



## **Project 2: Securing and Monitoring Resources with AWS**

Name: Yousef Hassan Yousef Eltobgy

Student ID: 21031713

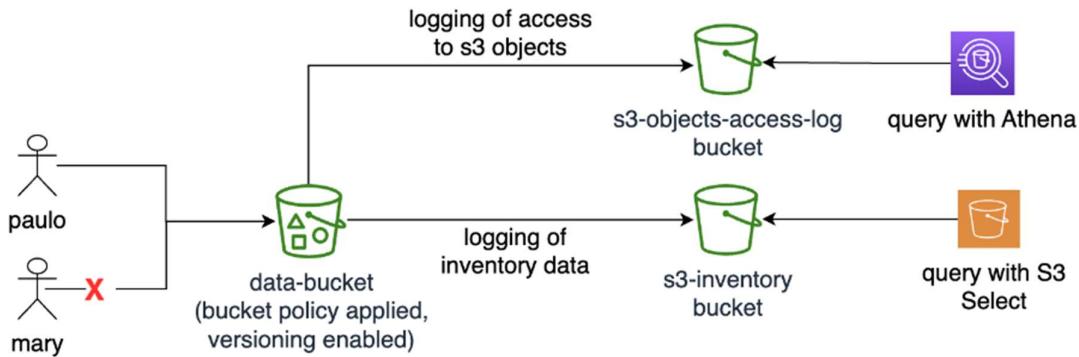
Email: eltobggy@gmail.com

Track: AWS Cloud Solution Admin & Architect

Group Code: ALX1\_ISS4\_M1e

## Project 2: Securing and Monitoring Resources with AWS

### Phase 1: Securing data in Amazon S3



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

Created the bucket below

Name	AWS Region	IAM Access Analyzer	Creation date
aws-config-08f7f4a372b453cb3	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	October 6, 2024, 21:04:41 (UTC+03:00)
cloudtrail-logs-08f7f4a372b453cb3	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	October 6, 2024, 21:04:41 (UTC+03:00)
<b>data-bucket-08f7f4a372b453cb3</b>	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	October 6, 2024, 21:12:32 (UTC+03:00)
s3-inventory-08f7f4a372b453cb3	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	October 6, 2024, 21:04:41 (UTC+03:00)
s3-objects-access-log-08f7f4a372b453cb3	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	October 6, 2024, 21:04:41 (UTC+03:00)

Uploaded a file

Name	Type	Last modified	Size	Storage class
myfile.txt	txt	October 6, 2024, 21:40:26 (UTC+03:00)	11.0 B	Standard

I added the below policy to allow all Amazon S3 service actions for all principals for data-bucket and all objects in it, only for the ARN equals the ARN for the voclabs IAM role, the paulo IAM user, or the sofia IAM user.




**Bucket policy**

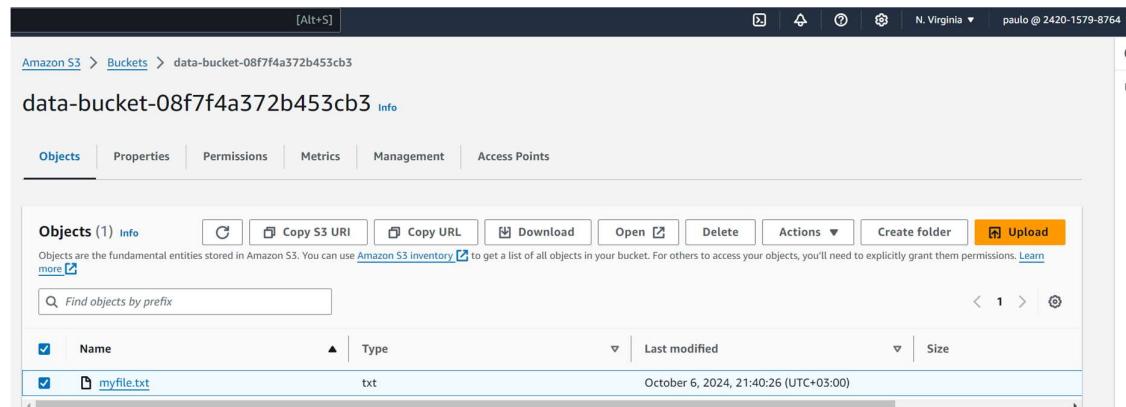
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

**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",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "AWS": [
        "arn:aws:iam::242015798764:user/sofia",
        "arn:aws:iam::242015798764:role/voclabs",
        "arn:aws:iam::242015798764:user/paulo"
      ],
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::data-bucket-08f7f4a372b453cb3",
        "arn:aws:s3:::data-bucket-08f7f4a372b453cb3/*"
      ]
    },
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::data-bucket-08f7f4a372b453cb3",
        "arn:aws:s3:::data-bucket-08f7f4a372b453cb3/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalArn": [
            "arn:aws:iam::242015798764:role/voclabs",
            "arn:aws:iam::242015798764:user/paulo",
            "arn:aws:iam::242015798764:user/sofia"
          ]
        }
      }
    }
  ]
}
```

[Copy](#)

As per below I can verify that the user named Paulo has permission to access the S3 bucket and can download the file and has other actions that he can do.



Amazon S3 > Buckets > data-bucket-08f7f4a372b453cb3 [Info](#)

data-bucket-08f7f4a372b453cb3 [info](#)

Objects Properties Permissions Metrics Management Access Points

Objects (1) [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](#)

<input checked="" type="checkbox"/>	Name	Type	Last modified	Size
<input checked="" type="checkbox"/>	myfile.txt	txt	October 6, 2024, 21:40:26 (UTC+03:00)	

But the user named Mary whom I didn't put her ARN in the policy to allow her to make actions in the bucket, can't view its content.

The screenshot shows the AWS S3 console with the following details:

- Breadcrumbs:** Amazon S3 > Buckets > data-bucket-08f7f4a372b453cb3
- Bucket Name:** data-bucket-08f7f4a372b453cb3
- Tab Selection:** Objects
- Message Box:** 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.

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

Enabled the versioning on the bucket.

The screenshot shows the AWS S3 Properties tab for the bucket 'data-bucket-08f7f4a372b453cb3'. The 'Bucket Versioning' section includes the following information:

- Bucket Versioning:** Enabled
- Multi-factor authentication (MFA) delete:** Disabled

Enabled the Server access logging on the bucket.

The screenshot shows the AWS S3 Properties tab for the bucket 'data-bucket-08f7f4a372b453cb3'. The 'Server access logging' section includes the following configuration:

- Server access logging:** Enabled
- Log object key format:** data-bucket[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
- Destination bucket:** s3://s3-objects-access-log-08f7f4a372b453cb3

I verified that the policy in the bucket allows the whole account to add files in the bucket so there would be no problems when the data bucket put the logs in it. I added the ARN of the data bucket to be allowed to put logs in it.



```
{  
    "Version": "2012-10-17",  
    "Id": "S3-Console-Auto-Gen-Policy-1728241602971",  
    "Statement": [  
        {  
            "Sid": "S3PolicyStmt-DO-NOT-MODIFY-1728241602736",  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "logging.s3.amazonaws.com"  
            },  
            "Action": "s3:PutObject",  
            "Resource": "arn:aws:s3:::s3-objects-access-log-08f7f4a372b453cb3/*",  
            "Condition": {  
                "StringEquals": {  
                    "aws:SourceArn": "arn:aws:s3:::data-bucket-08f7f4a372b453cb3",  
                    "aws:SourceAccount": "242015798764"  
                }  
            }  
        }  
    ]  
}
```

### Task 1.3: Implement the S3 Inventory feature on a bucket

Created the inventory for our data-bucket, and the destination is the “s3-inventory” bucket.

The screenshot shows the 'Inventory configurations' section of the AWS S3 console. It displays a single configuration named 'Inventory'. The configuration details are as follows:

- Name: Inventory
- Status: Enabled
- Scope: Entire bucket
- Destination: s3://s3-inventory-08f7f4...
- Frequency: Daily
- Last export: -
- Format: Apache Parquet

### Task 1.4: Confirm that versioning works as intended

Created a file named “customers.csv” with the below data.

A	B	C	D	E	F	G
CustomerID	First Name	Last Name	Join Date	Street Address	City,State	Phone
1	Alejandro	Rosalez	12/12/2013	123 Main St.	Any Town,MD	301-555-0158
2	Jane	Doe	10/5/2014	456 State St.	Anywhere,WA	360-555-0163

I uploaded the file with the user named Paulo

Amazon S3 > Buckets > data-bucket-08f7f4a372b453cb3

data-bucket-08f7f4a372b453cb3 [info](#)

Objects Properties Permissions Metrics Management Access Points

**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
<a href="#">customers.csv</a>	csv	j1F91uemcB l7j2hJ.Sbo9I UYKC4kvFT	October 6, 2024, 22:26:18 (UTC+03:00)	8.7 KB	Standard
<a href="#">myfile.txt</a>	txt	null	October 6, 2024, 21:40:26 (UTC+03:00)	11.0 B	Standard

Then I made the below change in the file.

A	B	C	D	E	F	G
CustomerID	First Name	Last Name	Join Date	Street Address	City,State	Phone
1	Alejandro	Rosalez	12/12/2013	123 Main St.	Any Town,MD	301-555-0158
2	Jane	Doe	10/5/2014	456 State St.	Anywhere,WA	360-555-0163
3	x	x	x			

Then uploaded it again. As we can see the versioning is working, the same file has two versions.

Amazon S3 > Buckets > data-bucket-08f7f4a372b453cb3

data-bucket-08f7f4a372b453cb3 [info](#)

Objects Properties Permissions Metrics Management Access Points

**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
<a href="#">customers.csv</a>	csv	RXUK0MHeYk o1.NhRMbZ xOQvpYu4IG o5	October 6, 2024, 22:31:21 (UTC+03:00)	8.7 KB	Standard
<a href="#">customers.csv</a>	csv	j1F91uemcB l7j2hJ.Sbo9I UYKC4kvFT	October 6, 2024, 22:26:18 (UTC+03:00)	8.7 KB	Standard
<a href="#">myfile.txt</a>	txt	null	October 6, 2024, 21:40:26 (UTC+03:00)	11.0 B	Standard

Tried to log in with the user named Mary to make logs of unauthorized access.



Amazon S3 > Buckets > data-bucket-08f7f4a372b453cb3

### data-bucket-08f7f4a372b453cb3 [Info](#)

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

**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](#)

Find objects by prefix  Show versions

Name	Type	Last modified	Size	Storage class
<b>Insufficient permissions to list objects</b> After you or your AWS administrator has updated your permissions to allow the s3>ListBucket action, refresh the page. Learn more about <a href="#">Identity and access management in Amazon S3</a>				

The logs folder was created successfully automatically and the logs were put inside it.

Amazon S3 > Buckets > s3-objects-access-log-08f7f4a372b453cb3 > data-bucket/

### data-bucket/

[Objects](#) [Properties](#)

**Objects (14) [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

Name	Type	Last modified	Size	Storage class
2024-10-06-20-11-48-6145F7CD10A074DB	-	October 6, 2024, 23:11:49 (UTC+03:00)	744.0 B	Standard
2024-10-06-20-12-10-DF225CEC7124F5AB	-	October 6, 2024, 23:12:11 (UTC+03:00)	707.0 B	Standard
2024-10-06-20-13-15-AB8E6B0C05CA3533	-	October 6, 2024, 23:13:16 (UTC+03:00)	647.0 B	Standard
2024-10-06-20-13-16-556915AD8875340A	-	October 6, 2024, 23:13:17 (UTC+03:00)	697.0 B	Standard
2024-10-06-20-13-54-15B2B833C7907420	-	October 6, 2024, 23:13:55 (UTC+03:00)	687.0 B	Standard
2024-10-06-20-14-02-F19360CFCB99110F	-	October 6, 2024, 23:14:03 (UTC+03:00)	693.0 B	Standard
2024-10-06-20-14-09-EA54E2024B29734D	-	October 6, 2024, 23:14:10 (UTC+03:00)	704.0 B	Standard
2024-10-06-20-14-18-9AFF55450E61F688	-	October 6, 2024, 23:14:19 (UTC+03:00)	663.0 B	Standard
2024-10-06-20-14-27-0A8E6B0C05CA3533	-	October 6, 2024, 23:14:28 (UTC+03:00)	740.0 B	Standard

And the deny log appeared as per below.

https://s3-objects-access-log-08f7f4a372b453cb3.s3.amazonaws.com/data-bucket/2024-10-06-20-11-48-6145F7CD10A074DB

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>Access Denied</Message>
  <RequestId>CAH8KYFHJD9WCCB0</RequestId>
  <HostId>VJRdPYXdn6q8J0t0HhUYLgaVgkmPabJyXJLrm/Ke5JNm5EuS+AfvWgxxyKQ6Qy7hDBDYt3JY32WsxnAuqt6yXp9E0aNDcsn0iz51PlWkiIY=</HostId>
</Error>
```

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



I downloaded one of the log files and this is what is inside it.

```
File Edit View

0ceba13b9b1642ab6e03aa433562738f9a98e061013711e9b923e5b34a193faeb data-bucket-08f7f4a372b453cb3 [06/Oct/2024:19:35:16 +0000]
154.180.126.184 arn:aws:iam::242015798764:user/mary Y8NQD8T9XNEBSEE REST.GET.OWNERSHIP_CONTROLS - "GET /data-bucket-08f7f4a372b453cb3?
ownershipControls= HTTP/1.1" 403 AccessDenied 400 - 41 40 "-" "S3Console/0.4, aws-internal/3 aws-sdk-java/1.12.750
Linux/5.10.225-191.878.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.412-b09 java/1.8.0_412 vendor/Oracle_Corporation cfg/retry-
mode/standard" - WmbjFiAaNbQ21hwBsR2kNpt3OJON2PG5DYhtuojyHeIMWFIn1EDHyTyg61K1Q4S1h4z1Y61A= SigV4 TLS_AES_128_GCM_SHA256 AuthHeader
s3.amazonaws.com TLSv1.3 -
```

Then I created a bucket for athena results.

The screenshot shows the Amazon S3 console interface. The top navigation bar includes 'Amazon S3 > Buckets > athena-results-08f7f4a372b453cb3'. Below the navigation is a header with tabs: 'Objects' (selected), 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. Under the 'Objects' tab, there is a toolbar with actions like 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and 'Upload'. A search bar labeled 'Find objects by prefix' is present. A table below lists objects, with columns for 'Name', 'Type', 'Last modified', 'Size', and 'Storage class'. A message 'No objects' indicates the bucket is currently empty. At the bottom right of the table area is a large orange 'Upload' button.

Then created a workgroup and configured it to store the results in the “athena results” bucket.

The screenshot shows the Amazon Athena console interface. The top navigation bar includes 'Amazon Athena > Workgroups > project2'. Below the navigation is a header with buttons for 'Edit', 'Turn off workgroup', and 'Delete'. The main area is titled 'Overview details' and contains several configuration items in a grid format:

Workgroup name project2	Query engine version status Automatic	Query result location s3://athena-results-08f7f4a372b453cb3/
Description -	Override client side settings Turned off	Encrypt query results -
Created on 2024-10-06T23:20:23.638+03:00	Queries with requester pays buckets Turned off	Expected bucket owner -
Query engine version Athena engine version 3	Workgroup ARN arn:aws:athena:us-east-1:242015798764:workgroup/project2	Assign bucket owner full control over query results Turned off
Workgroup state Turned on	Publish metrics to Amazon CloudWatch Turned on	
Authentication AWS Identity and Access Management (IAM)		

I ran the query in the workgroup that I just created. This created the table named “bucket\_logs”.



Amazon Athena > Query editor tabs

Editor Recent queries Saved queries Settings Workgroup project2

**Data**

Data source: AwsDataCatalog Database: default

Tables and views: Create Filter tables and views

Tables (1) < 1 >

bucket\_logs

Views (0) < 1 >

**Query 1 :**

```
1 - CREATE EXTERNAL TABLE `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 )
13 ROW FORMAT SERDE
14   'org.apache.hadoop.hive.serde2.RegexSerDe'
15 WITH SERDEPROPERTIES (
16   'input.regex' = '([^\"]*) ([^\"]*) \\([.*?]\\) ([^\"]*) ([^\"]*) ([^\"]*) ([^\"]*) ([^\"]*) ([^\"]*) ([^\"]*) ([^\"]*) ([^\"]*) ([^\"]*) ([^\"]*) ([^\"]*) ([^\"]*) '
17   ([^\"]*) ([^\"]*) (\\"[^\"]*\\") ([^\"]*) ([^\"]*) ([^\"]*) ([^\"]*) '
18 )
19 LOCATION
20 's3://s3-objects-access-log-08f7f4a372b453cb3/'
```

SQL Ln 20, Col 50

Run again Explain Cancel Clear Create Reuse query results up to 60 minutes ago

**Query results** | **Query status**

Completed Time in queue: 86 ms Run time: 457 ms Data scanned: -

Query successful.

I used the below query to get records for actions taken as the paulo user, because that user can access the bucket and its objects.

Amazon Athena > Query editor tabs

Editor Recent queries Saved queries Settings Workgroup project2

**Data**

Data source: AwsDataCatalog Database: default

Tables and views: Create Filter tables and views

Tables (1) < 1 >

bucket\_logs

Views (0) < 1 >

**Query 1 : X** | **Query 2 : X**

```
1 SELECT requester, operation, key, httpstatus
2 FROM `default`.`bucket_logs`
3 WHERE requester LIKE 'arn:aws:iam::242015798764:user/paulo';
```

Amazon Athena > Query editor tabs

Editor Recent queries Saved queries Settings Workgroup project2

**Data**

Data source: AwsDataCatalog Database: default

Tables and views: Create Filter tables and views

Tables (1) < 1 >

bucket\_logs

Views (0) < 1 >

**Query 1 : X** | **Query 2 : X**

```
1 SELECT requester, operation, key, httpstatus
2 FROM `default`.`bucket_logs`
3 WHERE requester LIKE 'arn:aws:iam::242015798764:user/paulo';
```

## Cost assessment to secure Amazon S3



For the low size files that were used there was no additional costs for using versioning, service access logging, and S3 Inventory on a bucket. And Athena and S3 Select to analyze access logs.

AWS Pricing Calculator > My Estimate

My Estimate [Edit](#)

Estimate summary [Info](#)

Upfront cost	Monthly cost	Total 12 months cost
0.00 USD	0.00 USD	<b>0.00 USD</b> Includes upfront cost

Getting Started with AWS

[Get started for free](#) [Contact Sales](#)

**My Estimate**

Service Name	Status	Upfront cost	Monthly cost	Description	Region	Config Summary
Amazon Athena	-	0.00 USD	0.00 USD	-	US East (N. Virginia)	Total number of queries (...)
Amazon Simple Storage ...	-	0.00 USD	0.00 USD	-	US East (N. Virginia)	S3 Standard storage (0.0...)

Billing and Cost Management home [Info](#)

Reset layout

**Cost summary** [Info](#)

Month-to-date cost	Last month's cost for same time period
<b>\$0.00</b>	<b>\$0.00</b> Sep 1–6

↓ 0% compared to last month for same period

Total forecasted cost for current month [Data unavailable](#)

Last month's total cost **\$0.00**

[View bill](#)

**Cost monitor** [Info](#)

Budgets status
<b>Setup required</b> No budget created

Cost anomalies status (MTD) [Setup required](#)  
No monitor created

**Cost breakdown** [Info](#)

Group costs by [Service](#)

Costs (\$)

0.00

May 2024 Jun 2024 Jul 2024 Aug 2024 Sep 2024 Oct 2024

Others

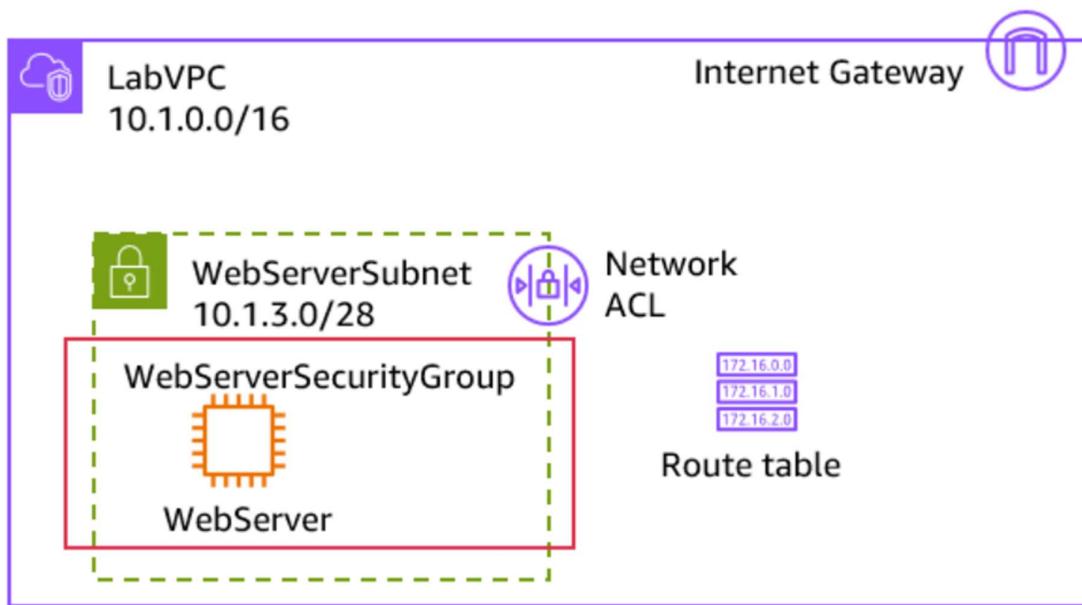
Analyze your costs in Cost Explorer

**Recommended actions (1)** [Info](#)

**Getting started**  
Create a Cost Anomaly monitor to automatically detect cost anomalies. [Create a monitor](#)

## Phase 2: Securing VPCs

The following diagram shows the resources that already exist in the lab environment.



### Task 2.1: Review LabVPC and its associated resources

analyzed the resource map of the existing LabVPC. It contains the following resources: A subnet named WebServerSubnet, A route table which is the main route table that is created by default for any VPC, and an internet gateway.

The screenshot shows the AWS VPC console for the LabVPC:

**Details** tab (top half):

VPC ID: <a href="#">vpc-0e044f7e5ad5c1c11</a>	State: Available	DNS hostnames: Enabled	DNS resolution: Enabled
Tenancy: Default	DHCP option set: <a href="#">dopt-032beccb57d7ca3b8d</a>	Main route table: <a href="#">rtb-0bc86dae57191a490</a>	Main network ACL: <a href="#">acl-0ccb176ce905b1101</a>
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: <a href="#">242015798764</a>	-

**Resource map** tab (bottom half):

This tab displays the relationships between the VPC, Subnets, Route tables, and Network connections:

- VPC**: Your AWS virtual network (LabVPC)
- Subnets (1)**: Subnets within this VPC (us-east-1a, WebServerSubnet)
- Route tables (1)**: Route network traffic to resources (rtb-0bc86dae57191a490)
- Network connections (1)**: Connections to other networks (LabVPCIG)

Review the permissions that are granted to the “VPCFlowLogsRole” IAM role.

**VPCFlowLogsRole**

**Permissions policies (1)**

```

1 - [ { "Statement": [ 2 - { 3 - "Action": [ 4 - "logs:CreateLogGroup", 5 - "logs:CreateLogStream", 6 - "logs:PutLogEvents" 7 - ], 8 - "Resource": "*", 9 - "Effect": "Allow" 10 - } 11 - } 12 - ] 13 - }
14 - ]

```

Then I observed the details for the WebServer instance.

Detail	Value
Instance ID	i-023b64da58389ffad (WebServer)
IPv6 address	-
Hostname type	IP name: ip-10-1-3-4.ec2.internal
Answer private resource DNS name	-
Auto-assigned IP address	-
IAM Role	WebServerRole
IMDSv2	Required
Public IPv4 address	54.146.76.192
Instance state	Running
Private IP DNS name (IPv4 only)	ip-10-1-3-4.ec2.internal
Instance type	t2.micro
VPC ID	vpc-0e044f7e5ad5c1c11 (LabVPC)
Subnet ID	subnet-0492ff8d06803e009 (WebServerSubnet)
Instance ARN	arn:aws:ec2:us-east-1:242015798764:instance/i-023b64da58389ffad
Owner ID	242015798764
Launch time	Mon Oct 07 2024 13:44:55 GMT+0300 (Eastern European Summer Time)

## Task 2.2: Create a VPC flow log

Create VPC flow logs in our “LabVPC”.

VPC > Your VPCs > vpc-0e044f7e5ad5c1c11 / LabVPC

**Details**

VPC ID vpc-0e044f7e5ad5c1c11	State Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-032becb57d7ca3b8d	Main route table rtb-0bc86dae57191a490	Main network ACL acl-0ccb176ce905b1101
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 242015798764	-

Resource map | CIDRs | **Flow logs** | Tags | Integrations

**Flow logs (1)**

Name	Flow log ID	Filter	Destination type	Destination name	IAM role ARN
LabVPCFlowLogs	fl-0b5e1cbdb42e1f886	ALL	cloud-watch-logs	LabVPCFlowLogs	arn:aws:iam::242015798764:role/VPCF

And I put the Destination log group to the group named “LabVPCFlowLogs”.

CloudWatch > Log groups > LabVPCFlowLogs

**Log group details**

Log class Standard	Stored bytes -	KMS key ID -
ARN arn:aws:logs:us-east-1:242015798764:log-group:LabVPCFlowLogs:*	Metric filters 0	Anomaly detection <a href="#">Configure</a>
Creation time 5 minutes ago	Subscription filters 0	Data protection -
Retention Never expire	Contributor Insights rules -	Sensitive data count -

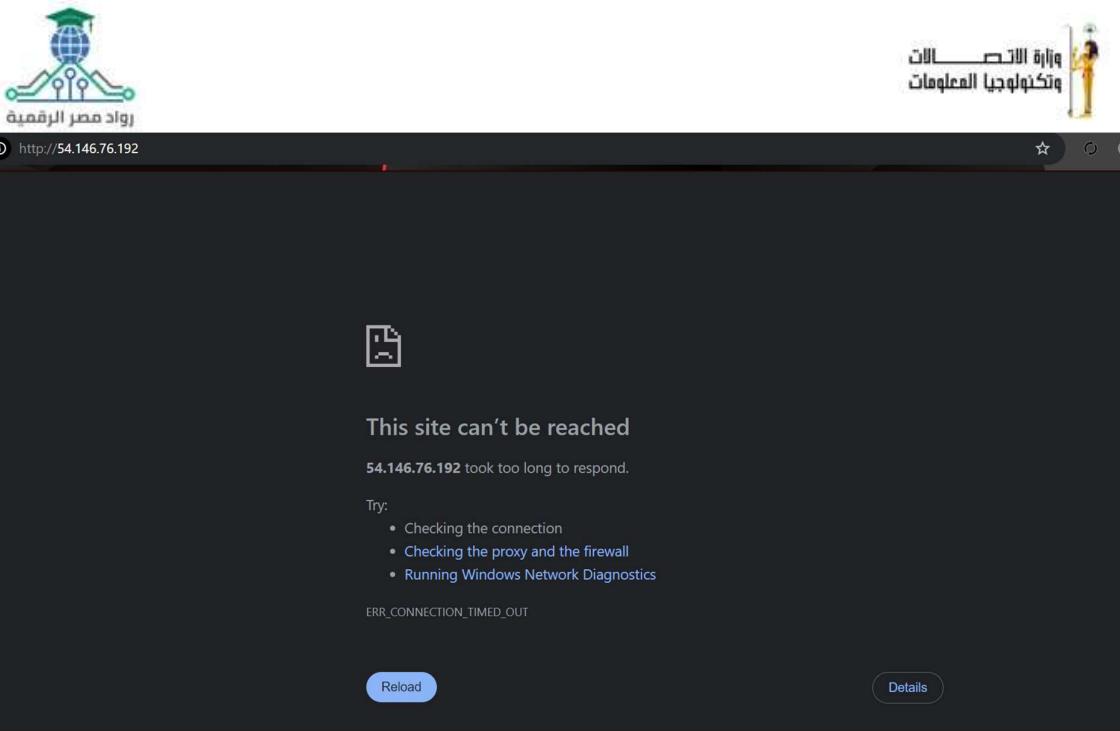
Log streams | Tags | Anomaly detection | Metric filters | Subscription filters | Contributor Insights | Data protection

**Log streams (1)**

Log stream	Last event time
eni-007b8201c963effa7-all	2024-10-07 12:35:36 (UTC)

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

Tried to access the web server instance from its public IP but it is not reachable



Tested the connectivity to it from port 80 but the command is loading and will lead to timeout. It means that it can't reach the instance from port 80.

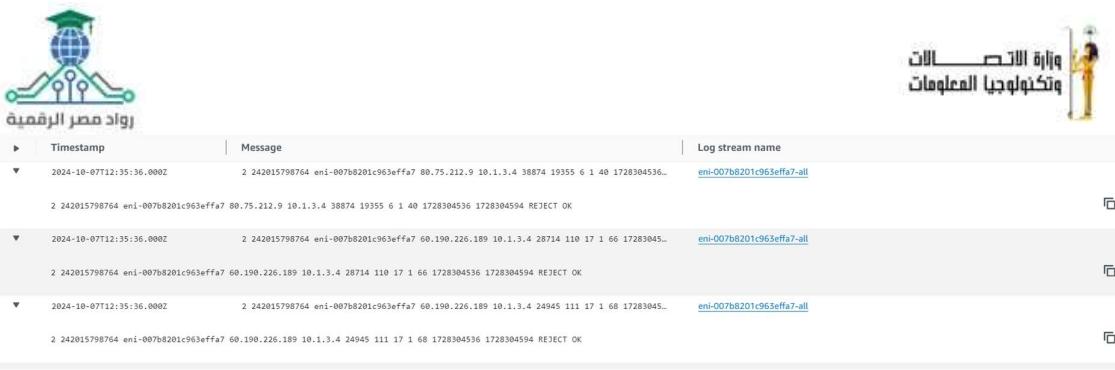
I also tried testing connection for port 22 but same problem

```
voclabs:~/environment $ 
voclabs:~/environment $ nc -vz 54.146.76.192 80
^C
voclabs:~/environment $ nc -vz 54.146.76.192 22
^C
voclabs:~/environment $ 
```

There are many logs in the log group

Log events		Actions ▾ Start tailing Create metric filter									
Filter events - press enter to search		Clear	1m	30m	1h	12h	Custom	UTC timezone ▾	Display ▾	⋮	
▶	Timestamp	Message									
▶	2024-10-07T12:35:36.000Z	2 242015798764 eni-007b8201c963effa7 88.75.212.9 10.1.3.4 38874 19355 6 1 40 1728304536..									
▶	2024-10-07T12:35:36.000Z	2 242015798764 eni-007b8201c963effa7 60.190.226.189 10.1.3.4 28714 110 17 1 66 17283045..									
▶	2024-10-07T12:35:36.000Z	2 242015798764 eni-007b8201c963effa7 60.190.226.189 10.1.3.4 24945 111 17 1 68 17283045..									
▶	2024-10-07T12:35:36.000Z	2 242015798764 eni-007b8201c963effa7 79.110.62.148 10.1.3.4 43503 15768 6 1 40 17283045..									
▶	2024-10-07T12:35:36.000Z	2 242015798764 eni-007b8201c963effa7 185.91.127.83 10.1.3.4 36711 18676 6 1 40 17283045..									
▶	2024-10-07T12:35:36.000Z	2 242015798764 eni-007b8201c963effa7 185.91.127..83 10.1.3.4 55663 20863 6 1 40 17283045..									
▶	2024-10-07T12:35:36.000Z	2 242015798764 eni-007b8201c963effa7 154.213.184.15 10.1.3.4 48171 60823 6 1 40 1728304..									
▶	2024-10-07T12:35:36.000Z	2 242015798764 eni-007b8201c963effa7 113.200.98.17 10.1.3.4 43627 2375 6 1 40 172830453..									
▶	2024-10-07T12:35:36.000Z	2 242015798764 eni-007b8201c963effa7 60.190.226.188 10.1.3.4 13580 111 6 1 52 172830453..									
▶	2024-10-07T12:35:36.000Z	2 242015798764 eni-007b8201c963effa7 60.190.226.188 10.1.3.4 14005 110 6 1 52 172830453..									
▶	2024-10-07T12:35:36.000Z	2 242015798764 eni-007b8201c963effa7 45.156.128.53 10.1.3.4 36683 84 6 1 40 172830453 ..									
▶	2024-10-07T12:36:34.000Z	2 242015798764 eni-007b8201c963effa7 185.167.96.150 10.1.3.4 41882 143 6 1 40 172830459..									
▶	2024-10-07T12:36:34.000Z	2 242015798764 eni-007b8201c963effa7 185.91.127..83 10.1.3.4 43684 10014 6 1 40 17283045..									
▶	2024-10-07T12:36:34.000Z	2 242015798764 eni-007b8201c963effa7 95.214.55.138 10.1.3.4 33153 83 6 1 40 1728304594 ..									
▶	2024-10-07T12:36:34.000Z	2 242015798764 eni-007b8201c963effa7 222.105.70.186 10.1.3.4 51523 23 6 1 40 1728304594..									
▶	2024-10-07T12:36:34.000Z	2 242015798764 eni-007b8201c963effa7 60.190.226.189 10.1.3.4 45082 123 6 1 52 172830459..									
▶	2024-10-07T12:36:34.000Z	2 242015798764 eni-007b8201c963effa7 47.236.90.162 10.1.3.4 3247 2222 6 1 40 1728304594..									

And Message field for all entries indicate "Reject".



I used the below command to get the IP of the Cloud9 instance.

```
voclabs:~/environment $  
voclabs:~/environment $ curl http://169.254.169.254/latest/meta-data/public-ipv4  
52.1.136.202voclabs:~/environment $  
voclabs:~/environment $
```

I filtered the logs with the cloud9 IP to get the logs related to it

Log events									
You can use the filter bar below to search for and match terms, phrases, or values in your log events. <a href="#">Learn more about filter patterns</a>									
<input type="text" value="52.1.136.202"/> <span>X</span> <span>Clear</span> <span>1m</span> <span>30m</span> <span>1h</span> <span>12h</span> <span>Custom</span> <span>UTC timezone</span> <span>Display</span> <span>Export</span>									
Timestamp	Message								Log stream name
2024-10-07T13:39:46.000Z	2.242015798764 eni-007b8201c963effa7 52.1.136.202 10.1.3.4 49702 80 6 360 1728308386 ...								<a href="#">eni-007b8201c963effa7-all</a>
	2.242015798764 eni-007b8201c963effa7 52.1.136.202 10.1.3.4 49702 80 6 360 1728308438 REJECT OK								<a href="#">eni-007b8201c963effa7-all</a>
2024-10-07T13:40:42.000Z	2.242015798764 eni-007b8201c963effa7 52.1.136.202 10.1.3.4 49702 80 6 1 60 1728308442 1...								<a href="#">eni-007b8201c963effa7-all</a>
	2.242015798764 eni-007b8201c963effa7 52.1.136.202 10.1.3.4 49702 80 6 1 60 1728308442 1728308498 REJECT OK								<a href="#">eni-007b8201c963effa7-all</a>
2024-10-07T13:41:58.000Z	2.242015798764 eni-007b8201c963effa7 52.1.136.202 10.1.3.4 33980 22 6 3 180 1728308518 ...								<a href="#">eni-007b8201c963effa7-all</a>
	2.242015798764 eni-007b8201c963effa7 52.1.136.202 10.1.3.4 33980 22 6 3 180 1728308518 1728308558 REJECT OK								<a href="#">eni-007b8201c963effa7-all</a>

## Task 2.4: Configure route table and security group settings

I edited the security group for the web server instance to allow the HTTP from anywhere (0.0.0.0/0) and SSH from an IP range that EC2 Instance Connect uses in the us-east-1 Region. I also deleted unnecessary rules.

sg-0b65318258df26dc4 - WebServerSecurityGroup								
Actions ▾								
Security group name	<a href="#">sg-0b65318258df26dc4</a> - WebServerSecurityGroup	Description	VPC ID					
<a href="#">WebServerSecurityGroup</a>	<a href="#">sg-0b65318258df26dc4</a>	<a href="#">WebServerSecurityGroup</a>	<a href="#">xpc-0e044f7e5ad5c1c11</a>					
Owner	<a href="#">242015798764</a>	Inbound rules count	Outbound rules count					
		2 Permission entries	1 Permission entry					
Inbound rules	Outbound rules	Tags						
Inbound rules (2)								
<input type="text"/> Search								
<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
<input type="checkbox"/>	-	sgr-0b038c5d57e2632...	IPv4	SSH	TCP	22	18.206.107.24/29	-
<input type="checkbox"/>	-	sgr-07a8d18cee097fef3	IPv4	HTTP	TCP	80	0.0.0.0/0	-



I got the IP range using the below commands

```
Installed:
jq.x86_64 0:1.5-1.amzn2.0.2

Dependency Installed:
oniguruma.x86_64 0:5.9.6-1.amzn2.0.7

Complete!
voclabs:~/environment $ curl https://ip-ranges.amazonaws.com/ip-ranges.json| jq -r '.prefixes[] | select(.region=="us-east-1") | select(.service=="EC2_INSTANCE_CONNECT") | .ip_prefix'
% Total    % Received   % Xferd  Average Speed   Time     Time      Current
          Dload  Upload   Total Spent  Left  Speed
100 1673K  100 1673K    0     0  13.5M    0 --:--:-- --:--:-- 13.6M
18.206.107.24/29
voclabs:~/environment $
```

If we test from the cloud9 instance again, it will still not work.

```
voclabs:~/environment $
voclabs:~/environment $ nc -vz 54.146.76.192 80
^C
voclabs:~/environment $ nc -vz 54.146.76.192 22
^C
voclabs:~/environment $
```

So I added route in the route table that is associated with the web server instance to route traffic through the internet gateway

The screenshot shows the AWS VPC Route Tables interface. A new route table named 'rtb-0bc86dae57191a490' has been created. The 'Details' tab is selected, showing the route table ID, VPC ID, and other basic information. The 'Routes' tab is active, displaying two routes:

Destination	Target	Status	Propagated
0.0.0.0/0	igw-08ff7f4a372b453cb3	Active	No
10.1.0.0/16	local	Active	No

|

And now it succeeded

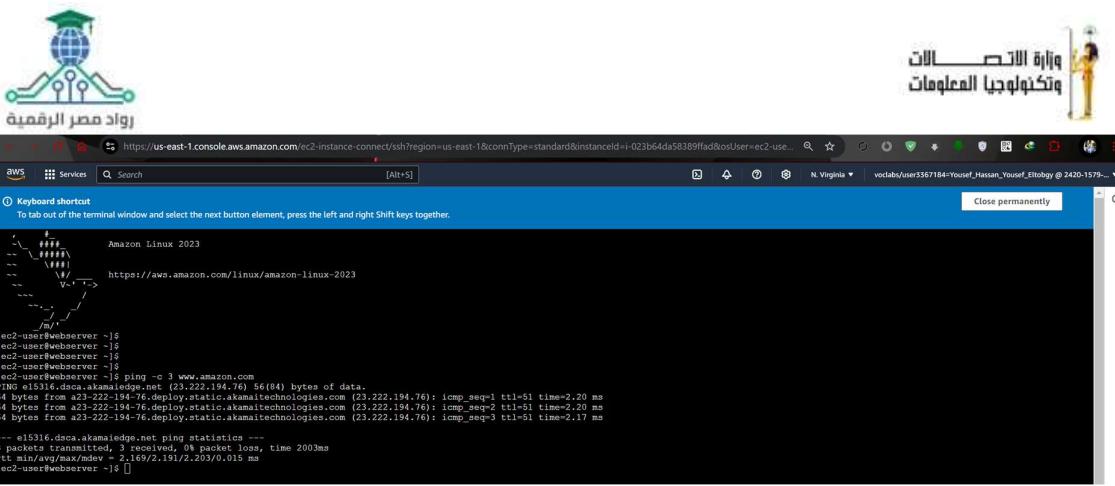
```
voclabs:~/environment $
voclabs:~/environment $ nc -vz 54.146.76.192 80
Connection to 54.146.76.192 port [tcp/http] succeeded!
voclabs:~/environment $
```

And we can access the webserver from the browser window



Hello world from WebServer!

And the SSH is working too through EC2 instance connect



## Task 2.5: Secure the WebServerSubnet with a network ACL

If I edited the rule number 100 from allow to deny the connection through port 22 will fail.

Inbound rules (2)						
<input type="text" value="Filter inbound rules"/> <span style="float: right;">Edit inbound rules</span>						
Rule number	Type	Protocol	Port range	Source	Allow/Deny	
100	SSH (22)	TCP (6)	22	0.0.0.0/0	<input checked="" type="radio"/> Deny	
*	All traffic	All	All	0.0.0.0/0	<input checked="" type="radio"/> Deny	

And it really failed from the cloud9 instance.

```

voclabs:~/environment $ 
voclabs:~/environment $ nc -vz 54.146.76.192 22
^C
voclabs:~/environment $ 

```

So now we allow the traffic on ports 80 and 22 in the NACL.

Inbound rules (3)						
<input type="text" value="Filter inbound rules"/> <span style="float: right;">Edit inbound rules</span>						
Rule number	Type	Protocol	Port range	Source	Allow/Deny	
90	HTTP (80)	TCP (6)	80	0.0.0.0/0	<input checked="" type="radio"/> Allow	
100	SSH (22)	TCP (6)	22	0.0.0.0/0	<input checked="" type="radio"/> Allow	
*	All traffic	All	All	0.0.0.0/0	<input checked="" type="radio"/> Deny	

And connection worked again fine.



```
vclabs:~/environment $ nc -vz 54.146.76.192 80
Connection to 54.146.76.192 port [tcp/http] succeeded!
vclabs:~/environment $
```

## Task 2.6: Review NetworkFirewallVPC and its associated resources

Here we have the below properties in the VPC named NetworkFirewallVPC.

The screenshot shows the AWS VPC console for the VPC named 'NetworkFirewallVPC'. In the 'Details' tab, it lists various configuration parameters such as VPC ID (vpc-021ceeed0c7f8d510), State (Available), DHCP option set (dopt-032becb57d7ca3b8d), and Main route table (rtb-08ef05f6b6caeaff18). The 'Resource map' tab displays the network topology, showing a VPC connected to two Subnets (us-east-1a and us-east-1a) via a Route table (rtb-08ef05f6b6caeaff18), which then connects to a single Network connection (NetworkFirewallIG).

The NACL of the two subnets allow all traffic.

The screenshot shows the AWS Network ACL console for two Network ACLs: 'Network ACL: acl-045df48ede81b22bf' and 'Network ACL: acl-045df48ede81b22bf'. Both ACLs have 2 inbound and 2 outbound rules. All rules allow all traffic (All traffic, All protocol, All port range, All source/destination) and are set to 'Allow'. The 'Edit network ACL association' button is visible for both.

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny
Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny



This WebServer2 instance is deployed in this VPC and it is reachable fine.

Hello world from WebServer2!

The below are the rules in its security group

Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
-	sgr-03115915e67c7fdb49	8080	TCP	0.0.0.0/0	<a href="#">WebServer2SecurityGroup</a>	-
-	sgr-07ba8e78fd8c81a04	22	TCP	0.0.0.0/0	<a href="#">WebServer2SecurityGroup</a>	-
-	sgr-0da8472ff85a145cd	80	TCP	0.0.0.0/0	<a href="#">WebServer2SecurityGroup</a>	-

And connection is working fine from the cloud9

```
voclabs:~/environment $ 
voclabs:~/environment $ nc -vz 98.82.64.232 80
Connection to 98.82.64.232 80 port [tcp/http] succeeded!
voclabs:~/environment $ 
voclabs:~/environment $ 
voclabs:~/environment $ nc -vz 98.82.64.232 22
Connection to 98.82.64.232 22 port [tcp/ssh] succeeded!
voclabs:~/environment $ 
```

I will now test the connection on port 80 so I have to run the below command in the WebServer2 instance.

```
'~\_\_ #####_          Amazon Linux 2023
~~ \_\_ #####\_
~~ \#\#\#
~~ \#/ ,--> https://aws.amazon.com/linux/amazon-linux-2023
~~ V~,-->
~~~ /
~~ . / /
~/ ,/
[ec2-user@webserver2 ~]$ 
[ec2-user@webserver2 ~]$ 
[ec2-user@webserver2 ~]$ 
[ec2-user@webserver2 ~]$ 
[ec2-user@webserver2 ~]$ 
[ec2-user@webserver2 ~]$ python3 -m http.server 8080 &
[1] 4857
[ec2-user@webserver2 ~]$ Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080) ...
154.180.126.184 - - [07/Oct/2024 15:38:00] "GET / HTTP/1.1" 200 -
154.180.126.184 - - [07/Oct/2024 15:38:00] code 404, message File not found
154.180.126.184 - - [07/Oct/2024 15:38:00] "GET /favicon.ico HTTP/1.1" 404 -
```

And then it will work fine.



الإلكترونية  
نحوه المعلومات

← → G ⌂ Not secure http://98.82.64.232:8080

Hello world from WebServer2 port 8080!

### **Task 2.7: Create a network firewall**

I created the below firewall in the us-east-1a Availability Zone for FirewallSubnet and IP address type IPv4. And Named the firewall policy as FirewallPolicy.

The screenshot shows the AWS VPC Network Firewall interface. A new NetworkFirewall named "NetworkFirewall" has been created. It is associated with a VPC "vpc-021ceeed0c7f8d510" and a Firewall Policy "FirewallPolicy". The firewall status is "Ready". The "Firewall details" tab is selected, showing the name "NetworkFirewall" and a description "-". The "VPC" tab shows the associated VPC and its subnets. The "Firewall endpoints" tab lists one endpoint in the "us-east-1a" availability zone, which is also marked as "Ready".

Availability Zone	Firewall subnet	Endpoint ID	Firewall endpoint status
us-east-1a	subnet-09a87ecd1b3753f5d	vpce-0befce856cc0ece8	Ready

### **Task 2.8: Create route tables**

Created the below route tables and added route where I set the destination to be the CIDR block of the subnet that the WebServer2 instance runs in, and I set the target to the only Gateway Load Balancer Endpoint that is available.

VPC > Route tables > rtb-0eac8e590cb079913

### rtb-0eac8e590cb079913 / IGW-Ingress-Route-Table

**Details Info**

Route table ID rtb-0eac8e590cb079913	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-021ceeded0c7f8d510   NetworkFirewallVPC	Owner ID 242015798764		

**Routes (2)**

Destination	Target	Status	Propagated
10.1.0.0/16	local	Active	No
10.1.3.0/28	vpc-e0befce856cc0ece8	Active	No

I then added an edge association to the IGW-Ingress-Route-Table so that the NetworkFirewallIG internet gateway is associated with the route table.

VPC > Route tables > rtb-0eac8e590cb079913

### rtb-0eac8e590cb079913 / IGW-Ingress-Route-Table

**Details Info**

Route table ID rtb-0eac8e590cb079913	Main No	Explicit subnet associations -	Edge associations igw-0b8d5c219e382a77d / NetworkFirewallIG
VPC vpc-021ceeded0c7f8d510   NetworkFirewallVPC	Owner ID 242015798764		

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

**Associated internet gateways (1)**

ID	State	VPC	Owner
igw-0b8d5c219e382a77d / NetworkFirewallIG	Attached	vpc-021ceeded0c7f8d510	242015798764

I then created a new route table.

VPC > Route tables > rtb-083f19f73618c9c23

### rtb-083f19f73618c9c23 / Firewall-Route-Table

**Details Info**

Route table ID rtb-083f19f73618c9c23	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-021ceeded0c7f8d510   NetworkFirewallVPC	Owner ID 242015798764		

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

**Routes (2)**

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0b8d5c219e382a77d	Active	No
10.1.0.0/16	local	Active	No

Then I associated it with the subnet named “FirewallSubnet”.



رواد مصر الرقمية

VPC > Route tables > rtb-083f19f73618c9c23

### rtb-083f19f73618c9c23 / Firewall-Route-Table

**Details** **Info**

Route table ID rtb-083f19f73618c9c23	Main No	Explicit subnet associations subnet-09a87ecd1b3753f5d / FirewallSubnet	Edge associations -
VPC vpc-021ceeed0c7f8d510   NetworkFirewallVPC	Owner ID 242015798764		

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

**Explicit subnet associations (1)**

Edit subnet associations			
< 1 > ⌂			
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
FirewallSubnet	subnet-09a87ecd1b3753f5d	10.1.0.0/28	-

**Subnets without explicit associations (0)**

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Edit subnet associations			
< 1 > ⌂			
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
WebServer2Subnet	subnet-07472e5359d17dd57	10.1.3.0/28	-

Then I created another route table named "WebServer2-Route-Table". And added a route so that 0.0.0.0/0 traffic is routed to the Gateway Load Balancer Endpoint.

VPC > Route tables > rtb-0f9c136486b91873a

### rtb-0f9c136486b91873a / WebServer2-Route-Table

**Details** **Info**

Route table ID rtb-0f9c136486b91873a	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-021ceeed0c7f8d510   NetworkFirewallVPC	Owner ID 242015798764		

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

**Routes (2)**

Both Edit routes			
< 1 > ⌂			
Destination	Target	Status	Propagated
0.0.0.0/0	vpc-e856cc0ece8	Active	No
10.1.0.0/16	local	Active	No

Then created association between the "Webserver2Subnet" subnet and the route table

VPC > Route tables > rtb-0f9c136486b91873a

### rtb-0f9c136486b91873a / WebServer2-Route-Table

**Details** **Info**

Route table ID rtb-0f9c136486b91873a	Main No	Explicit subnet associations subnet-07472e5359d17dd57 / WebServer2Subnet	Edge associations -
VPC vpc-021ceeed0c7f8d510   NetworkFirewallVPC	Owner ID 242015798764		

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

**Explicit subnet associations (1)**

Edit subnet associations			
< 1 > ⌂			
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
WebServer2Subnet	subnet-07472e5359d17dd57	10.1.3.0/28	-

**Subnets without explicit associations (0)**

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Edit subnet associations			
< 1 > ⌂			
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
No subnets without explicit associations			
All your subnets are associated with a route table.			



## Task 2.9: Configure logging for the network firewall

I created a log group

The screenshot shows the AWS CloudWatch Log Groups interface. At the top, there are navigation links: CloudWatch > Log groups > NetworkFirewallVPCLogs. To the right are buttons for Actions, View in Logs Insights, Start tailing, and Search log group. Below this is a table titled "Log group details" with columns for Log class (Info), ARN (arn:aws:logs:us-east-1:242015798764:log-group:NetworkFirewallVPCLogs:\*, Standard), Creation time (Now), and Retention (6 months). On the right side of the table, there are sections for Stored bytes (0), Metric filters (0), Subscription filters (0), Contributor Insights rules (0), KMS key ID (-), Anomaly detection (Configure), Data protection (-), and Sensitive data count (-). Below the table are tabs for Log streams, Tags, Anomaly detection, Metric filters, Subscription filters, Contributor Insights, and Data protection. The "Log streams" tab is selected, showing a section titled "Log streams (0)" with a search bar, filter options (Exact match, Show expired), and a message stating "There are no log streams."

I then configured logging in the firewall that we created.

The screenshot shows the AWS Network Firewall Logging configuration page. At the top left is a "Logging" section with the subtext "Network Firewall generates logs for stateful rule groups. You can configure different destinations for different log types." To the right is an "Edit" button. Below this are four destination configurations: Log type (Flow, Alert), Alert log destination (CloudWatch log group - NetworkFirewallVPCLogs), Flow log destination (CloudWatch log group - NetworkFirewallVPCLogs), and TLS log destination (Not configured).

The webserver2 will not be accessible. This is expected because the network firewall policy isn't yet configured to allow HTTP traffic on port 80.

The screenshot shows a browser window with the URL http://98.82.64.232. The page displays a "This site can't be reached" error message. It states "The connection was reset." and "Try:" followed by three suggestions: "Checking the connection", "Checking the proxy and the firewall", and "Running Windows Network Diagnostics". Below the message is the error code ERR\_CONNECTION\_RESET. At the bottom are "Reload" and "Details" buttons.

And we can check the logs in the cloudwatch log group "NetworkFirewallVPCLogs".

CloudWatch > Log groups > NetworkFirewallVPCLogs > All events

**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
2024-10-07T16:34:01.000Z	{"firewall_name": "NetworkFirewall", "availability_zone": "us-east-1a", "event_timestamp": "...", "log_stream_created_by": "aws_to_validate_log_delivery_subscriptions", "log_stream_name": "/aws/network-firewall/flow/NetworkFirewall_2024-10-07-16", "log_stream_status": "VALIDATED", "log_stream_version": "1", "log_type": "AWS", "source": "aws_to_validate_log_delivery_subscriptions", "version": "1"} Permissions are set correctly to allow AWS CloudWatch Logs to write into your log while NetworkFirewall is validating its log delivery subscriptions.	/aws/network-firewall/flow/NetworkFirewall_2024-10-07-16
2024-10-07T16:34:05.479Z	{...}	log_stream_created_by_aws_to_validate_log_delivery_subscriptions
2024-10-07T16:34:09.000Z	{...}	/aws/network-firewall/flow/NetworkFirewall_2024-10-07-16
2024-10-07T16:34:10.000Z	{...}	/aws/network-firewall/flow/NetworkFirewall_2024-10-07-16
2024-10-07T16:34:10.000Z	{...}	/aws/network-firewall/flow/NetworkFirewall_2024-10-07-16
2024-10-07T16:34:19.000Z	{...}	/aws/network-firewall/flow/NetworkFirewall_2024-10-07-16
2024-10-07T16:34:21.000Z	{...}	/aws/network-firewall/flow/NetworkFirewall_2024-10-07-16

## Task 2.10: Configure the firewall policy and test access

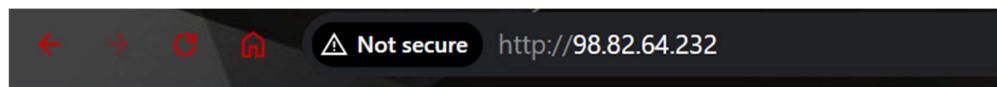
I then created a stateful route group in the firewall policy to allow connection on port 80, 22, 443 and ICMP protocol, but I set it to reject connection on port 8080.

Stateful rule groups (1)					Actions
	Priority	Name	Capacity	Is managed?	Run in alert mode?
	1	NetworkFirewallVPCRuleGroup	100	No	Not available

Here are the rules.

Rules (5)										Edit
Description	Geo IP	Protocol	Source	Destination	Destination port	Direction	Action	Keyword		
-	-	TCP	ANY	ANY	8080	Forward	Drop	sid:2		
-	-	TCP	ANY	ANY	80	Forward	Pass	sid:3		
-	-	TCP	ANY	ANY	22	Forward	Pass	sid:4		
-	-	TCP	ANY	ANY	443	Forward	Pass	sid:5		
-	-	ICMP	ANY	ANY	ANY	Forward	Pass	sid:6		

And now the WebServer2 is accessible again. The below is on port 80.



Hello world from WebServer2!

Here the below is on port 22 and it says successful from the cloud9 instance.

```
voclabs:~/environment $ nc -vz 98.82.64.232 22
Connection to 98.82.64.232 22 port [tcp/ssh] succeeded!
voclabs:~/environment $
```

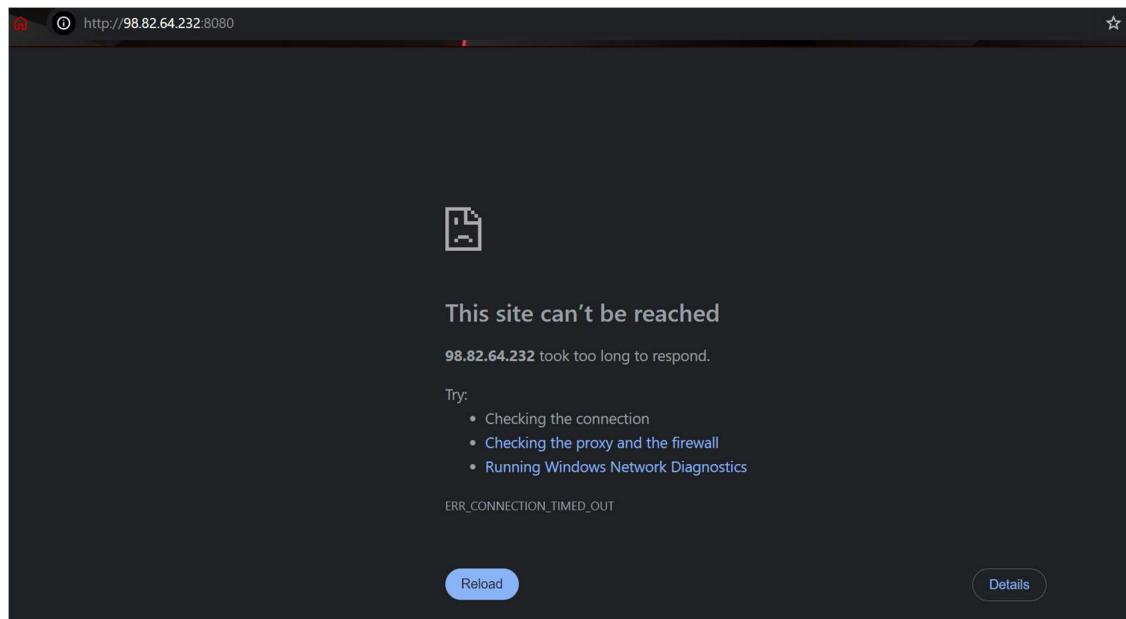
The ICMP is also working fine and we can see the active ports that the WebServer2 instance is listening to.



```
[ec2-user@webserver2 ~]$ 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=56 time=3.29 ms
64 bytes from 162.219.225.118 (162.219.225.118): icmp_seq=2 ttl=56 time=3.28 ms
64 bytes from 162.219.225.118 (162.219.225.118): icmp_seq=3 ttl=56 time=2.67 ms

--- www-amazon-com.customer.fastly.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.665/3.077/3.285/0.291 ms
[ec2-user@webserver2 ~]$ sudo netstat -tulpn | grep -i listen
tcp        0      0 0.0.0.0:22              0.0.0.0:*          LISTEN      2326/sshd: /usr/sbi
tcp        0      0 0.0.0.0:8080            0.0.0.0:*          LISTEN      4857/python3
tcp6       0      0 ::1:22                ::*:*           LISTEN      2326/sshd: /usr/sbi
tcp6       0      0 ::1:80                ::*:*           LISTEN      1993/httpd
[ec2-user@webserver2 ~]$
```

And if we tried to access on port 8080, the connection will fail because of the firewall rule.



## **Cost estimate to secure a VPC with a network firewall**

We need to get the estimated cost for the below data

CRITERIA	ESTIMATE PER MONTH
EC2 - WebServer2	1 On-demand (Shared Instance, 100% usage)
VPC - NetworkFirewallVPC	1 IPAM
Inbound data transfer from (internet free)	100 GB
Outbound data transfer to (US East, N. Virginia) - outbound not Intra-Region	1 TB
Network firewall - number of endpoints	1
Network firewall - usage per endpoint	30 days
Network firewall - data processed per month	2.0 TB



So, here is the cost estimate:

AWS Pricing Calculator > My Estimate

My Estimate [Edit](#)

Estimate summary [Info](#)

Upfront cost 0.00 USD	Monthly cost 421.95 USD	Total 12 months cost <b>5,063.40 USD</b> Includes upfront cost
--------------------------	----------------------------	--

Getting Started with AWS

[Get started for free](#) [Contact Sales](#)

My Estimate

<input type="checkbox"/> Service Name	Status	Upfront cost	Monthly cost	Description	Region	Config Summary
Amazon Virtual Private Cloud	-	0.00 USD	0.20 USD	-	US East (N. Virginia)	Number of active IP addresses...
AWS Network Firewall	-	0.00 USD	417.52 USD	-	US East (N. Virginia)	Number of AWS Network...
Amazon EC2	-	0.00 USD	4.23 USD	-	US East (N. Virginia)	Tenancy (Shared Instance...)

Duplicate Delete Move to Create group Add support Add service

Here is the cost estimate in the pdf format.

Export date: 10/7/2024 Language: English

Estimate URL: <https://calculator.aws/#/estimate?id=56d9639499ef1e1b45993e9079d27127a33df9ee>

Estimate summary				
Upfront cost	Monthly cost	Total 12 months cost		
<b>0.00 USD</b>	<b>421.95 USD</b>	<b>5,063.40 USD</b>		
Includes upfront cost				

#### Detailed Estimate

Name	Group	Region	Upfront cost	Monthly cost
Amazon Virtual Private Cloud (VPC)	No group applied	US East (N. Virginia)	0.00 USD	0.20 USD
<b>Status:</b> -				
<b>Description:</b>				
<b>Config summary:</b> Number of active IP addresses (1)				
AWS Network Firewall	No group applied	US East (N. Virginia)	0.00 USD	417.52 USD
<b>Status:</b> -				
<b>Description:</b>				
<b>Config summary:</b> Number of AWS Network Firewall endpoints (1), Usage per endpoint (30 days), Data processed per month (2 TB)				
Amazon EC2	No group applied	US East (N. Virginia)	0.00 USD	4.23 USD
<b>Status:</b> -				
<b>Description:</b>				
<b>Config summary:</b> Tenancy (Shared Instances), Operating system (Linux), Workload (Consistent, Number of instances: 1), Advance EC2 instance (t2.micro), Pricing strategy (Compute Savings Plans 3yr No Upfront), Enable monitoring (disabled), DT Inbound: Internet (100 GB per month),				



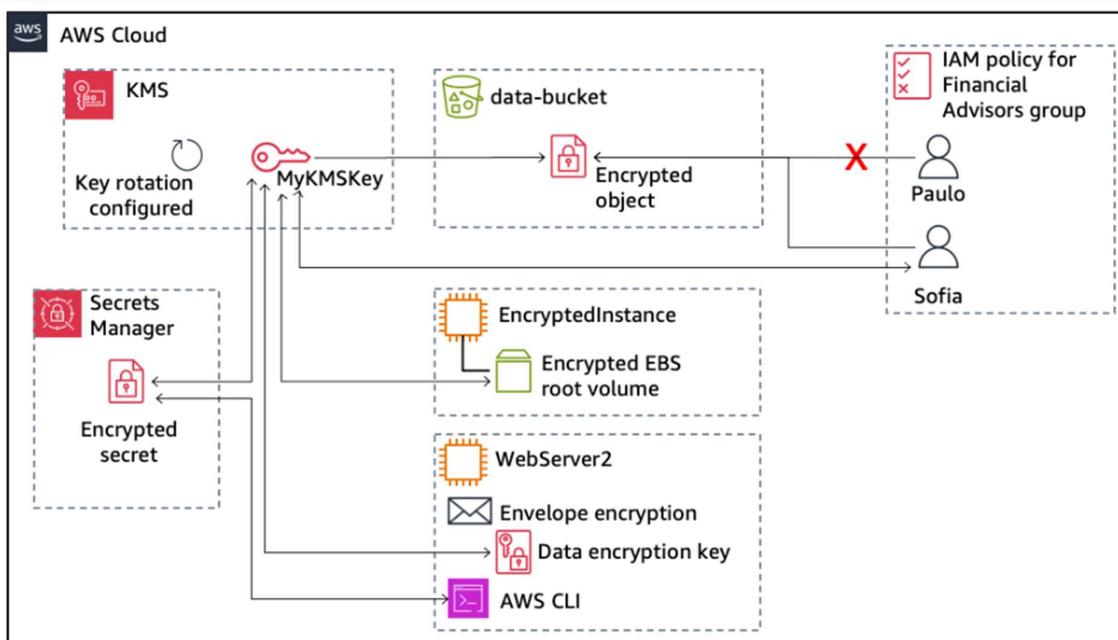
الإذاعة والتلفزيون  
الإذاعة والتلفزيون

Here is it in the csv format.

Estimate summary						
Upfront	Monthly	Total	12 m	Currency	Status	Configuration summary
0	421.95	5063.4	USD			* Includes upfront cost
Detailed Estimate						
Group hier Region Description Service Upfront Monthly First 12 m Currency Status Configuration summary						
My Estima US East (N. Virginia) IPAM 0 0.2 24 USD Number of active IP addresses (1)						
My Estima US East (N. Virginia) AWS Netw 0 417.52 5010.24 USD Number of AWS Network Firewall endpoints (1), Usage per endpoint (30 days), Data processed per month (2 TB)						
My Estima US East (N. Virginia) Amazon EC 0 4.234 50.81 USD Tenancy (Shared Instances), Operating system (Linux), Workload (Consistent, Number of instances: 1), Advance EC2 instance (t2.micro), Pricing strategy (Compute Savings Plans 3yr No						
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

By the end of this phase, you will have created the architecture that is shown in the following diagram.



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

Created a new key and granted the Key administrator and Key user permissions to the voclabs role

A screenshot of the AWS KMS 'Customer-managed keys' page. It shows a table with one row for 'MyKMSKey'. The table includes columns for Aliases, Key ID, Status, Key type, Key spec, and Key usage. The key is enabled, symmetric, and has a usage of 'Encrypt and decrypt'. There are buttons for 'Key actions' and 'Create key' at the top right.

I then enabled the automatic key rotation. So that it is automatically rotated every year.



وزارة الاتصالات  
وتقنيات المعلومات

KMS > Customer-managed keys > Key ID: cf00f35b-e905-46c4-bc61-d4e0cf34b195

cf00f35b-e905-46c4-bc61-d4e0cf34b195

Key actions ▾ Edit

#### General configuration

Alias  
MyKMSKey

Status  
Enabled

Creation date  
Oct 07, 2024 20:53 EEST

ARN

Description

Regionality  
Single region

arn:aws:kms:us-east-1:242015798764:key/cf00f35b-e905-46c4-bc61-d4e0cf34b195

Key policy Cryptographic configuration Tags Key rotation Aliases

#### Automatic key rotation Info

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

Edit

Status  
 Enabled

Rotation period  
365

Date of last automatic rotation  
-

Next rotation date  
Oct 07, 2025

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

Added user named Sofia to the key administrators

KMS > Customer-managed keys > Key ID: cf00f35b-e905-46c4-bc61-d4e0cf34b195

cf00f35b-e905-46c4-bc61-d4e0cf34b195

Key actions ▾ Edit

#### General configuration

Alias  
MyKMSKey

Status  
Enabled

Creation date  
Oct 07, 2024 20:53 EEST

ARN

Description

Regionality

arn:aws:kms:us-east-1:242015798764:key/cf00f35b-e905-46c4-bc61-d4e0cf34b195

Key policy Cryptographic configuration Tags Key rotation Aliases

#### Key policy

Switch to policy view

##### Key administrators (1/2)

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 roles to administer this key from this console. [Learn more](#)

Add Remove

Search Key administrators

< 1 >

Name	Path	Type
voclabs	/	Role
<input checked="" type="checkbox"/> sofia	/	User

And here it is modified in the configuration



Key policy    Cryptographic configuration    Tags    Key rotation    Aliases

### Key policy

```
},
  "Action": "kms:*",
  "Resource": "*"
},
{
  "Sid": "Allow access for Key Administrators",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::242015798764:role/voclabs",
      "arn:aws:iam::242015798764:user/sofia"
    ]
  },
}
```

I analyzed the policy named “PolicyForFinancialAdvisors”, It is configured to allow full actions on S3 (like PUT, GET, etc.) and also allow some actions, like: encrypt, decrypt, etc.

### Modify permissions in PolicyForFinancialAdvisors [Info](#)

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

#### Policy editor

```
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Action": [
6         "s3:GetAccountPublicAccessBlock",
7         "s3:GetBucketAcl",
8         "s3:GetBucketPolicyStatus",
9         "s3:GetBucketPublicAccessBlock",
10        "s3:GetObject",
11        "s3:ListAccessPoints",
12        "s3:ListAllBuckets",
13        "s3:ListBucket",
14        "s3:PutObject"
15      ],
16      "Resource": "arn:aws:s3:::*",
17      "Effect": "Allow"
18    },
19    {
20      "Action": [
21        "kms:Encrypt",
22        "kms:Decrypt",
23        "kms:DescribeKey",
24        "kms:GenerateDataKey"
25      ],
26      "Resource": "*",
27      "Effect": "Allow"
28    }
29 ]
```

Visual

JSON

Actions ▾



Edit statement

Select a statement

Select an existing statement in the policy or  
add a new statement.

+ Add new statement

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

Modified the encryption settings on the data-bucket S3 bucket so that the bucket uses SSE-KMS encryption.

#### Default encryption [Info](#)

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

Edit

#### Encryption type [Info](#)

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

#### Encryption key ARN

[arn:aws:kms:us-east-1:242015798764:key/cf00f35b-e905-46c4-bc61-d4e0cf34b195](#)

#### 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



Created a file named “loan-data.csv” with the below data.

1	date	description	amount	principal	interest
2	1/14/2023	payment	1000	845.52	154.48
3	12/22/2022	payment	1021.52	742.8	278.72
4	11/15/2022	payment	1000	855.27	144.73

I uploaded it to the S3 bucket using the user named “Sofia”.

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with 'Services' and a search bar. Below that, the path 'Amazon S3 > Buckets > data-bucket-08f7f4a372b453cb3' is shown. The main area is titled 'data-bucket-08f7f4a372b453cb3 Info'. Under the 'Objects' tab, there's a table listing three objects:

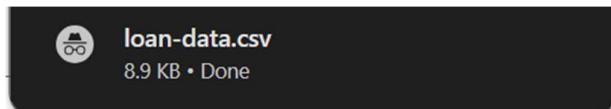
Name	Type	Last modified	Size	Storage class
customers.csv	csv	October 6, 2024, 22:49:25 (UTC+0:00)	8.7 KB	Standard
<b>loan-data.csv</b>	csv	October 9, 2024, 13:38:34 (UTC+0:00)	8.9 KB	Standard
myfile.txt	txt	October 7, 2024, 13:51:50 (UTC+0:00)	11.0 B	Standard

And The encryption type for the object is SSE-KMS.

The screenshot shows the 'Server-side encryption settings' for the 'loan-data.csv' object. It includes the following details:

- Encryption type:** SSE-KMS
- Encryption key ARN:** [arn:aws:kms:us-east-1:242015798764:key/cf00f35b-e905-46c4-bc61-d4e0cf34b195](#)
- Bucket Key:** Enabled

I successfully downloaded the file using the user Sofia. This means that the user can retrieve the KMS key and detect the file on S3 bucket and download the file in plain text.



If I try to open the file using the user Paulo, it will result in error and tell me the user is not authorized to perform: kms:Decrypt on resource.

```
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::242015798764:user/paulo is not authorized to perform: kms:Decrypt on resource: arn:aws:kms:us-east-1:242015798764:key/cf00f35b-e905-46c4-bc61-d4e0cf34b195 because no identity-based policy allows the action 'kms:Decrypt' on the resource with ID 'arn:aws:kms:us-east-1:242015798764:key/cf00f35b-e905-46c4-bc61-d4e0cf34b195'.</Message>  
  <RequestId>405C7DEA-SASH-4D9D-85C9-044r2RCJT0z5vyAdTJ8YQaAXEMc2DHq5e+JClvwL9sY6yntip25qv8=</RequestId>  
</Error>
```

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



I created new EC2 instance and enabled encryption on its AMI root volume by using MyKMSKey.

EC2 > Instances > i-03071291af5783287

### Instance summary for i-03071291af5783287 (EncryptedInstance) [Info](#)

Updated less than a minute ago

Instance ID	Public IPv4 address	Private IPv4 addresses
i-03071291af5783287 (EncryptedInstance)	3.236.163.130   <a href="#">open address</a>	10.1.3.8
IPv6 address	Instance state	Public IPv4 DNS
-	<span>Running</span>	ec2-3-236-163-130.compute-1.amazonaws.com   <a href="#">open address</a>
Hostname type	Private IP DNS name (IPv4 only)	Elastic IP addresses
IP name: ip-10-1-3-8.ec2.internal	ip-10-1-3-8.ec2.internal	-
Answer private resource DNS name	Instance type	AWS Compute Optimizer finding
-	t2.micro	<a href="#">Opt-in to AWS Compute Optimizer for recommendations.</a>   <a href="#">Learn more</a>
Auto-assigned IP address	VPC ID	Auto Scaling Group name
3.236.163.130 [Public IP]	vpc-021ceeed0c7f8d510 (NetworkFirewallVPC)	-
IAM Role	Subnet ID	
<a href="#">WebServerRole</a>	subnet-07472e5359d17dd57 (WebServer2Subnet)	
IMDSv2	Instance ARN	
Required	arn:aws:ec2:us-east-1:242015798764:instance/i-03071291af5783287	

[Details](#) | [Status and alarms](#) | [Monitoring](#) | [Security](#) | [Networking](#) | **Storage** | [Tags](#)

**Root device details**

Root device name	Root device type	EBS optimization
/dev/xvda	EBS	disabled

**Block devices**

<input type="text"/> Filter block devices	Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encrypted	KMS key ID	Delete on termi
<input checked="" type="checkbox"/>	Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encrypted	KMS key ID	Delete on termi
<input checked="" type="checkbox"/>	vol-066345312c5e416ef	/dev/xvda	8	Attaching	2024/10/09 13:52 GMT+3	Yes	cf00f35b-e905-46c4-bc61-d4e0cf34b195	Yes

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

I connected to the webserver2 instance and created a file in it.

```
[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 ~]$
```

I listed all the AWS KMS keys in the account using the below command.

```
[ec2-user@webserver2 ~]$ aws kms list-keys
{
    "Keys": [
        {
            "KeyId": "71752706-a4ac-4d09-ae82-8797c1307811",
            "KeyArn": "arn:aws:kms:us-east-1:242015798764:key/71752706-a4ac-4d09-ae82-8797c1307811"
        },
        {
            "KeyId": "cf00f35b-e905-46c4-bc61-d4e0cf34b195",
            "KeyArn": "arn:aws:kms:us-east-1:242015798764:key/cf00f35b-e905-46c4-bc61-d4e0cf34b195"
        },
        {
            "KeyId": "d9010741-21da-44b2-bae1-3b0ab7031e05",
            "KeyArn": "arn:aws:kms:us-east-1:242015798764:key/d9010741-21da-44b2-bae1-3b0ab7031e05"
        }
    ]
}
[ec2-user@webserver2 ~]$ 
```

I ran the following commands to generate a data key for the MyKMSKey, saved it to a bash variable, and then echoed the data key details in JSON format:



```
[ec2-user@webserver2 ~]$ result=$(aws kms generate-data-key --key-id alias/MyKMSKey --key-spec AES_256)
[ec2-user@webserver2 ~]$ echo $result | python3 -m json.tool
[{"Plaintext": "B845v2jNlGbmCNb6wfxr8TUpqrmAMCSMN9oB", "KeyId": "arn:aws:kms:us-east-1:242015798764:key/e0f035b-e905-46cb-bc61-d4e0cf34b195"}]
[ec2-user@webserver2 ~]$
```

Then to save the data key to disk. First I export the CiphertextBlob value from the result and save it to a text file in base64-encoded format,

```
[ec2-user@wbeverse2 ~]$ dk_cipher=$(/bin/sh -c $(echo $res1 | jq '.CiphertextBlob' | cut -d '"' -f2))
[ec2-user@wbeverse2 ~]$ echo $dk_cipher
[ec2-user@wbeverse2 ~]$ echo $dk_cipher
[ec2-user@wbeverse2 ~]$ base64 -d $dk_cipher > data_key_ciphertext
[ec2-user@wbeverse2 ~]$ echo $dk_cipher | base64 --decode > data_key_ciphertext
[ec2-user@wbeverse2 ~]$
```

then to see that the data key is stored in encrypted (not human-readable) format:

To view it in clear text (human-readable) format:

```
[ec2-user@webserver2 ~]$ aws kms decrypt --ciphertext-blob fileb://./data_key_ciphertext --query Plaintext --output text  
BBu4SyRZjVh1NGhMnBe60wxP+8TUfq0rmACS+MNW08=  
[ec2-user@webserver2 ~]$
```

To save the result to a file in base64-encoded format

```
[ec2-user@webserver2 ~]$ aws kms decrypt --ciphertext-blob file:///data/key/ciphertext --query Plaintext --output text | base64 --decode > data_key_plaintext_encrypted
[ec2-user@webserver2 ~]$
```

Then I will use the data key to encrypt the file that I created earlier, and delete the unencrypted version of the file.

```
[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__XXXXXXXXXXXXXXg0X0xMXXXXXXXXXXXXXX[ec2-user@webserver2 ~]$  
[ec2-user@webserver2 ~]$  
[ec2-user@webserver2 ~]$ rm data_unencrypted.txt  
[ec2-user@webserver2 ~]$
```

Then I will decrypt the file to prove that the data is retrievable.

```
[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 ~]$  
[ec2-user@webserver2 ~]$ cat data_decrypted.txt  
Let's encrypt these file contents. Sensitive data here.  
[ec2-user@webserver2 ~]$  
[ec2-user@webserver2 ~]$ █
```

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

Created a new secret



AWS Secrets Manager > Secrets > mysecret

mysecret

Secret details	
Encryption key MyKMSKey	Secret description -
Secret name mysecret	
Secret ARN arn:aws:secretsmanager:us-east-1:242015798764:secret:mysecret-cts9r5	

Then I used EC2 Instance Connect to connect to the WebServer2 instance, and then used the AWS CLI to retrieve the secret.

```
[ec2-user@webserver2 ~]$ aws secretsmanager list-secrets
{
    "SecretList": [
        {
            "ARN": "arn:aws:secretsmanager:us-east-1:242015798764:secret:mysecret-cts9r5",
            "Name": "mysecret",
            "KmsKeyId": "arn:aws:kms:us-east-1:242015798764:key/cf00f35b-e905-46c4-bc61-d4e0cf34b195",
            "LastChangedDate": "2024-10-09T11:24:51.955000+00:00",
            "LastAccessedDate": "2024-10-09T00:00:00+00:00",
            "Tags": [],
            "SecretVersionsToStages": {
                "50e02c16-edd3-49cf-8e8f-246a3ed18a78": [
                    "AWSCURRENT"
                ],
                "CreatedDate": "2024-10-09T11:24:51.879000+00:00"
            }
        }
    ]
}
[ec2-user@webserver2 ~]$ aws secretsmanager get-secret-value --secret-id mysecret
{
    "ARN": "arn:aws:secretsmanager:us-east-1:242015798764:secret:mysecret-cts9r5",
    "Name": "mysecret",
    "VersionId": "50e02c16-edd3-49cf-8e8f-246a3ed18a78",
    "SecretString": "{\"secret\":\"my secret data\"}",
    "VersionStages": [
        "AWSCURRENT"
    ],
    "CreatedDate": "2024-10-09T11:24:51.943000+00:00"
}
```

## Cost assessment for using AWS KMS



AWS Pricing Calculator > My Estimate

## My Estimate [Edit](#)

[Export](#) [Share](#)

### Estimate summary [Info](#)

Upfront cost  
0.00 USD

Monthly cost  
11.12 USD

Total 12 months cost  
**133.44 USD**  
Includes upfront cost

### Getting Started with AWS

[Get started for free](#)

[Contact Sales](#)

### My Estimate

[Duplicate](#) [Delete](#) [Move to](#) [Create group](#) [Add support](#) [Add service](#)

< 1 > ⌂

Find resources

<input type="checkbox"/>	Service Name	Status	Upfront cost	Monthly cost	Description	Region	Config Summary
<input type="checkbox"/>	AWS Key Management Se...	-	0.00 USD	1.60 USD	-	US East (N. Virginia)	Number of customer ma...
<input type="checkbox"/>	AWS Secrets Manager	-	0.00 USD	0.41 USD	-	US East (N. Virginia)	Number of secrets (1), Av...
<input type="checkbox"/>	Amazon Simple Storage ...	-	0.00 USD	0.00 USD	-	US East (N. Virginia)	S3 Standard storage (0.0...
<input type="checkbox"/>	Amazon EC2	-	0.00 USD	9.11 USD	-	US East (N. Virginia)	Tenancy (Shared Instance...

Here it is in csv format

Estimate summary	Upfront cost	Monthly cost	Total 12 m	Currency	
	0	11.12	133.44	USD	
* Includes upfront cost					
<b>Detailed Estimate</b>					
Group hier Region Description Service Upfront Monthly First 12 m Currency Status Configuration summary					
My Estimate: US East (N. Virginia) AWS Key M 0 1.6 19.2 USD Number of customer managed Customer Master Keys (CMK) (1), Number of symmetric requests (200000)					
My Estimate: US East (N. Virginia) AWS Secret 0 0.41 4.92 USD Number of secrets (1), Average duration of each secret (30 days), Number of API calls (2000 per month)					
My Estimate: US East (N. Virginia) S3 Standard 0 0 0 USD S3 Standard storage (0.01 GB per month)					
My Estimate: US East (N. Virginia) Amazon EC 0 9.108 109.3 USD Tenancy (Shared Instances), Operating system (Linux), Workload (Consistent, Number of instances: 1), Advance EC2 instance (t2.micro), Pricing strategy (On-Demand Utilization: 100 %)					
<b>Acknowledgement</b>					
* 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

Created a new CloudTrail trail. It will store the logs in the existing cloudtrail-logs S3 bucket

[CloudTrail](#) > [Trails](#) > arn:aws:cloudtrail:us-east-1:242015798764:trail/data-bucket-reads-writes

### data-bucket-reads-writes

[Delete](#) [Stop logging](#)

#### General details

[Edit](#)

Trail logging  
 Logging

Trail log location  
cloudtrail-logs-08f7fa372b453cb3/AWSLogs/242015798764

Log file validation  
Disabled

SNS notification delivery  
Disabled

Trail name  
data-bucket-reads-writes

Last file validation delivered

Last SNS notification

Multi-region trail  
Yes

Last log file delivered

-

Apply trail to my organization  
Not enabled

Log file SSE-KMS encryption  
Not enabled

It will record both management events and data events in the trail. And for data events, it will log all S3 events.



## Management events

Edit

API activity	Exclude AWS KMS events
All	No Exclude Amazon RDS Data API events No

## Data events

Edit

### Data events: S3

Log selector template  
Log all events

### Selector name

1

## All events

Created a new file locally named “customer-data.csv” and with the below contents:

A	B	C	D	E	F	G	H
Customer	First Name	Last Name	Join Date	Street Adc	City,State	Phone	
1	Alejandro	Rosalez	12/12/2013	123 Main	Any Town	301-555-0158	
2	Jane	Doe	10/5/2014	456 State	!Anywhere	360-555-0163	
3	John	Stiles	9/20/2016	1980 8th S	Nowhere,	914-555-0122	
4	Li	Juan	6/29/2011	1323 22nd	Anytown,	914-555-0149	

Created an Athena table that describes the format of the data in the *clouptrail-logs* S3 bucket.

The screenshot shows the AWS CloudTrail Logs interface. The left sidebar displays the Data source as 'AwsDataCatalog' and the Database as 'default'. Under 'Tables and views', there are two tables: 'bucket\_logs' and 'cloudtrail\_logs\_cloudtrail\_logs\_08f7f4a372b453cb3'. The second table has a row ID '72b455cb5'. The main area shows a query editor with the following content:

```
Query 1 : x | Query 2 : x | Query 3 : x
1 | SELECT * FROM "default"."cloudtrail_logs_cloudtrail_logs_08f7f4a372b453cb3" limit 10;
```

The results pane shows 10 rows of data, each containing eventversion and useridentity fields. The first few rows are:

#	eventversion	useridentity
1	1.09	(type=AWSService, principalId=null, arn=null, accountId=null, invokedBy=cloudtrail.amazonaws.com, accessKeyId=null, username=null, sessionContext=null)
2	1.09	(type=AWSService, principalId=null, arn=null, accountId=null, invokedBy=cloudtrail.amazonaws.com, accessKeyId=null, username=null, sessionContext=null)
3	1.09	(type=AWSService, principalId=null, arn=null, accountId=null, invokedBy=cloudtrail.amazonaws.com, accessKeyId=null, username=null, sessionContext=null)



## Results (10)

 Search rows

Copy

[Download results](#)

< 1 > | 

#	v	eventversion	useridentity
1		1.09	{type=AWSService, principalid=null, arn=null, accountid=null, invokedby=cloudtrail.amazonaws.com, accesskeyid=null, username=null, sessioncontext=null}
2		1.09	{type=AWSService, principalid=null, arn=null, accountid=null, invokedby=cloudtrail.amazonaws.com, accesskeyid=null, username=null, sessioncontext=null}
3		1.09	{type=AWSService, principalid=null, arn=null, accountid=null, invokedby=cloudtrail.amazonaws.com, accesskeyid=null, username=null, sessioncontext=null}
4		1.09	{type=AWSService, principalid=null, arn=null, accountid=null, invokedby=cloudtrail.amazonaws.com, accesskeyid=null, username=null, sessioncontext=null}
5		1.08	{type=AssumedRole, principalid=AROATQWKEAXWLMJPQKBR2i-03071291af5783287, arn=aws:sts::242015798764:assumed-role/WebServerRole/i-03071291af5783287, acco
6		1.08	{type=AssumedRole, principalid=AROATQWKEAXWLMJPQKBR2i-09c84b7b7c201db65, arn=aws:sts::242015798764:assumed-role/WebServerRole/i-09c84b7b7c201db65, acco
7		1.08	{type=AssumedRole, principalid=AROATQWKEAXWCJE5F6G64:user3367184=Yousef_Hassan_Yousef_Eltobgy, arn=aws:sts::242015798764:assumed-role/voclabs/user3367184=
8		1.08	{type=AssumedRole, principalid=AROATQWKEAXWCJE5F6G64:user3367184=Yousef_Hassan_Yousef_Eltobgy, arn=aws:sts::242015798764:assumed-role/voclabs/user3367184=
9		1.08	{type=AssumedRole, principalid=AROATQWKEAXWCJE5F6G64:user3367184=Yousef_Hassan_Yousef_Eltobgy, arn=aws:sts::242015798764:assumed-role/voclabs/user3367184=
10		1.08	{type=AssumedRole, principalid=AROATQWKEAXWCJE5F6G64:user3367184=Yousef_Hassan_Yousef_Eltobgy, arn=aws:sts::242015798764:assumed-role/voclabs/user3367184=

I ran an Athena query to retrieve the CloudTrail event log data for when I uploaded the customer-data.csv file to Amazon S3

The screenshot shows the AWS CloudTrail SQL Query Editor interface. The left sidebar displays the Data source as 'AwsDataCatalog' and the Database as 'default'. Under 'Tables and views', there are two tables: 'bucket\_logs' and 'cloudtrail\_logs'. The 'cloudtrail\_logs' table has two rows: 'cloudtrail\_logs\_08f7f4a3' and '72b453cb5'. The right panel contains a query editor with the following SQL:

```
1 SELECT eventtime, useridentity.principalid, requestparameters, eventname
2 FROM cloudtrail_logs.cloudtrail_logs_08f7f4a3
3 WHERE
4   eventname in ('PutObject') AND
5   requestparameters LIKE '%customer-data.csv%'
6 limit 10;
```

The status bar at the bottom indicates 'SQL Ln 6, Col 10'. Below the editor are buttons for 'Run again', 'Explain', 'Cancel', 'Clear', and 'Create'. The results tab shows one completed result row:

#	eventtime	principalid	requestparameters
1	2024-10-09T12:28:05Z	AROATQWKEAXWCJE5F6G64:user3367184:Yousef_Hassan_Yousef_Eltobgy	{"X-Amz-Date": "20241009T122805Z", "bucketName": "data-bucket-08f7f4a372b453cb5"}

I also created a similar Athena query to retrieve the CloudTrail log information for when I opened (or downloaded) the customer-data.csv file.



# جامعة الاتصالات وتكنولوجيا المعلومات

جامعة مصر الرقمية

Data

Data source: AwsDataCatalog

Database: default

Tables and views

Filter tables and views

Tables (2)

- bucket\_logs
- cloudtrail\_logs\_cloudtrail\_logs\_08f7f14a372b455cb3

Views (0)

Query 1 : x | Query 4 : x

```
1 SELECT eventtime, useridentity.principalid, requestparameters, eventname
2 FROM cloudtrail_logs_cloudtrail_logs_08f7f14a372b455cb3
3 WHERE
4   eventname IN ('GetObject') AND
5   requestparameters LIKE '%customer-data.csv%'
6 limit 10;
```

SQL Ln 6, Col 10

Run again Explain Cancel Clear Create

Reuse query results up to 60 minutes ago

Query results

Completed

Time in queue: 72 ms Run time: 675 ms Data scanned: 140.42 KB

Results (1)

Search rows

#	eventtime	principalid	requestparameters
1	2024-10-09T12:51:03Z	AROATQWKEAXWCJE5F6664:user3367184:Yousef_Hassan_Yousef_Eltobgy	"X-Amz-Date": "20241009T125101Z", "bucketName": "data-bucket-08f7f14a372b455cb3",

Copy Download results

## Task 4.2: Use CloudWatch Logs to monitor secure logs

I created a new CloudWatch log group.

CloudWatch > Log groups > EncryptedInstanceSecureLogs			
Actions ▾ View in Logs Insights Start tailing Search log group			
EncryptedInstanceSecureLogs			
<b>▼ Log group details</b>			
Log class <a href="#">Info</a> Standard	Stored bytes -	KMS key ID -	
ARN <a href="#">arn:aws:logs:us-east-1:242015798764:log-group:EncryptedInstanceSecureLogs:*</a>	Metric filters 0	Anomaly detection <a href="#">Configure</a>	
Creation time Now	Subscription filters 0	Data protection -	
Retention Never expire	Contributor Insights rules -	Sensitive data count -	

Then I used EC2 Instance Connect to connect to EncryptedInstance, and installed the CloudWatch agent and a Linux daemon named collectd, which the CloudWatch agent will use.

```
[ec2-user@ip-10-1-3-8 ~]$ sudo yum install -y amazon-cloudwatch-agent
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Resolving Dependencies
--> Running transaction check
-->> Package amazon-cloudwatch-agent.x86_64 0:1.300044.0-1.amzn2 will be installed
-->> Finished Dependency Resolution

Dependencies Resolved

=====
Package           Arch      Version       Repository   Size
=====
Installing:
amazon-cloudwatch-agent x86_64  1.300044.0-1.amzn2    amzn2-core  135 M

Transaction Summary
Install 1 Package

Total download size: 135 M
Installed size: 445 M
Downloaded packages:
amazon-cloudwatch-agent-1.300044.0-1.amzn2.x86_64.rpm | 135 MB  00:00:01

Running transaction check
Running transaction test
Transaction test succeeded
Preparing transaction
  create group cwagent, result: 0
  create user cwagent, result: 0
  Installing : amazon-cloudwatch-agent-1.300044.0-1.amzn2.x86_64
  Verifying  : amazon-cloudwatch-agent-1.300044.0-1.amzn2.x86_64

Installed:
  amazon-cloudwatch-agent.x86_64 0:1.300044.0-1.amzn2

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



```
[ec2-user@ip-10-1-3-8 ~]$ sudo amazon-linux-extras install -y collectd
Installing collectd
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Cleaning repos: amzn2-core amzn2extra-collectd amzn2extra-docker amzn2extra-kernel-5.10
0 packages available
0 metadata files removed
6 sqlite files removed
0 metadata files removed
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd

amzn2extra-collectd
amzn2extra-docker
amzn2extra-kernel-5.10
amzn2extra-kernel-5.10
  amzn2-core/x86_64/updateinfo
(3/9): amzn2-core/x86_64/group.gz
(3/9): amzn2extra-docker/x86_64/primary_db
(4/9): amzn2extra-kernel-5.10/x86_64/updateinfo
(4/9): amzn2extra-kernel-5.10/x86_64/primary_db
(6/9): amzn2extra-collectd/x86_64/primary_db
(7/9): amzn2extra-docker/x86_64/updateinfo
(8/9): amzn2extra-kernel-5.10/x86_64/primary_db
(8/9): amzn2extra-kernel-5.10/x86_64/primary_db
Resolving Dependencies
--> Running transaction check
--> Package collectd.x86_64 0:5.8.1-1.amzn2.0.2 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

-----
```

Package	Arch	Version	Repository	Size
collectd	x86_64	5.8.1-1.amzn2.0.2	amzn2extra-collectd	706 K

Then I downloaded and configured a JSON file that provides configuration details for the CloudWatch agent

```
[ec2-user@ip-10-1-3-8 ~]$ sudo wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-RE-200-ACCPA6-91846/capstone-6-security/s3/config.json -P /opt/aws/amazon-cloudwatch-agent/bin/
[ec2-user@ip-10-1-3-8 ~]$ curl -v https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-RE-200-ACCPA6-91846/capstone-6-security/s3/config.json
Resolving aws-tc-largeobjects.s3.us-west-2.amazonaws.com (aws-tc-largeobjects.s3.us-west-2.amazonaws.com)... 52.92.152.234, 52.218.232.177, 52.92.241.2, ...
Connecting to aws-tc-largeobjects.s3.us-west-2.amazonaws.com (aws-tc-largeobjects.s3.us-west-2.amazonaws.com)|52.92.152.234|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2278 (2.2K) [application/json]
Saving to: '/opt/aws/amazon-cloudwatch-agent/bin/config.json'

100%[=====] 2,278 --.-K/s in 0s

2024-10-09 13:01:32 (171 MB/s) - '/opt/aws/amazon-cloudwatch-agent/bin/config.json' saved [2278/2278]

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

To print out the file template so that I can see what it specifies:

```
[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": {
                "collected": {
                    "metrics_aggregation_interval": 60
                },
                "disk": {
                    "measurement": [
                        "used_percent"
                    ],
                    "metrics_collection_interval": 60,
                    "resources": [
                        "*"
                    ],
                    "ignore_file_system_types": [
                        "sysfs", "devtmpfs"
                    ]
                },
                "mem": {
                    "measurement": [
                        "mem_used_percent"
                    ],
                    "metrics_collection_interval": 60
                },
                "statsd": {
                    "metrics_aggregation_interval": 60,
                    "metrics_collection_interval": 10,
                    "service_address": ":8125"
                }
            }
        ]
    }
}
[ec2-user@ip-10-1-3-8 ~]$
```

Then I started the CloudWatch agent.



```
[ec2-user@ip-10-1-3-8 ~]$ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json
*** processing configuration for CloudWatch Agent ***
!! Trying to detect region from ec2 D! [Ec2] Found active network interface !! imds retry client will retry 1 timesSuccessfully fetched the config and saved in /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp
Start configuration validation...
2024/10/09 13:03:18 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp ...
2024/10/09 13:03:18 !! Valid Json input schema.
2024/10/09 13:03:18 D! ec2tagger processor required because append_dimensions is set
2024/10/09 13:03:18 Configuration validation first phase succeeded
2024/10/09 13:03:18 D! Trying to detect region from ec2
D! [Ec2] Found active network interface
!! 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
amazon-cloudwatch-agent has already been stopped
Created symlink /etc/systemd/system/multi-user.target.wants/amazon-cloudwatch-agent.service to /etc/systemd/system/amazon-cloudwatch-agent.service.
[ec2-user@ip-10-1-3-8 ~]$
```

and confirmed that it is running:

```
[ec2-user@ip-10-1-3-8 ~]$ 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 13:03:19 UTC; 16s ago
      Main PID: 814 (amazon-cloudwatch)
        CPU: 0.000 CPU(s) @ 2.00GHz
         CPU%: 0.00%
       CGroup: /system.slice/amazon-cloudwatch-agent.service
                 └─ 814 /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml -envconfig /opt/aws/amazon-cloudwatch-agent/etc...

Oct 09 13:03:20 ip-10-1-3-8.ec2.internal start-amazon-cloudwatch-agent[814]: 2024/10/09 13:03:20 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json ...
Oct 09 13:03:20 ip-10-1-3-8.ec2.internal start-amazon-cloudwatch-agent[814]: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json does not exist or cannot read. Skipp...
n agent... .json ...
Oct 09 13:03:20 ip-10-1-3-8.ec2.internal start-amazon-cloudwatch-agent[814]: 2024/10/09 13:03:20 !! Valid Json input schema.
Oct 09 13:03:20 ip-10-1-3-8.ec2.internal start-amazon-cloudwatch-agent[814]: 2024/10/09 13:03:20 !! Detecting run_as_user...
Oct 09 13:03:20 ip-10-1-3-8.ec2.internal start-amazon-cloudwatch-agent[814]: 2024/10/09 13:03:20 !! Detecting region from ec2
Oct 09 13:03:20 ip-10-1-3-8.ec2.internal start-amazon-cloudwatch-agent[814]: 2024/10/09 13:03:20 D! ec2tagger processor required because append_dimensions is set
Oct 09 13:03:20 ip-10-1-3-8.ec2.internal start-amazon-cloudwatch-agent[814]: 2024/10/09 13:03:20 Configuration validation first phase succeeded
Oct 09 13:03:20 ip-10-1-3-8.ec2.internal start-amazon-cloudwatch-agent[814]: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json does not exist or cannot read. Skipp...
g it.
Oct 09 13:03:20 ip-10-1-3-8.ec2.internal start-amazon-cloudwatch-agent[814]: !! Detecting run_as_user...
Hint: Some lines were ellipsized, use -l to show in full.
[ec2-user@ip-10-1-3-8 ~]$
```

To confirm that the CloudWatch agent is able to reach the CloudWatch service in your AWS account,

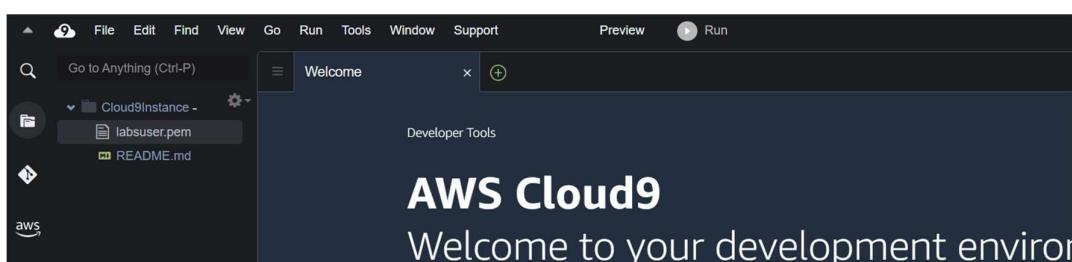
```
[ec2-user@ip-10-1-3-8 ~]$ 
[ec2-user@ip-10-1-3-8 ~]$ sudo cat /opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log
2024/10/09 13:03:20 I! Config has been translated into TOML /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml
2024/10/09 13:03:20 D! config [agent]
  collection_jitter = "0s"
  debug = false
  flush_interval = "1s"
  flush_jitter = "0s"
  hostname = ""
  interval = "60s"
  logfile = "/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log"
  logtarget = "lumberjack"
  metric_batch_size = 1000
  metric_buffer_limit = 10000

2024/10-09T13:03:21Z I! First time setting retention for log group EncryptedInstanceSecureLogs, update map to avoid setting twice
2024/10-09T13:03:21Z I! [outputs.cloudwatchlogs] Configured middleware on AWS client
2024/10-09T13:03:21Z I! [logagent] piping log from EncryptedInstanceSecureLogs->EncryptedInstancesecureLogs-1-03071291af5783287(/var/log/secure) to cloudwatchlogs with retention 180
2024/10-09T13:03:26Z W! [outputs.cloudwatchlogs] Retried 0 time, going to sleep 161.589796ms before retrying.
[ec2-user@ip-10-1-3-8 ~]$
```

To actively tail the /var/log/secure file so that you can monitor the logs that will be created in the next step, I used the following command:

```
[ec2-user@ip-10-1-3-8 ~]$ 
[ec2-user@ip-10-1-3-8 ~]$ sudo tail -f /var/log/secure
Oct 9 13:03:16 ip-10-1-3-8 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Oct 9 13:03:19 ip-10-1-3-8 sudo: pam_unix(sudo:session): session closed for user root
Oct 9 13:03:35 ip-10-1-3-8 sudo: ec2-user : TTY:pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/sbin/service#040amazon-cloudwatch-agent#040status
Oct 9 13:03:35 ip-10-1-3-8 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Oct 9 13:07:20 ip-10-1-3-8 sudo: ec2-user : TTY:pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/cat#040/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log
Oct 9 13:07:20 ip-10-1-3-8 sudo: pam_unix(sudo:session): session closed for user root
Oct 9 13:08:52 ip-10-1-3-8 sudo: ec2-user : TTY:pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/tail#040-f#040/var/log/secure
Oct 9 13:08:52 ip-10-1-3-8 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
^C
[ec2-user@ip-10-1-3-8 ~]$
```

Then I uploaded the key to the cloud9 instance





Then I became able to SSH to the EncryptedInstance instance from the cloud9 instance.

```
voclabs:~/environment $ chmod 400 labsuser.pem
voclabs:~/environment $
voclabs:~/environment $ ssh -i labsuser.pem ec2-user@3.236.163.130
The authenticity of host '3.236.163.130 (3.236.163.130)' can't be established.
EDSA key fingerprint is SHA256:mkb8xuvMyb3LRtpmXs203EBDAYxpFRCWHR6IykX0q0Q.
EDSA key fingerprint is MD5:c7:39:ac:8b:b0:49:8a:b7:c7:5e:4a:05:74:3e:57:57.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '3.236.163.130' (EDSA) to the list of known hosts.
Last login: Wed Oct  9 12:59:08 2024 from ec2-18-206-107-27.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.
~/'      https://aws.amazon.com/linux/amazon-linux-2023/
[ec2-user@ip-10-1-3-8 ~]$
```

But if I tried with user “ubuntu”, it will result in permission denied. Because it doesn't exist on this Amazon Linux instance.

```
voclabs:~/environment $
voclabs:~/environment $ ssh -i labsuser.pem ubuntu@3.236.163.130
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $
```

And here are the logs that recorded the successful connection from ec2-user, and the failed request from user ubuntu

▼ 2024-10-09T13:16:57.653Z	Oct 9 13:12:14 ip-10-1-3-8 sshd[919]: Accepted publickey for ec2-user from 52.1.136.202 port 46392 ssh2: RSA SHA256:RJP8SO+vEvSAH6Zebbgkpien02VFaRJPd2PtKSUfHw	<a href="#">EncryptedInstanceSecureLogs-i-03071291af5783287</a>
▶ 2024-10-09T13:16:57.653Z	Oct 9 13:12:14 ip-10-1-3-8 sshd[919]: pam_unix(sshd:session): session opened for user ec2-user on terminal pts/0	<a href="#">EncryptedInstanceSecureLogs-i-03071291af5783287</a>
▶ 2024-10-09T13:16:57.653Z	Oct 9 13:16:57 ip-10-1-3-8 sshd[1116]: Received disconnect from 52.1.136.202 port 46392 (ssh2)	<a href="#">EncryptedInstanceSecureLogs-i-03071291af5783287</a>
▶ 2024-10-09T13:16:57.653Z	Oct 9 13:16:57 ip-10-1-3-8 sshd[1116]: Disconnected from 52.1.136.202 port 46392 (ssh2)	<a href="#">EncryptedInstanceSecureLogs-i-03071291af5783287</a>
▶ 2024-10-09T13:17:02.224Z	Oct 9 13:16:57 ip-10-1-3-8 sshd[919]: pam_unix(sshd:session): session closed for user ec2-user	<a href="#">EncryptedInstanceSecureLogs-i-03071291af5783287</a>
▼ 2024-10-09T13:17:19.959Z	Oct 9 13:17:19 ip-10-1-3-8 sshd[1147]: Invalid user ubuntu from 52.1.136.202 port 51576	<a href="#">EncryptedInstanceSecureLogs-i-03071291af5783287</a>
Oct 9 13:17:19 ip-10-1-3-8 sshd[1147]: Invalid user ubuntu from 52.1.136.202 port 51576		
▼ 2024-10-09T13:17:19.959Z	Oct 9 13:17:19 ip-10-1-3-8 sshd[1147]: input_userauth_request: invalid user ubuntu [preauth]	<a href="#">EncryptedInstanceSecureLogs-i-03071291af5783287</a>
Oct 9 13:17:19 ip-10-1-3-8 sshd[1147]: input_userauth_request: invalid user ubuntu [preauth]		
▼ 2024-10-09T13:17:24.224Z	Oct 9 13:17:19 ip-10-1-3-8 sshd[1147]: Connection closed by 52.1.136.202 port 51576 [preauth]	<a href="#">EncryptedInstanceSecureLogs-i-03071291af5783287</a>
Oct 9 13:17:19 ip-10-1-3-8 sshd[1147]: Connection closed by 52.1.136.202 port 51576 [preauth]		

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

Created a new metric filter in the EncryptedInstanceSecureLogs CloudWatch log group.

The screenshot shows the AWS CloudWatch Metrics Filter interface. At the top, there are tabs for Log streams, Tags, Anomaly detection, Metric filters (which is selected), Subscription filters, Contributor Insights, and Data protection. Below the tabs, a search bar says "Find metric filters". There is a single metric filter listed:

- Not valid users**
- Filter pattern: "Invalid user"
- Metric: `secure / NotValidUsers`
- Metric value: 1
- Default value: 0
- Unit: Count
- Dimensions: -
- Alarms: None.

Created a CloudWatch alarm from the metric filter that I just created. It will send a notification for Not valid access attempts over SSH to the EncryptedInstance server are greater than or equal 5 in the last 24 hours.

The screenshot shows the AWS CloudWatch Alarms interface. At the top, there are buttons for Hide Auto Scaling alarms, Clear selection, Create composite alarm, Actions, and Create alarm (which is highlighted). Below the buttons, a search bar and filters are shown. A single alarm is listed:

- Name**: Not valid users exceeding limit on EncryptedInstance
- State**: Insufficient data
- Last state update (UTC)**: 2024-10-09 13:28:00
- Conditions**: `NotValidUsers >= 5 for 1 datapoints within 1 day`
- Actions**: Actions enabled

And confirmed the subscription.

The screenshot shows a web browser displaying a confirmation message from the Simple Notification Service (AWS SNS). The URL is [https://sns.us-east-1.amazonaws.com/confirmation.html?TopicArn=arn:aws:sns:us-east-1:242015798764:Not\\_valid\\_users\\_exceeding\\_limit&Token=2336412f37fb68](https://sns.us-east-1.amazonaws.com/confirmation.html?TopicArn=arn:aws:sns:us-east-1:242015798764:Not_valid_users_exceeding_limit&Token=2336412f37fb68).

The message content is:

**Subscription confirmed!**

You have successfully subscribed.

Your subscription's id is:  
`arn:aws:sns:us-east-1:242015798764:Not_valid_users_exceeding_limit:8087072c-99e1-4789-b335-f76d76dc8bf`

If it was not your intention to subscribe, [click here to unsubscribe](#).

I made five invalid SSH access attempts to connect to the EncryptedInstance public IP address over SSH



```
voclabs:~/environment $  
voclabs:~/environment $ ssh -i labsuser.pem ubuntu@3.236.163.130  
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).  
voclabs:~/environment $  
voclabs:~/environment $  
voclabs:~/environment $  
voclabs:~/environment $ ssh -i labsuser.pem ubuntu@3.236.163.130  
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).  
voclabs:~/environment $  
voclabs:~/environment $  
voclabs:~/environment $  
voclabs:~/environment $  
voclabs:~/environment $ ssh -i labsuser.pem ubuntu@3.236.163.130  
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).  
voclabs:~/environment $  
voclabs:~/environment $  
voclabs:~/environment $  
voclabs:~/environment $  
voclabs:~/environment $ ssh -i labsuser.pem ubuntu@3.236.163.130  
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).  
voclabs:~/environment $  
voclabs:~/environment $  
voclabs:~/environment $  
voclabs:~/environment $  
voclabs:~/environment $ ssh -i labsuser.pem ubuntu@3.236.163.130  
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).  
voclabs:~/environment $  
voclabs:~/environment $
```

There are logs in the log group that detected the invalid user trying to log in

▶ 2024-10-09T13:30:16.627Z	Oct 9 13:30:16 ip-10-1-3-8 sshd[1183]: Invalid user ubuntu from 52.1.13...	<a href="#">EncryptedInstanceSecureLogs-i-03071291af5f783287</a>
▼ 2024-10-09T13:30:18.633Z	Oct 9 13:30:18 ip-10-1-3-8 sshd[1185]: Invalid user ubuntu from 52.1.13...	<a href="#">EncryptedInstanceSecureLogs-i-03071291af5f783287</a>
Oct 9 13:30:18 ip-10-1-3-8 sshd[1185]: Invalid user ubuntu from 52.1.136.202 port 47682		
▼ 2024-10-09T13:30:20.386Z	Oct 9 13:30:20 ip-10-1-3-8 sshd[1187]: Invalid user ubuntu from 52.1.13...	<a href="#">EncryptedInstanceSecureLogs-i-03071291af5f783287</a>
Oct 9 13:30:20 ip-10-1-3-8 sshd[1187]: Invalid user ubuntu from 52.1.136.202 port 47684		
▼ 2024-10-09T13:31:29.566Z	Oct 9 13:31:29 ip-10-1-3-8 sshd[1190]: Invalid user ubuntu from 52.1.13...	<a href="#">EncryptedInstanceSecureLogs-i-03071291af5f783287</a>
Oct 9 13:31:29 ip-10-1-3-8 sshd[1190]: Invalid user ubuntu from 52.1.136.202 port 52732		
▼ 2024-10-09T13:31:32.324Z	Oct 9 13:31:32 ip-10-1-3-8 sshd[1192]: Invalid user ubuntu from 52.1.13...	<a href="#">EncryptedInstanceSecureLogs-i-03071291af5f783287</a>
Oct 9 13:31:32 ip-10-1-3-8 sshd[1192]: Invalid user ubuntu from 52.1.136.202 port 52736		
▼ 2024-10-09T13:31:34.831Z	Oct 9 13:31:34 ip-10-1-3-8 sshd[1194]: Invalid user ubuntu from 52.1.13...	<a href="#">EncryptedInstanceSecureLogs-i-03071291af5f783287</a>
Oct 9 13:31:34 ip-10-1-3-8 sshd[1194]: Invalid user ubuntu from 52.1.136.202 port 44082		
Back to top ^		

Also the CloudWatch alarm became in “in alarm” state

CloudWatch > Alarms						
Alarms (1)						
<input type="checkbox"/> Name		State	Last state update (UTC)	Conditions	Actions	
<input type="checkbox"/>	Not valid users exceeding limit on Encryptedinstance	<span style="color: red;">⚠ In alarm</span>	2024-10-09 13:31:46	NotValidUsers >= 5 for 1 datapoints within 1 day	<span style="color: green;">Actions enabled</span>	

Plus I received a notification on the mail.



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



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

to me ▾

16:31 (1 minute 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 [5.0 (08/10/24 13:31:00)] was greater than or equal to the threshold (5.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Wednesday 09 October, 2024 13:31:46 UTC".

View this alarm in the AWS Management Console:

<https://us-east-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-1#alarms/V2: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: INSUFFICIENT\_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [5.0 (08/10/24 13:31:00)] was greater than or equal to the threshold (5.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Wednesday 09 October, 2024 13:31:46 UTC
- AWS Account: 242015798764
- Alarm Arn: arn:aws:cloudwatch:us-east-1:242015798764: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-1:242015798764:Not\_valid\_users\_exceeding\_limit]
- INSUFFICIENT\_DATA:

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

I have two roles the first role grants permissions that you will need to set up AWS Config, and the second role is the role that AWS Systems Manager will use when it performs remediation actions with an AWS Config managed rule that you will use.

IAM > Roles > AWSConfigRole

**AWSConfigRole** [Info](#) [Delete](#)

AWSConfigRole, based upon

**Summary** [Edit](#)

Creation date	ARN
October 06, 2024, 21:04 (UTC+03:00)	<a href="#">arn:aws:iam::242015798764:role/AWSConfigRole</a>
Last activity	Maximum session duration
-	1 hour

**Permissions** [Trust relationships](#) [Tags \(1\)](#) [Last Accessed](#) [Revoke sessions](#)

**Permissions policies (2)** [Info](#) [Add permissions](#)

You can attach up to 10 managed policies.

Filter by Type: All types

Policy name	Type	Attached entities
<a href="#">AWS_ConfigRole</a>	AWS managed	1
<a href="#">S3Full</a>	Customer inline	0



IAM > Roles > SSMAutomationRole

### SSMAutomationRole [Info](#)

Used by AWS Config to turn on object logging.

Summary		<a href="#">Edit</a>
Creation date	October 06, 2024, 21:04 (UTC+03:00)	ARN
Last activity	-	arn:aws:iam::242015798764:role/SSMAutomationRole
		Maximum session duration 1 hour

[Permissions](#) [Trust relationships](#) [Tags \(1\)](#) [Last Accessed](#) [Revoke sessions](#)

**Permissions policies (2) [Info](#)**

You can attach up to 10 managed policies.

Policy name		Type	Attached entities
<input type="checkbox"/>	<a href="#">AmazonS3FullAccess</a>	AWS managed	3
<input type="checkbox"/>	<a href="#">AmazonSSMAutomationRole</a>	AWS managed	1

I also have the below bucket that AWS Config will use this bucket for logging purposes.

Amazon S3 > Buckets > aws-config-08f7f4a372b453cb3 [Info](#)

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

**Objects (0) [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
No objects					
You don't have any objects in this bucket.					

[Upload](#)

I created the below bucket

Amazon S3 > Buckets > compliance-bucket-08f7f4a372b453cb3 [Info](#)

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

**Objects (0) [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
No objects					
You don't have any objects in this bucket.					

[Upload](#)

Then I edited the object ownership in the “s3-objects-access-log” bucket. I enabled ACLs.



#### 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.

[Edit](#)

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.

Then I set up AWS Config to record all current and future resources that are supported in the us-east-1 Region. For AWS Config role, I used the existing AWSConfigRole role. For delivery method, I chose the existing aws-config bucket. And I didn't select any managed rules.

Then I created AWS Config Rule:

AWS Config > Rules > s3-bucket-logging-enabled

### s3-bucket-logging-enabled

Actions ▾

Rule details			
Description	Enabled evaluation mode	Detective evaluation trigger type	
Checks if logging is enabled for your S3 buckets. The rule is NON_COMPLIANT if logging is not enabled.	• DETECTIVE	• Oversized configuration changes	
Config rule ARN	Last successful detective evaluation	• Configuration changes	
arn:aws:config:us-east-1:242015798764:config-rule/config-rule-92zjd	⌚ Not available	Scope of changes	
		Resources	
		Resource types	
		S3 Bucket	
Parameters			
Key	Type	Value	Description
targetBucket	String	-	Target S3 bucket for storing server access logs.
targetPrefix	String	-	Prefix of the S3 bucket for storing server access logs.

Confirmed that the s3-bucket-logging-enabled rule that I defined is finding resources that are in scope. I also confirmed that the compliance-bucket is flagged as noncompliant.

Resources in scope

Noncompliant ▾

View details Remediate ⌂

ID	Type	Status	Annotation	Compliance
athena-results-08f7f4a372b453cb3	S3 Bucket	-	-	⚠ Noncompliant
aws-athena-query-results-242015798764-us-east-1	S3 Bucket	-	-	⚠ Noncompliant
aws-cloudtrail-logs-242015798764-79b6b913	S3 Bucket	-	-	⚠ Noncompliant
aws-config-08f7f4a372b453cb3	S3 Bucket	-	-	⚠ Noncompliant
cloudtrail-logs-08f7f4a372b453cb3	S3 Bucket	-	-	⚠ Noncompliant
compliance-bucket-08f7f4a372b453cb3	S3 Bucket	-	-	⚠ Noncompliant
s3-inventory-08f7f4a372b453cb3	S3 Bucket	-	-	⚠ Noncompliant
s3-objects-access-log-08f7f4a372b453cb3	S3 Bucket	-	-	⚠ Noncompliant

The compliance-bucket is flagged as Noncompliant, that is because the “server access logging” is disabled.



### Server access logging

Log requests for access to your bucket. Use [CloudWatch](#) to check the health of your server access logging. [Learn more](#)

Edit

Server access logging  
Disabled

Then I configured manual remediation settings for the s3-bucket-logging-enable rule.

Remediation action			
Remediation action	AWS-ConfigureS3BucketLogging	Description	Enables Logging on S3 Bucket
<strong>Parameters</strong>			
<strong>Key</strong>			
AutomationAssumeRole	arn:aws:iam::242015798764:role/SSMAutomationRole	Description	(Optional) The ARN of the role that allows Automation to perform the remediation action.
TargetPrefix	-	Description	(Optional) Specifies a prefix for the keys under which the log files will be stored.
GranteeEmailAddress	-	Description	(Optional) Email address of the grantee.
GranteeType	CanonicalUser	Description	(Optional) Type of grantee.
BucketName	RESOURCE_ID	Description	(Required) The name of the Amazon S3 Bucket for which you want to enable logging.
GranteeId	0ceba13b9b1642ab6e03a433562738f9a98e061013711e9b923e5b34a193faeb	Description	(Optional) The canonical user ID of the grantee.
GranteeUri	-	Description	(Optional) URI of the grantee group.
TargetObjectKeyPartitionDataSource	-	Description	(Optional) Specifies the partition date source for the partitioned prefix.
GrantedPermission	FULL_CONTROL	Description	(Optional) Logging permissions assigned to the Grantee for the bucket.

Then to test this, I select the “compliance bucket” bucket and then chose “remediate” button. That is to invoke the AWS Config remediation action so that object logging is enabled on the “compliance-bucket”.

Resources in scope					
Noncompliant		View details		Remediate	C
ID	Type	Status	Annotation	Compliance	
athena-results-08f7f4a372b453cb3	S3 Bucket	-	-	<span style="color: red;">⚠ Noncompliant</span>	
aws-athena-query-results-242015798764-us-east-1	S3 Bucket	-	-	<span style="color: red;">⚠ Noncompliant</span>	
aws-cloudtrail-logs-242015798764-79b6b913	S3 Bucket	-	-	<span style="color: red;">⚠ Noncompliant</span>	
aws-config-08f7f4a372b453cb3	S3 Bucket	-	-	<span style="color: red;">⚠ Noncompliant</span>	
cloudtrail-logs-08f7f4a372b453cb3	S3 Bucket	-	-	<span style="color: red;">⚠ Noncompliant</span>	
compliance-bucket-08f7f4a372b453cb3	S3 Bucket	<span style="color: green;">⌚ Action execution queued..</span>	-	<span style="color: red;">⚠ Noncompliant</span>	
s3-inventory-08f7f4a372b453cb3	S3 Bucket	-	-	<span style="color: red;">⚠ Noncompliant</span>	
s3-objects-access-log-08f7f4a372b453cb3	S3 Bucket	-	-	<span style="color: red;">⚠ Noncompliant</span>	

Then I confirmed that the server access logging is now enabled on the compliance-bucket. It was enabled by the remediation rule that I just ran.

### Server access logging

Log requests for access to your bucket. Use [CloudWatch](#) to check the health of your server access logging. [Learn more](#)

Edit

Server access logging  
Enabled

Destination bucket  
<s3://s3-objects-access-log-08f7f4a372b453cb3>

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



## Cost assessment for monitoring and logging

does the use of CloudTrail, CloudWatch, and AWS Config security features result in additional cost in the account?

Here is the answer.

AWS Pricing Calculator > My Estimate

## My Estimate [Edit](#)

[Export](#) [Share](#)

**Estimate summary** [Info](#)

Upfront cost 0.00 USD	Monthly cost 130.30 USD	Total 12 months cost <b>1,563.60 USD</b> Includes upfront cost
--------------------------	----------------------------	--

**Getting Started with AWS**

[Get started for free](#) [Contact Sales](#)

---

### My Estimate

<input type="checkbox"/>	Service Name	Status	Upfront cost	Monthly cost	Description	Region	Config Summary
<input type="checkbox"/>	AWS CloudTrail	0 -	0.00 USD	0.00 USD	-	US East (N. Virginia)	Management events unit...
<input type="checkbox"/>	Amazon CloudWatch	0 -	0.00 USD	0.30 USD	-	US East (N. Virginia)	Number of Metrics (incl...)
<input type="checkbox"/>	AWS Config	0 -	0.00 USD	130.00 USD	-	US East (N. Virginia)	Number of Continuous C...

Here it is in csv format:



## The Badge



This badge was issued to [Yousef Hassan Yousef Eltobgy](#) on October 09, 2024  
[View celebrations](#)

[Share](#) [...](#)



### AWS Academy Graduate - AWS Academy Cloud Security Builder

Issued by [Amazon Web Services Training and Certification](#)

Earners of this badge have completed AWS Academy Lab Project - Cloud Security Builder.

[Learn more](#)

#### Skills





**Yousef Hassan Yousef Eltobgy**

**Certificate of Completion for**  
AWS Academy Graduate - AWS Academy Cloud Security Builder

**Course hours completed**  
12 hours

**Issued on**  
10/09/2024

**Digital badge**  
<https://www.credly.com/go/nYaMg99a>

**aws academy**