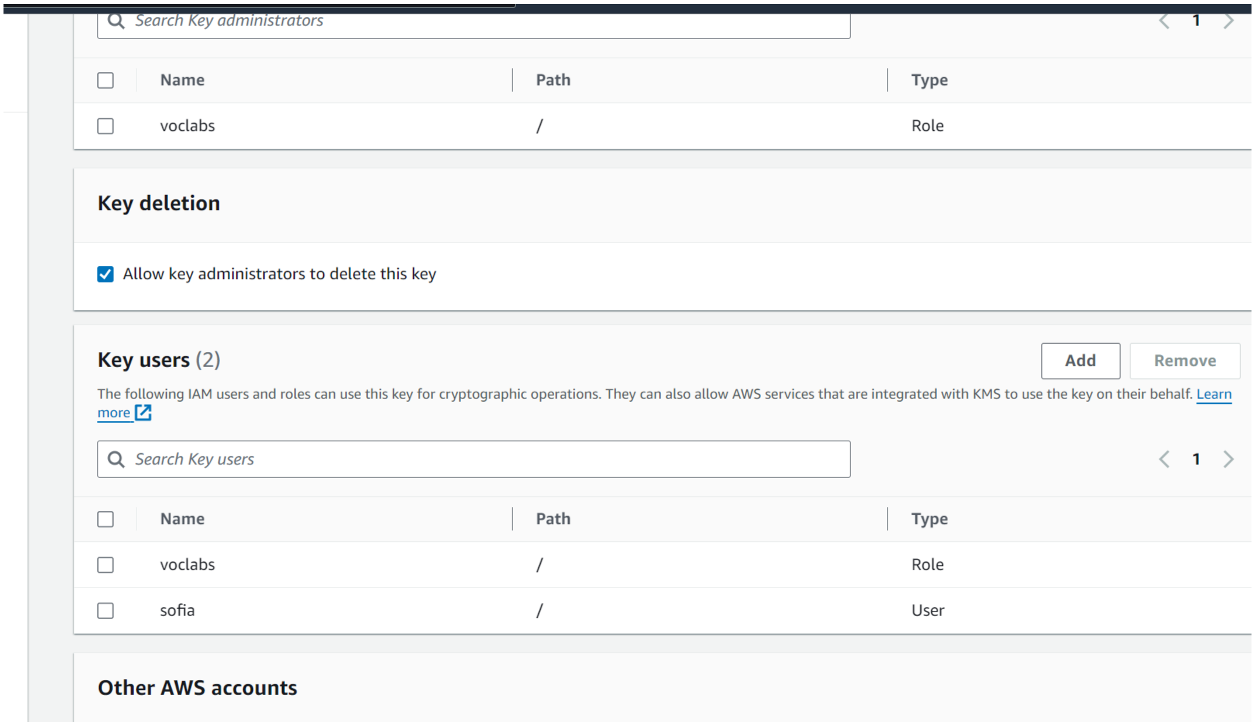


Success
Your AWS KMS key was created with alias **MyKMSKey** and key ID **9fb54ce7-e71c-435a-ab5a-f2be4f573a7b**.

Customer managed keys (1)

□	Aliases	Key ID	Status	Key type	Key spec	Key usage
□	MyKMSKey	9fb54ce7-e71c-4...	Enabled	Symmetric	SYMMETRIC_DEF...	Encrypt and decr...

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



Search Key administrators

□	Name	Path	Type
□	voclabs	/	Role

Key deletion

☑ Allow key administrators to delete this key

Key users (2)

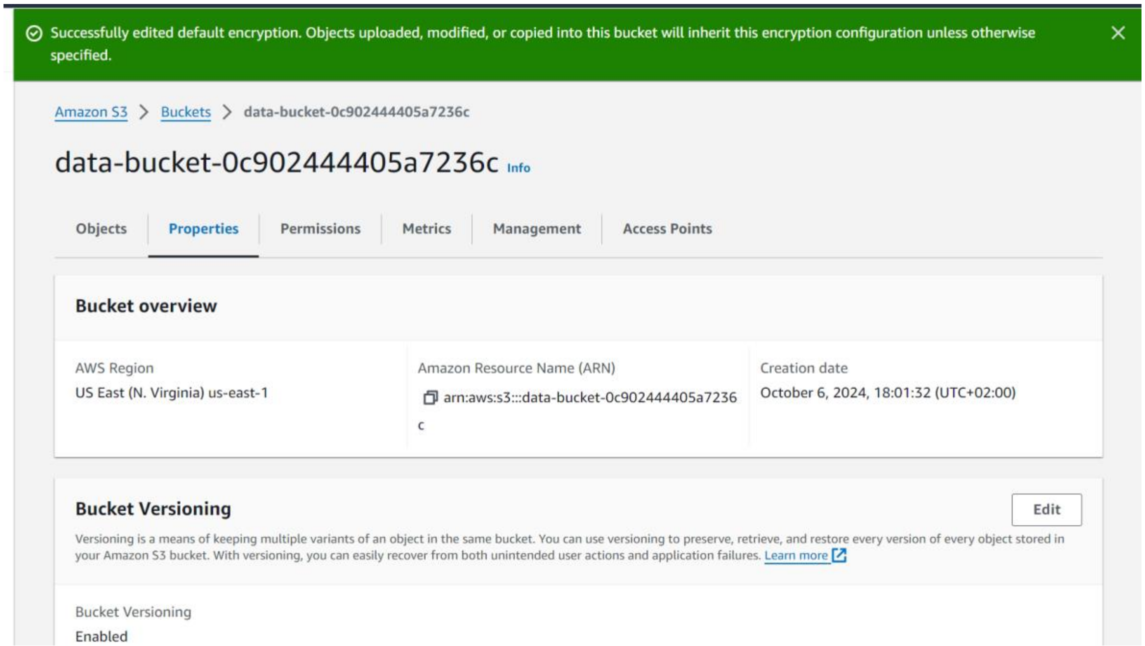
The following IAM users and roles can use this key for cryptographic operations. They can also allow AWS services that are integrated with KMS to use the key on their behalf. Learn more

Search Key users

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

Other AWS accounts

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



Successfully edited default encryption. Objects uploaded, modified, or copied into this bucket will inherit this encryption configuration unless otherwise specified.

Amazon S3 > Buckets > data-bucket-0c902444405a7236c

data-bucket-0c902444405a7236c Info

Bucket overview

AWS Region: US East (N. Virginia) us-east-1

Amazon Resource Name (ARN): arn:aws:s3:::data-bucket-0c902444405a7236c

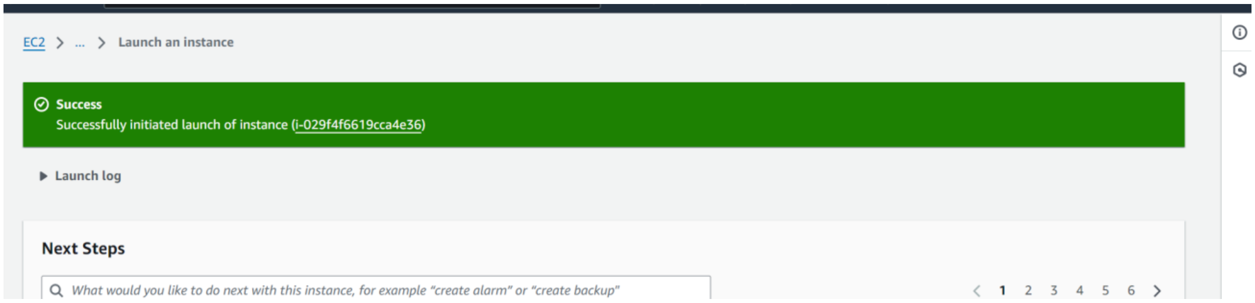
Creation date: October 6, 2024, 18:01:32 (UTC+02:00)

Bucket Versioning

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

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

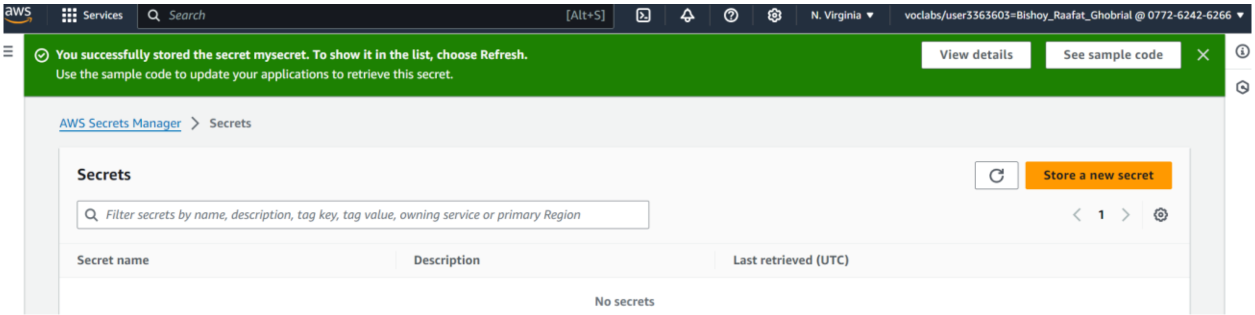


EC2 > ... > Launch an instance

Success
Successfully initiated launch of instance (i-029f4f6619cca4e36)

▶ Launch log
Next Steps
What would you like to do next with this instance, for example "create alarm" or "create backup"
< 1 2 3 4 5 6 >

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



aws
Services
Search
[Alt+S]
N. Virginia ▼
voclabs/user3363603=Bishoy_Raafat_Ghobrial @ 0772-6242-6266 ▼

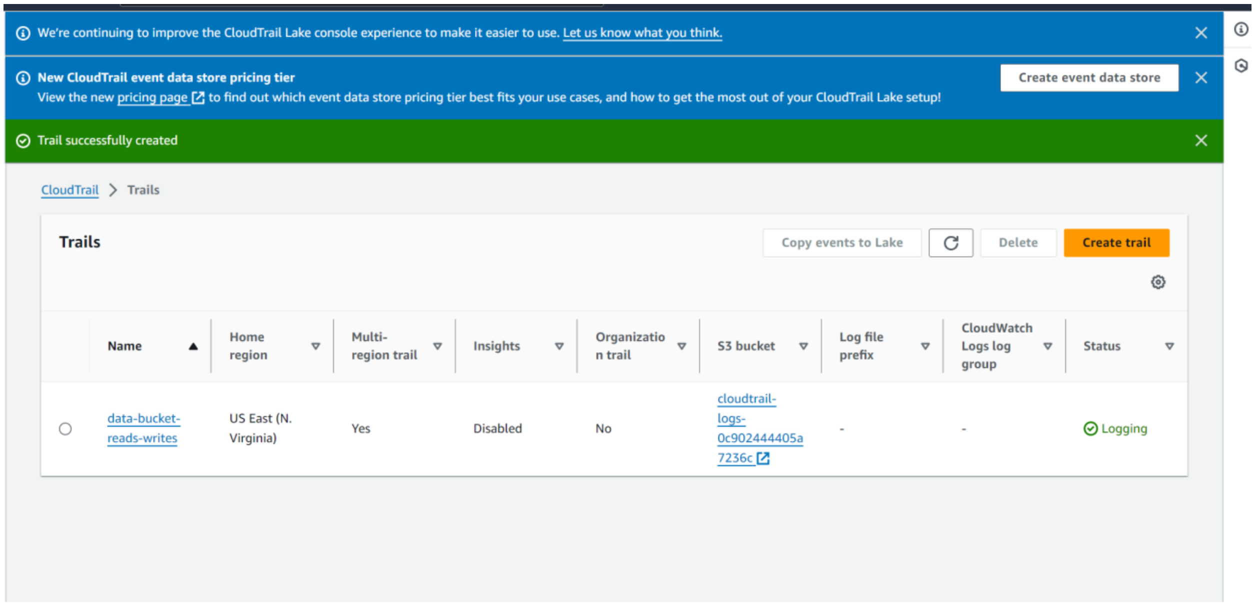
You successfully stored the secret mysecret. To show it in the list, choose Refresh.
Use the sample code to update your applications to retrieve this secret.

View details
See sample code
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)
No secrets		

Phase 4: Monitoring and logging

Task 4.1: Use CloudTrail to record Amazon S3 API calls



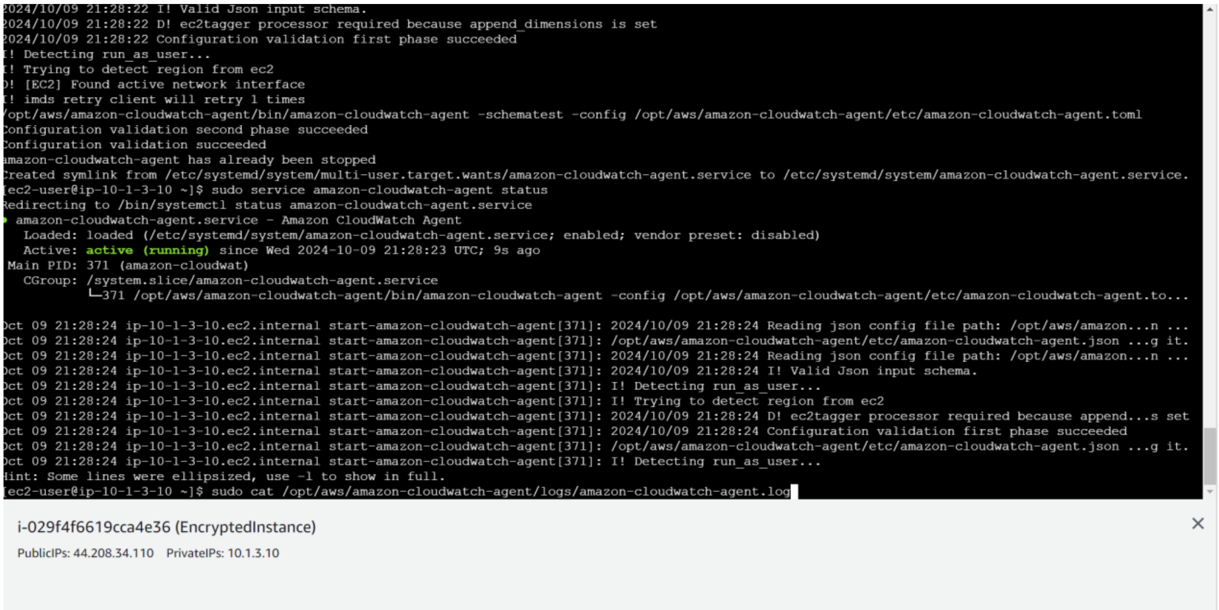
We're continuing to improve the CloudTrail Lake console experience to make it easier to use. Let us know what you think.

New CloudTrail event data store pricing tier
View the new pricing page to find out which event data store pricing tier best fits your use cases, and how to get the most out of your CloudTrail Lake setup!

Trail successfully created

	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-0c902444405a7236c	-	-	Logging

Task 4.2: Use CloudWatch Logs to monitor secure logs



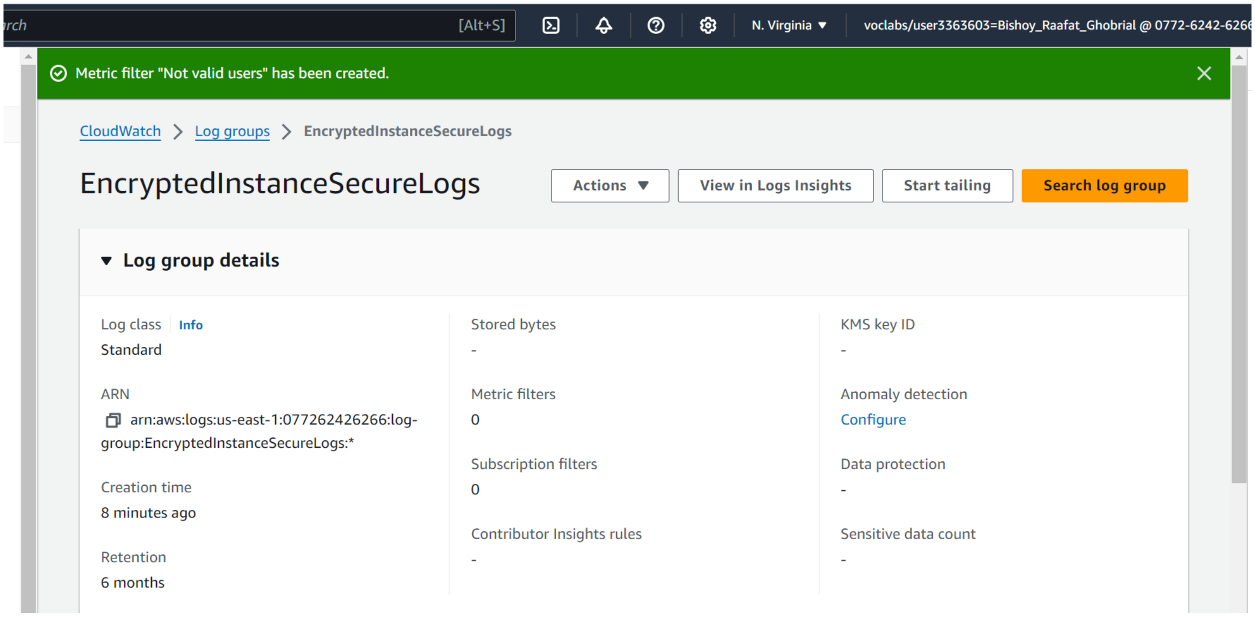
```
2024/10/09 21:28:22 I! Valid Json input schema.
2024/10/09 21:28:22 D! ec2tagger processor required because append_dimensions is set
2024/10/09 21:28:22 Configuration validation first phase succeeded
I! Detecting run_as_user...
I! Trying to detect region from ec2
D! [EC2] Found active network interface
I! imds retry client will retry 1 times
/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -schematest -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml
Configuration validation second phase succeeded
Configuration validation succeeded
amazon-cloudwatch-agent has already been stopped
Created symlink from /etc/systemd/system/multi-user.target.wants/amazon-cloudwatch-agent.service to /etc/systemd/system/amazon-cloudwatch-agent.service.
[ec2-user@ip-10-1-3-10 ~]$ sudo service amazon-cloudwatch-agent status
Redirecting to /bin/systemctl status amazon-cloudwatch-agent.service
● amazon-cloudwatch-agent.service - Amazon CloudWatch Agent
   Loaded: loaded (/etc/systemd/system/amazon-cloudwatch-agent.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2024-10-09 21:28:23 UTC; 9s ago
 Main PID: 371 (amazon-cloudwat)
   CGroup: /system.slice/amazon-cloudwatch-agent.service
           └─371 /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.to...

Oct 09 21:28:24 ip-10-1-3-10.ec2.internal start-amazon-cloudwatch-agent[371]: 2024/10/09 21:28:24 Reading json config file path: /opt/aws/amazon...n ...
Oct 09 21:28:24 ip-10-1-3-10.ec2.internal start-amazon-cloudwatch-agent[371]: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json ...g it.
Oct 09 21:28:24 ip-10-1-3-10.ec2.internal start-amazon-cloudwatch-agent[371]: 2024/10/09 21:28:24 Reading json config file path: /opt/aws/amazon...n ...
Oct 09 21:28:24 ip-10-1-3-10.ec2.internal start-amazon-cloudwatch-agent[371]: 2024/10/09 21:28:24 I! Valid Json input schema.
Oct 09 21:28:24 ip-10-1-3-10.ec2.internal start-amazon-cloudwatch-agent[371]: I! Detecting run_as_user...
Oct 09 21:28:24 ip-10-1-3-10.ec2.internal start-amazon-cloudwatch-agent[371]: I! Trying to detect region from ec2
Oct 09 21:28:24 ip-10-1-3-10.ec2.internal start-amazon-cloudwatch-agent[371]: 2024/10/09 21:28:24 D! ec2tagger processor required because append...s set
Oct 09 21:28:24 ip-10-1-3-10.ec2.internal start-amazon-cloudwatch-agent[371]: 2024/10/09 21:28:24 Configuration validation first phase succeeded
Oct 09 21:28:24 ip-10-1-3-10.ec2.internal start-amazon-cloudwatch-agent[371]: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json ...g it.
Oct 09 21:28:24 ip-10-1-3-10.ec2.internal start-amazon-cloudwatch-agent[371]: I! Detecting run_as_user...
Hint: Some lines were ellipsized, use -l to show in full.
[ec2-user@ip-10-1-3-10 ~]$ sudo cat /opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log
```

i-029f4f6619cca4e36 (EncryptedInstance)

PublicIPs: 44.208.34.110 PrivateIPs: 10.1.3.10

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


rch
[Alt+S]
N. Virginia ▼
voclabs/user3363603=Bishoy_Raafat_Ghobrial @ 0772-6242-626

Metric filter "Not valid users" has been created.

CloudWatch > Log groups > EncryptedInstanceSecureLogs

EncryptedInstanceSecureLogs

Actions ▼
View in Logs Insights
Start tailing
Search log group

▼ Log group details

Log class Info Standard	Stored bytes -	KMS key ID -
ARN arn:aws:logs:us-east-1:077262426266:log-group:EncryptedInstanceSecureLogs:*	Metric filters 0	Anomaly detection Configure
	Subscription filters 0	Data protection -
Creation time 8 minutes ago	Contributor Insights rules -	Sensitive data count -
Retention 6 months		

Conclusion

By the end of this project, we are be able to the following as below :

Secure network access to your virtual network.

Secure access to objects in an Amazon Simple Storage Service (Amazon S3) bucket.

Manage encryption keys by using AWS KMS.

Encrypt data at rest by using AWS Key Management Service (AWS KMS) on an Amazon Elastic Block Store (Amazon EBS) volume.

Create a monitoring and incident response system by using Amazon CloudWatch and AWS Config.